
EC-Council
USER
INTERFACE
NICE Cybersecurity
Workforce Framework (NCWF)
and EC-Council Certification Mapping

National Initiative for Cybersecurity Education (NICE)

About NICE

The National Initiative for Cybersecurity Education (NICE), led by the National Institute of Standards and Technology (NIST) in the U.S. Department of Commerce, is a partnership between government, academia, and the private sector focused on cybersecurity education, training, and workforce development. Located in the Information Technology Laboratory at NIST, the NICE Program Office operates under the Applied Cybersecurity Division, positioning the program to support the country's ability to address current and future cybersecurity challenges through standards and best practices.

The mission of NICE is to energize and promote a robust network and an ecosystem of cybersecurity education, training, and workforce development. NICE fulfills this mission by coordinating with government, academic, and industry partners to build on existing successful programs, facilitate change and innovation, and bring leadership and vision to increase the number of skilled cybersecurity professionals helping to keep our Nation secure.

NICE Strategic Plan

The NICE Strategic Plan is the result of engagement and deliberation among NICE partners in government, academia, and industry. The overall intent of the Strategic Plan is to provoke a national conversation and guide action on how to address the critical shortage of a skilled cybersecurity workforce.

Values:

- Seek Evidence – inform actions or decisions with data and pursue objective and reliable sources of information
- Pursue Action – create concrete steps towards deliverable outcomes to achieve mission and goals
- Challenge Assumptions – examine rationale for past and present education, training, and workforce approaches and apply critical analysis to future solutions
- Drive Change – seek creative and innovative solutions that might disrupt or defy the status quo
- Stimulate Innovation – inspire and experiment with new approaches to education, training, and skills development
- Foster Communication – raise awareness of cybersecurity education and workforce issues and encourage openness to build trust
- Facilitate Collaboration – combine the knowledge and skills of multiple stakeholders with multiple viewpoints to achieve the best outcomes
- Share Resources – leverage, support, and raise awareness of community-developed approaches and solutions
- Model Inclusion – encourage participation from stakeholders with diverse backgrounds and viewpoints
- Measure Results – assess the effectiveness of results through both quantitative metrics and qualitative measures

National Initiative for Cybersecurity Education (NICE)

Goal #1 Accelerate Learning and Skills Development

Inspire a sense of urgency in both the public and private sectors to address the shortage of skilled cybersecurity workers

Objectives:

1.1 Stimulate the development of approaches and techniques that can more rapidly increase the supply of qualified cybersecurity workers

1.2 Advance programs that reduce the time and cost for obtaining knowledge, skills, and abilities for in-demand work roles

1.3 Engage displaced workers or underemployed individuals who are available and motivated to assume cybersecurity work roles

1.4 Experiment with the use of apprenticeships and cooperative education programs to provide an immediate workforce that can earn a salary while they learn the necessary skills

1.5 Explore methods to identify gaps in cybersecurity skills and raise awareness of training that addresses identified workforce needs

Goal #2 Nurture a Diverse Learning Community

Strengthen education and training across the ecosystem to emphasize learning, measure outcomes, and diversify the cybersecurity workforce

Objectives:

2.1 Improve education programs, co-curricular experiences, and training and certifications

2.2 Encourage tools and techniques that effectively measure and validate individual aptitude, knowledge, skills, and abilities

2.3 Inspire cybersecurity career awareness with students in elementary school, stimulate cybersecurity career exploration in middle school, and enable cybersecurity career preparedness in high school

2.4 Grow creative and effective efforts to increase the number of women, minorities, veterans, persons with disabilities, and other underrepresented populations in the cybersecurity workforce

2.5 Facilitate the development and dissemination of academic pathways for cybersecurity careers

National Initiative for Cybersecurity Education (NICE)

Goal #3 Guide Career Development and Workforce Planning

Support employers to address market demands and enhance recruitment, hiring, development, and retention of cybersecurity talent.

Objectives:

3.1 Identify and analyze data sources that support projecting present and future demand and supply of qualified cybersecurity workers

3.2 Publish and raise awareness of the National Cybersecurity Workforce Framework and encourage adoption

3.3 Facilitate state and regional consortia to identify cybersecurity pathways addressing local workforce needs

3.4 Promote tools that assist human resource professionals and hiring managers with recruitment, hiring, development, and retention of cybersecurity professionals

3.5 Collaborate internationally to share best practices in cybersecurity career development and workforce planning

NICE Working Group

The NICE Working Group (NICEWG) has been established to provide a mechanism in which public and private sector participants can develop concepts, design strategies, and pursue actions that advance cybersecurity education, training, and workforce development.

NICE Working Group Structure and Leadership

The NICE Working Group is led by three co-chairs, each representing Academia, Private Industry, or Government. The current co-chairs are:

- Academic: Kathi Hiyane-Brown, President of Whatcom Community College
- Industry: Andre Thornton, Founder and CEO of Whitman Consulting
- Government: Rodney Petersen, Director of NICE at the National Institute of Standards and Technology

The NICE Working Group is comprised of five sub-working groups. Each subgroup meets independent of the NICEWG and reports out at the NICEWG Meetings. The subgroups are:

- K-12
- Collegiate
- Competitions

National Initiative for Cybersecurity Education (NICE)

- Training and Certifications
- Workforce Management

NICE Interagency Coordinating Council

The NICE Interagency Coordinating Council (ICC) convenes federal government partners of NICE for consultation, communication, and coordination of policy initiatives and strategic directions related to cybersecurity education, training, and workforce development.

NICE Cybersecurity Workforce Framework (NCWF)

Introduction to NICE Cybersecurity Workforce Framework (NCWF)

The NCWF can be viewed as a cybersecurity workforce dictionary, and consumers of the NCWF can reference it for different workforce development, education, and/or training purposes. For instance, it provides a starting point and helps set standards for developing academic pathways, career pathways, position descriptions, and training content. The NCWF helps to ensure our nation is able to educate, recruit, train, develop, and retain a highly-qualified cybersecurity workforce. It serves several key audiences within the cybersecurity community including:

- **Employers**, to help assess their cybersecurity workforce, identify critical gaps in cybersecurity staffing, and improve position descriptions;
- **Current and future employees**, to help explore Tasks and Work Roles and assist with understanding the KSAs that are being valued by employers for in-demand cybersecurity jobs and positions. The NCWF also enables staffing specialists and guidance counsellors to use the NCWF as a resource to support these employees or job seekers;
- **Training and certification providers** who desire to help current and future members of the cybersecurity workforce gain and demonstrate the KSAs;
- **Education providers** who may use the NCWF as a reference to develop curriculum, courses, seminars, and research that cover the KSAs and Tasks described; and
- **Technology providers** who can identify cybersecurity Work Roles and specific Tasks and KSAs associated with services and hardware/software products they supply.

As a mechanism to organize information technology (IT), cybersecurity, and cyber-related work, the NCWF helps organizations to organize roles and responsibilities through the following components:

- **Categories** – A high-level grouping of common cybersecurity functions;
- **Specialty Areas** – Distinct areas of cybersecurity work;
- **Work Roles** – The most detailed groupings of IT, cybersecurity, or cyber-related work, which include specific knowledge, skills, and abilities required to perform a set of tasks;
- **Tasks** – Specific work activities that could be assigned to a professional working in one of the NCWF's Work Roles; and
- **Knowledge, Skills, and Abilities (KSAs)** – Attributes required to perform Tasks, generally demonstrated through relevant experience or performance-based education and training.

The NCWF components work together to describe the range of cybersecurity work, from a high level to the very granular. Each Category contains Specialty Areas, each of which contains one or more Work Roles. Each Work Role is composed of numerous Tasks and KSAs. Providing this range of detail helps organizations to systematically build their cybersecurity workforce, which, in turn, enables improved performance, cost-effective workforce management, and continuous readiness.

While some of the NCWF is based on federal government programs, any organization with cybersecurity workforce needs will benefit from the standards described and can customize the NCWF as needed.

NICE Cybersecurity Workforce Framework (NCWF)

Using the NCWF as described above will help strengthen an organization's cybersecurity workforce. Investment in the existing workforce, such as through initiatives focused on training and retaining existing talent, will help the organization to prepare for and realize its risk management objectives. The common language provided by the NCWF also helps bridge workforce needs to external frameworks, such as the Cybersecurity Framework (CSF), the U.S. Department of Labor Competency Models, the U.S. Department of Education Employability Skills Framework, and the National Security Agency(NSA)/Department of Homeland Security(DHS) National Centers of Academic Excellence in Cyber Defense (CAE-CD) Knowledge Units.

The NCWF builds upon decades of industry research into how to effectively manage the risks to valuable organizational electronic and physical information. Cybersecurity tactics are ever-changing, always identifying new ways to gain information advantage through technology. As we evolve, the ways we perform cybersecurity functions continue to evolve, as must the components of the NCWF. As part of an ongoing collaborative approach, NICE will periodically consider recommendations received and will update the NCWF publication(s). Additionally, new reference materials or tools will be developed to cross-reference elements of the NCWF. To the extent possible, digital reference materials will be posted to the NICE website as an aid to applying and utilizing NCWF and associated materials.

NICE Cybersecurity Workforce Framework (NCWF)

The seven categories and a description of the types of specialty areas included in each are below.

SECURELY PROVISION (SP) - Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems (i.e., responsible for some aspect of systems development).

OPERATE AND MAINTAIN (OM) - Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

OVERSEE AND GOVERN (OV) - Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

PROTECT AND DEFEND (PR) - Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.

ANALYZE (AN) - Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

COLLECT AND OPERATE (CO) - Specialty areas responsible for specialized denial and deception operations and collection of cybersecurity information that may be used to develop intelligence.

INVESTIGATE (IN) - Specialty areas responsible for investigation of cyber events and/or crimes of information technology (IT) systems, networks, and digital evidence.

EC-Council at a Glance

EC-Council Group is a multidisciplinary institution of global Information Security professional services.

EC-Council Group is a dedicated Information Security organization that aims at creating knowledge, facilitating innovation, executing research, implementing development, and nurturing subject matter experts in order to provide their unique skills and niche expertise in cybersecurity.

Some of the finest organizations around the world such as the US Army, US Navy, DoD, the FBI, Microsoft, IBM, and the United Nations have trusted EC-Council to develop and advance their security infrastructure.

ICECC
International Council of E-Commerce Consultants
EC-Council Group

ECC
EC-Council Training & Certification
Division of Professional Workforce Development

EGS
EC-Council Global Services
Division of Corporate Consulting & Advisory Services

ECCU
EC-Council University
Division of Academic Education

EGE
EC-Council Global Events
Division of Conferences, Forums, Summits, Workshops & Industry Awards

ECF
EC-Council Foundation
Non-Profit Organization for Cyber Security Awareness Increase.

15+	40+	145+	350+	700+	3000+
YEARS EXPERIENCE	TRAINING & CERTIFICATION PROGRAMS	COUNTRIES	SUBJECT MATTER EXPERTS	TRAINING PARTNERS WORLDWIDE	TOOLS & TECHNOLOGIES

220,000+ CERTIFIED MEMBERS

Your Learning Options

Instructor-led Training

EC-Council has a large network of Accredited Training Centers (ATC) spread across 145 countries. Each center has a certified trainer to deliver the entire EC-Council program from a training facility in your city.

Online Training

iLearn online training is a distance learning program designed for those who cannot attend a live course. The program is for the people who have a very busy schedule and want to learn at their own pace through self-study. This modality is also available from our enterprise teams.

Mobile Learning

Our world class content is also available on a mobile device, allowing our students to learn on the go. This program is designed for those who are cannot attend a live course, but are keen to improve their cyber security skills. This modality is also available from our enterprise teams.

Computer-based Training

For people who work in secure facilities with limited or no access to the internet, we offer computer-based training (CBT) options delivered in an HD DVD format. The DVDs are an upgrade/add-on to the base iLearn program and are not sold independently. This modality is also available from our enterprise teams.

Hands-on Experience with the EC-Council Cyber Range (iLabs)

EC-Council iLabs allows students to dynamically access a host of virtual machines preconfigured with vulnerabilities, exploits, tools, and scripts from anywhere. Our simplistic web portal enables the student to launch an entire range of target machines and access them remotely with one simple click. It is the most cost-effective, easy to use, live range lab solution available. *Most of our courses are equipped with iLabs, but iLabs can be purchased independently as well.*

Customized Learning

Love a course we offer, but want it customized? No problem! EC-Council has a dedicated team to cater to your needs. We have access to the largest pool of EC-Council certified instructors via our ATC channel. Let us know where and when you want the training delivered, and we will arrange for an instructor and all that's required for a course to be taught at a location of your choice. Contact our accredited training partners for a custom solution.

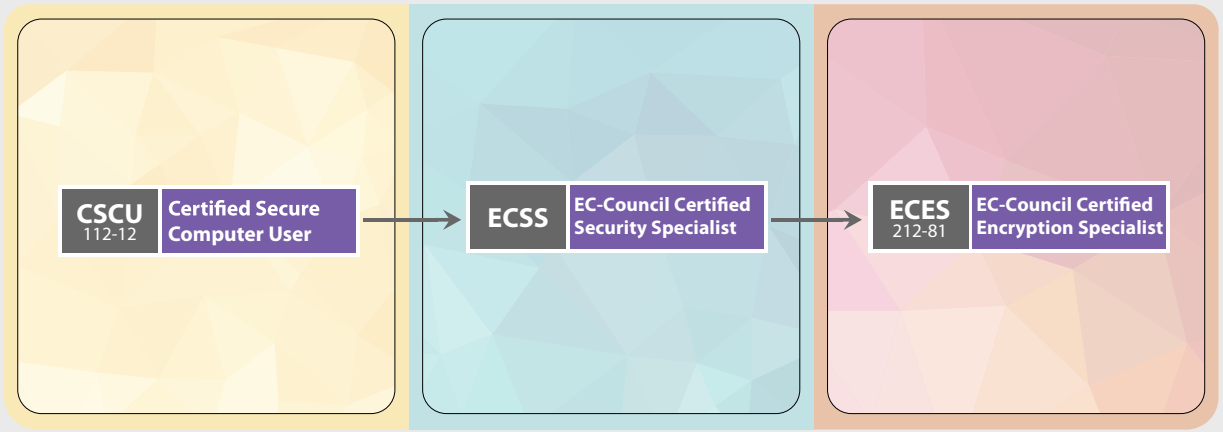
EC-Council client-site training includes official courseware, certification exam (ECC-Exam or VUE), iLabs, online labs (wherever available), and our test-pass guarantee.

Live Online Training

If self-study or self-paced learning does not fit into your personal learning style, we offer you our live online model, iWeek.

With iWeek, an instructor will teach you live online while you are seated in the comfort of your home. This training method gives you the freedom to get trained from a location of your choice. Individuals who choose this delivery method consistently attribute their choice to the preference of having a live instructor available for which questions can be asked and answered. We offer early-bird rates, group rates, and get even private courses delivered anytime.

Foundation Track



Target Audience

This track focuses on todays' computer users who use the internet extensively to work, study and play.

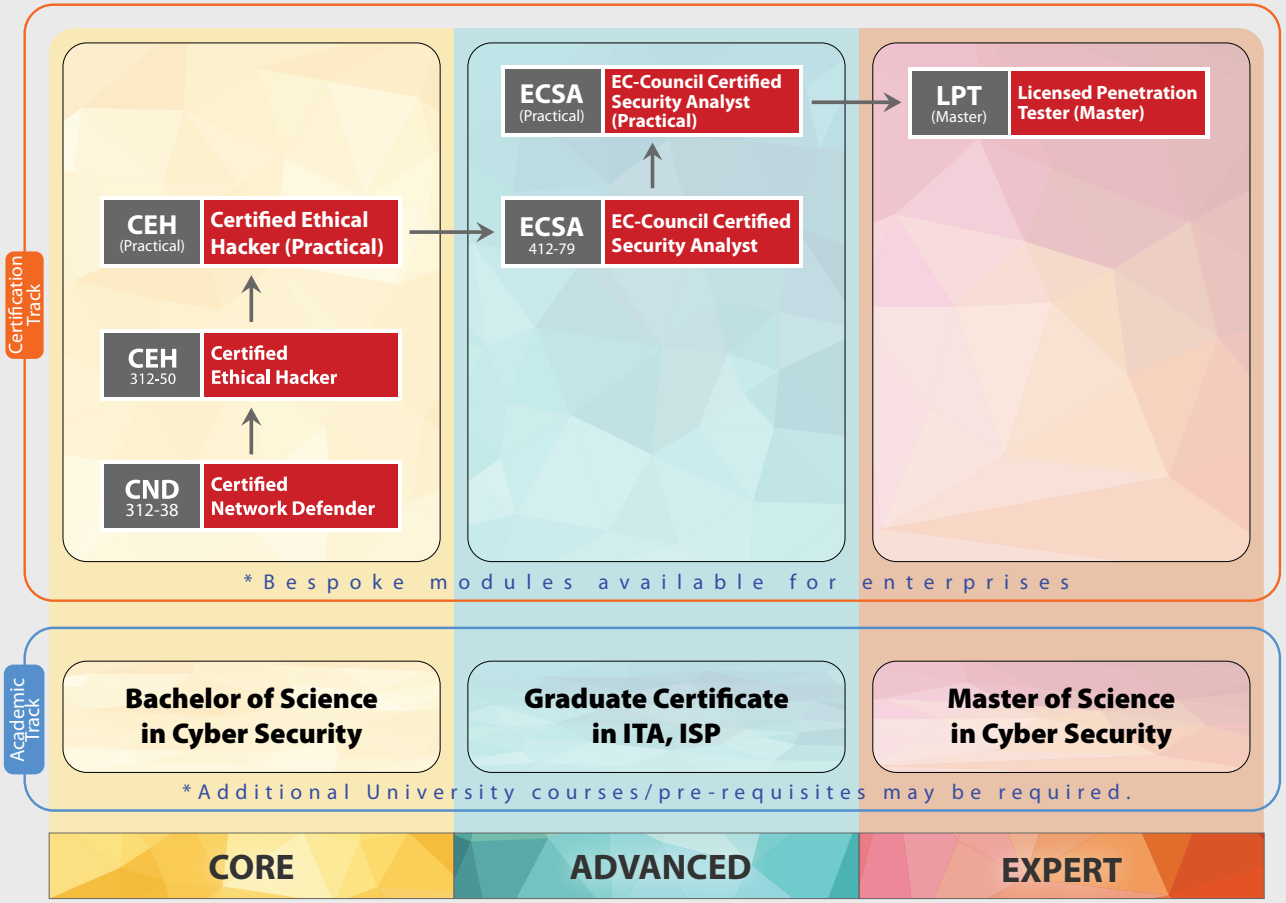
What will You Learn

- Cloud Security
- Password Security
- Social Engineering Countermeasures
- Mitigating Identity Theft
- Email Security
- Safe Browsing
- Data Protection
- Physical Security
- Mobile Device Security
- Encryption
- Social Network Security
- Antiviruses Protection
- Disaster Recovery
- Internet Security
- Credit Card Security
- Monitoring Kids Online
- Wireless & Home Network Security
- OS Security

Our Certified Foundation Professionals are Employed at:

Caritas, Grant Thornton, IBM, PALADION, Polytechnique, unique ACADEMY, Ministry of Defence, NTT DATA, CIT Group of Institutions, happiest minds, ingenia, icddr,b, Bank DCB Commercial Bank Plc, vodafone, UNP, RELIANCE, core4 factory, Nestlé, . . .

Vulnerability Assessment & Penetration Testing (VAPT)



Job Roles

- Information Assurance (IA) Security Officer
- Information Security Analyst/Administrator
- Information Security Manager/Specialist
- Information Systems Security Engineer/Manager
- Security Analyst
- Information Security Officers
- Information Security Auditors
- Risk/Vulnerability Analyst

Our Certified VAPT Professionals are Employed at:

Cisco, EY, Microsoft, Accenture, Infosys, Amazon, AIG, HP, Bank of America, Booz | Allen | Hamilton, Capgemini, Deloitte., NEC, bugcrowd, TATA, lastline, axiata, U.S. Army, Marriott, Hero

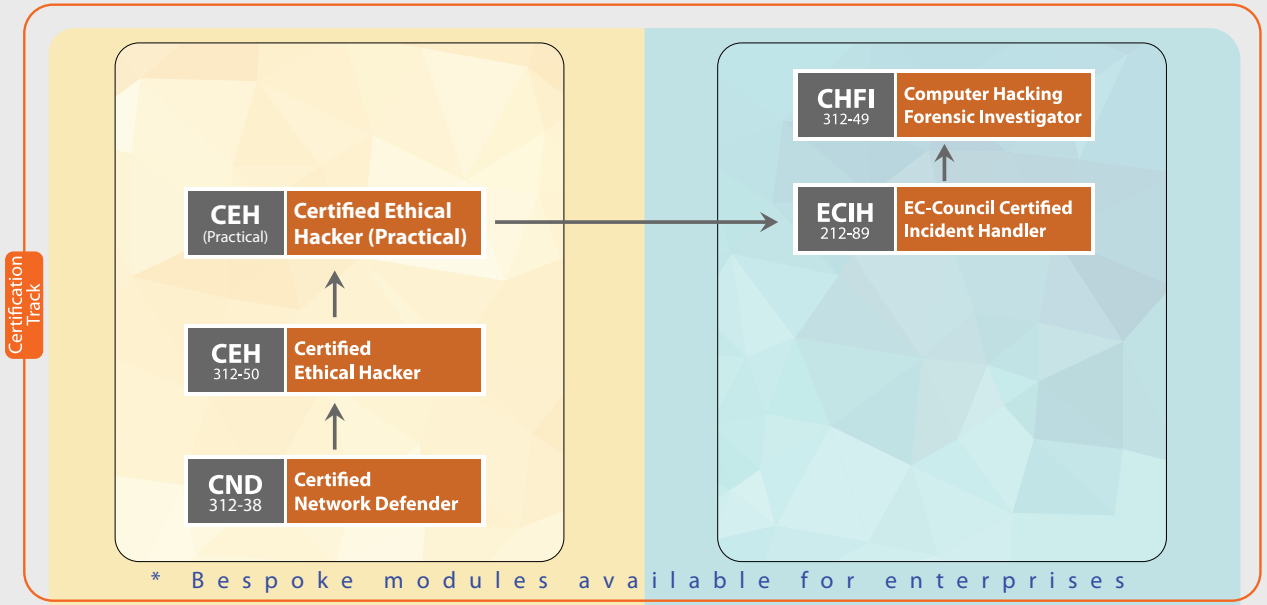
This track maps to NICE's Specialty Areas:

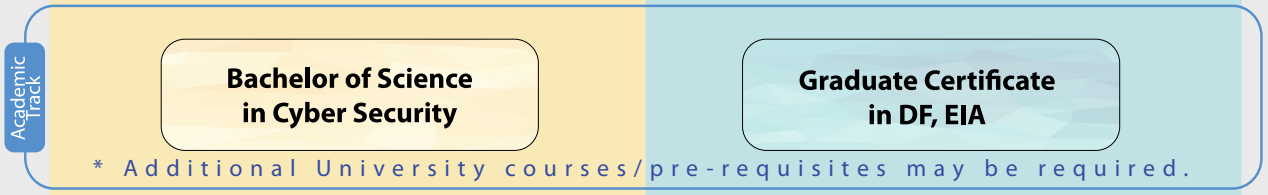
1. Protect and Defend (PR)
- a. Cybersecurity Defense Analysis (DA)
- b. Cybersecurity Defense Infrastructure Support (INF)
- c. Incident Response (IR)
- d. Vulnerability Assessment and Management (VA)

2. Securely Provision (SP)
- a. Test and Evaluation

3. Analyze (AN)
- a. Threat Analysis (TA)
- b. Exploitation Analysis (XA)

Cyber Forensics





CORE | ADVANCED

This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
a. Risk Management (RM)
b. Test and Evaluation
2. Operate and Maintain (OM)
a. Network Services (NET)
b. Systems Administration (SA)
c. Systems Analysis (AN)
3. Oversee and Govern (OV)
a. Cybersecurity Management (MG)
4. Protect and Defend (PR)
a. Cybersecurity Defense Analysis (DA)
b. Cybersecurity Defense Infrastructure Support (INF)
c. Incident Response (IR)
d. Vulnerability Assessment and Management (VA)
5. Analyze (AN)
a. Threat Analysis (TA)
b. Exploitation Analysis (XA)

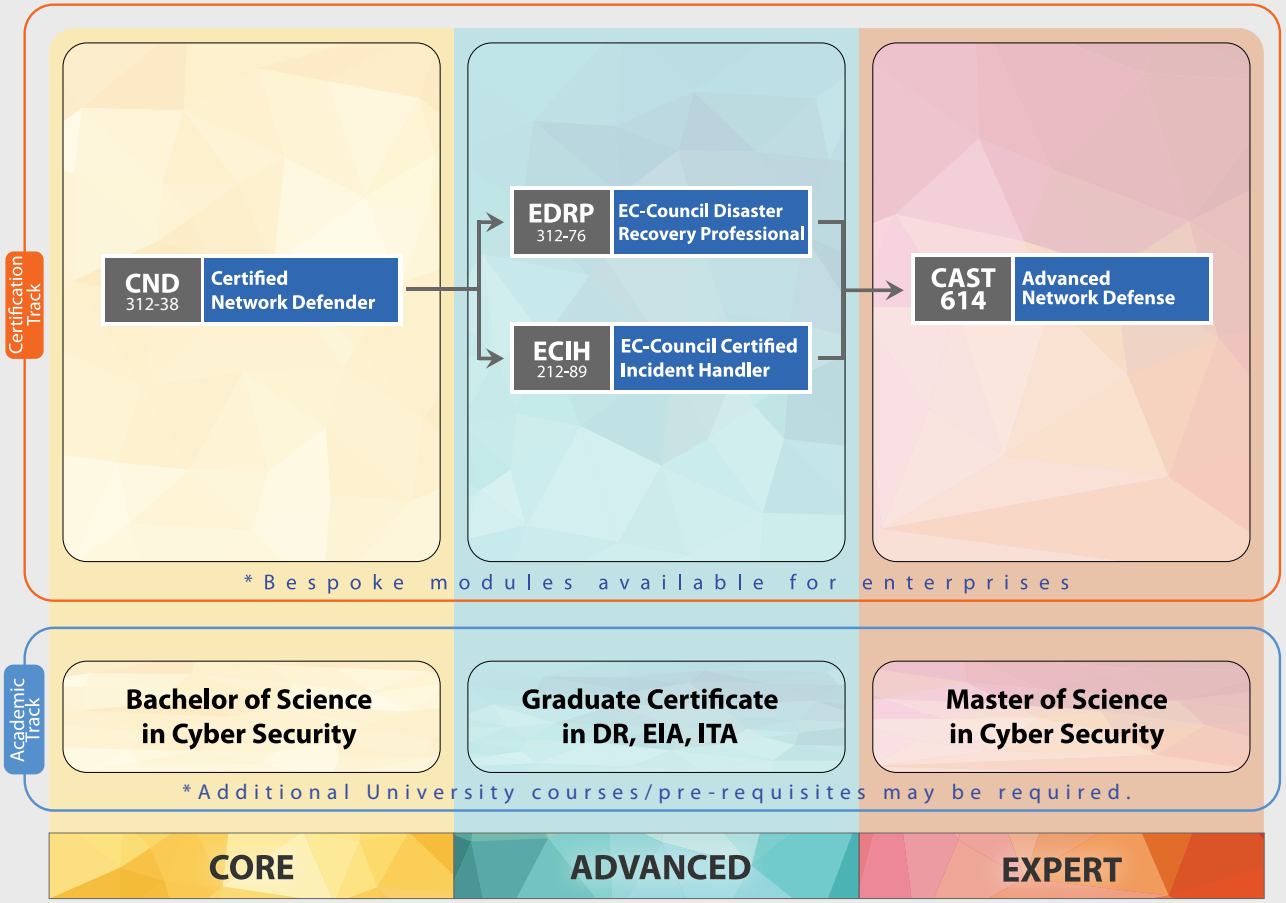
Job Roles

- Computer Forensic Analyst
- Computer Network Defense (CND)
- Forensic Analyst
- Digital Forensic Examiner

Our Certified Cyber Forensic Professionals are Employed at:

BARCLAYS, AIG, accenture, Infosys, U.S. ARMY, ICICI Bank, Bank of America, HDFC BANK, BMC SWITZERLAND, Telkom Indonesia, LEXINGTON MEDICAL CENTER, pwc, du, HSBC, WIPRO Applying Thought, ...

Network Defense and Operations



Job Roles

- Network Security Administrators
- Network Security Engineer/Specialist
- Network Defense Technicians
- Security Analyst
- Security Operator
- Computer Network Defense(CND) Analyst
- Cybersecurity Intelligence Analyst
- Enterprise Network Defense(END) Analyst

Our Certified Network Defense Professionals are Employed at:

FGB, IBM, KPMG, DISA, mitra solusi telematika, Ameriprise Financial, COMCAST, Florida State University, NCB الأهلي, IPDC Finance, Johnson Controls, sopra steria Consulting, Rockwell Automation, MAPFRE, • • •

This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
a. Risk Management (RM)
b. Test and Evaluation (TE)

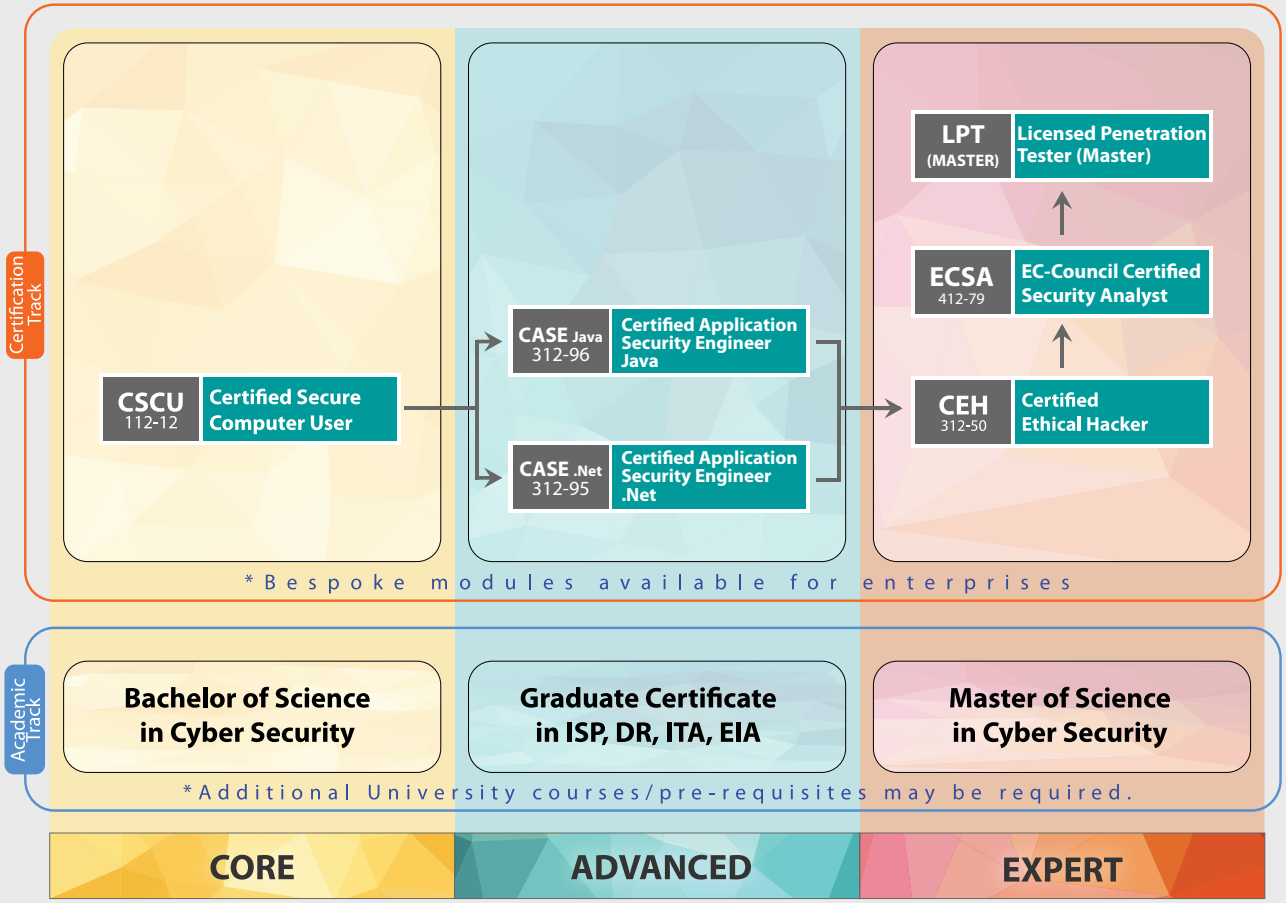
2. Operate and Maintain (OM)
a. Network Services (NET)
b. Systems Administration (SA)
c. Systems Analysis (AN)

3. Oversee and Govern (OV)
a. Cybersecurity Management (MG)

4. Protect and Defend (PR)
a. Cybersecurity Defense Analysis (DA)
b. Cybersecurity Defense Infrastructure Support (INF)
c. Incident Response (IR)
d. Vulnerability Assessment and Management (VA)

5. Analyze (AN)
a. Threat Analysis (TA)

Software Security



Job Roles

- Secure Software Engineer
- Security Engineer
- Software Developer
- Software Engineer/Architect
- Systems Analyst
- Web Application Developer
- Application Security Tester

Our Certified Software Security Professionals are Employed at:

WELLS FARGO, ITU, AIRBUS, TATA, axiata, BlueCross BlueShield, bol.com, alBaraka, Cognizant, Deloitte., EY Building a better working world, ecovadis, Infoblox CONTROL YOUR NETWORK, KASPERSKY, . . .

This Track Maps to NICE's Specialty Areas:

1. Securely Provision
a. Software Development (DEV)
b. Technology R&D (RD)

2. Operate and Maintain (OM)
a. Data Administration (DA)
b. Systems Analysis (AN)

3. Oversee and Govern (OV)
a. Cybersecurity Management (MG)

4. Protect and Defend (PR)
a. Cybersecurity Defense Analysis (DA)
b. Vulnerability Assessment

and Management (VA)

5. Analyze (AN)
a. Analyzes collected information to identify vulnerabilities and potential for exploitation.

Governance

Master of Science in Cyber Security

Graduate Certificate in:

- Information Security Professional
- Information Analyst
- Information Technology Analyst
- Disaster Recovery
- Digital Forensics

Job Roles

- Chief Information Security Officer (CISO)
- Chief Security Officer (CSO)
- Information Security (IS) Director
- Information Assurance (IA) Program Manager

Our Certified CCISO Professionals are Employed at:

marta, U.S. Army, Akamai, MUFG, Santander, BOFI Federal Bank, Chase, Chemical Bank, Generali, Government of South Australia, KPMG, Malwarebytes, Police Department, Arrow, Polycom, Rockwell Collins, Tadawul, The Bancorp, GE, HSBC, ICF, Juniper Networks, L'Oréal, Rabobank, vodafone, Telstra, ...

This Track Maps to NICE's Specialty Areas:

1. Securely Provision (SP)
- a. Risk Management (RM)
- b. Technology R&D (RD)
- c. Systems Requirements Planning (RP)

2. Oversee and Govern (OV)
- a. Legal Advice and Advocacy (LG)
- b. Training, Education, and Awareness (ED)
- c. Cybersecurity Management (MG)
- d. Strategic Planning and Policy (PL)
- e. Executive Cybersecurity Leadership (EX)
- f. Acquisition and Program/Project Management (PM)

3. Collect and Operate (CO)
- a. Cyber Operational Planning (PL)

Certified Secure Computer User (CSCU)

Course Description

CSCU provides individuals with the necessary knowledge and skills to protect their information assets.

This course covers fundamentals of various computer and network security threats such as identity theft, credit card fraud, phishing, virus and backdoors, emails hoaxes, loss of confidential information, hacking attacks, and social engineering.

Course Outline

1. Introduction to security
2. Securing operating systems
3. Malware and antivirus
4. Internet security
5. Security on social networking sites
6. Securing email communications
7. Securing mobile devices
8. Securing the cloud
9. Securing network connections
10. Data backup and disaster recovery

Key Outcomes

- Fundamentals of various computer and network security threats
- Understanding of identity theft, phishing scams, malware, social engineering, and financial frauds
- Learn to safeguard mobile, media and protect data
- Protecting computers, accounts, and social networking profiles as a user

Exam Information

- Exam name: CSCU (112-12) exam
- Number of questions: 50
- Passing score: 70%
- Test duration: 2 Hours
- Test format: Multiple choice
- Test delivery: EC-Council exam portal

Certified Network Defender (CND)

Course Description

CND is the world's most advanced network defense course with 14 of the most current network security domains any individuals will ever want to know when they are planning to protect, detect, and respond to the network attacks.

The course contains hands-on labs, based on major network security tools and techniques which will provide network administrators real world expertise on current network security technologies and operations.

Key Outcomes

- Knowledge on how to protect, detect, and respond to network attacks
- Network defense fundamentals
- Application of network security controls, protocols, perimeter appliances, secure IDS, VPN, and firewall configuration
- Intricacies of network traffic signature, analysis, and vulnerability scanning

Exam Information

- Exam title: CND
- Exam code: 312-38
- Number of questions: 100
- Duration: 4 hours
- Availability: ECC Exam
- Test format: Interactive Multiple Choice Questions

Course Outline

1. Computer network and defense fundamentals
2. Network security threats, vulnerabilities, and attacks
3. Network security controls, protocols, and devices
4. Network security policy design and implementation
5. Physical security
6. Host security
7. Secure firewall configuration and management
8. Secure IDS configuration and management
9. Secure VPN configuration and management
10. Wireless network defense
11. Network traffic monitoring and analysis
12. Network risk and vulnerability management
13. Data backup and recovery
14. Network incident response and management

CND Course Objecives

Module 01: Computer Network and Defense Fundamentals
1.1. Understand computer network fundamentals
1.2. Understand TCP/IP Networking
1.3. Describe TCP/IP Protocol Stack
1.4. Understand use of basic network administration utilities
1.5. Explain IP addressing concept
1.6. Understand Computer Network Defense(CND)
1.7. Describe CND layers
1.8. Describe CND process
Module 02: Network Security Threats, Vulnerabilities, and Attacks
2.1. Discuss network security concerns
2.2. Discuss network security vulnerabilities
2.3. Understand classification of network attacks
2.4. Discuss Network Reconnaissance Attacks
2.5. Discuss Network Access Attacks
2.6. Discuss Network DoS Attacks
2.7. Discuss Malware Attacks
Module 03: Network Security Controls, Protocols, and Devices
3.1. Understand fundamental elements of network security
3.2. Understand different types of network security controls
3.3. Explain network access control
3.4. Explain Identification, Authentication, Authorization and Accounting
3.5. Explain cryptography
3.6. Understand network security policy
3.7. Describe network security devices
3.8. Describe network security protocols
Module 04: Network Security Policy Design and Implementation
4.1. Understand security policy
4.2. Discuss the design and implementation of policy
4.3. Classification of security policies
4.4. Discuss the design of various security polices
4.5. Discuss about Security Policy Training and Awareness
4.6. Discuss various information security related standards, laws and acts
Module 05: Physical Security
5.1. Understand physical security
5.2. Describe types of physical security controls
5.3. Describe various physical security controls
5.4. Describe various access control authentication techniques
5.5. Understand workplace security
5.6. Understand personnel security
5.7. Describe environment controls
5.8. Physical security awareness and training
5.9. Discuss physical security checklist

CND Course Objecives

Module 06: Host Security
6.1. Understand host security
6.2. Understand OS security
6.3. Discuss Windows Security
6.4. Discuss Windows Patch Management
6.5. Discuss Windows log review and Audit
6.6. Discuss Linux security
6.7. Discuss Linux log review and audit
6.8. Discuss Servers security
6.9. Discuss router and switch security
6.10. Discuss Log review, audit, and management
6.11. Discuss application security
6.12. Discuss data security
6.13. Discuss virtualization security
Module 07: Secure Firewall Configuration and Management
7.1. Understand firewall security and their working
7.2. Understand firewalls security concerns
7.3. Describe types of firewalls
7.4. Describe various firewalls technologies
7.5. Explain different firewalls topologies and their appropriate selection
7.6. Discuss firewall rules and policies
7.7. Explain firewall implementation and deployment
7.8. Explain firewall administration
7.9. Discuss firewall logging and auditing
7.10. Discuss firewall anti-evasion techniques
7.11. Discuss Firewall Security Recommendations
7.12. Discuss firewall and firewall security auditing tools
Module 08: Secure IDS Configuration and Management
8.1. Understand intrusions
8.2. Describe Intrusion Detection and Prevention System(IDPS)
8.2. Explain Intrusion Detection System(IDS)
8.3. Explain IDS Implementation
8.4. Explain IDS deployment
8.5. Explain fine tuning of IDS alerts
8.6. Discuss IDS Recommendations
8.7. Explain Intrusion Prevention System(IPS)
8.8. Describe IDPS Product Selection Considerations
8.9. Explain technologies for complementing IDS functionality
8.10 Introduce various IDS/IPS Solutions and Vendors
Module 09: Secure VPN Configuration and Management
9.1. Understand Virtual Private Network (VPN)
9.2. Discuss various types of VPN
9.3. Discuss VPN Categories
9.4. Explain VPN Core Functions
9.5. Describe VPN technologies

CND Course Objecives

9.6. Explain various VPN topology
9.7. Discuss common threats and flaws in VPN implementation
9.8. Discuss security in VPN implementation
9.9. Discuss Quality of Service and Performance in VPNs
9.10. Discuss Auditing and Testing of VPN
9.11. Discuss VPN Security Recommendations
Module 10: Wireless Network Defense
10.1. Introduce various wireless terminologies
10.2. Introduce wireless networks
10.3. Discuss various wireless standards
10.4. Describe various wireless network topologies
10.5. Describe typical Use of Wireless Networks
10.6. Discuss various wireless network components
10.7. Discuss the use of various types of antenna
10.8. Explain Wireless Encryption technologies
10.9. Describe various methods for wireless authentication
10.10. Discuss various threats on wireless network
10.11. Implement security for wireless networks
10.12. Assess wireless network security
10.12. Discuss Wireless IDS/IPS deployment
10.13. Implement security on wireless routers
10.14 Discuss Wireless Network Security Guidelines

Module 11: Network Monitoring and Analysis
11.1. Introduction to network traffic monitoring and analysis
11.2. Discuss various techniques for network traffic monitoring and analysis
11.3. Describe position of machine for network monitoring
11.4. Understand network traffic signatures
11.5. Understand Wireshark components, working and features
11. 6. Demonstrate the use of various Wireshark filters
11.7. Demonstrate the monitoring LAN traffic against policy violation
11.8. Demonstrate the detection of various attacks using Wireshark
11.9. Discuss network bandwidth monitoring and performance improvement
Module 12: Network Risk and Vulnerability Management
12.1. Understand risk
12.2. Discuss Risk Management
12.3. Describe Risk Management phases
12.4. Discuss Enterprise Network Risk Management
12.5. Explain Vulnerability management and its phases
12.6. Demonstrate Vulnerability Assessment/scanning
Module 13: Data Backup and Recovery
13.1. Introduction to Data Backup
13.2. Explain RAID backup technology
13.3. Explain SAN backup technology
13.3. Explain NAS backup technology

13.4. Explain NAS backup technology
13.5. Describe various backup methods
13.6. Describe various locations for backup
13.7. Demonstrate various types of backup
13.8. Describe various backup solutions
13.9. Discuss the need of recovery drill test
13.10. Demonstrate data recovery
Module 14: Network Incident Response and Management
14.1. Understand Incident Handling and Response (IH&R)
14.2. Describe role of first responder in incident response
14.3. Describe Incident Handling and Response (IH&R) process
14.4. Overview of forensic investigation

Certified Ethical Hacker (CEH)

Course Description

CEH is the world's most advanced certified ethical hacking course with 18 of the most current security domains any individual will ever want to know when they are planning to beef-up the information security posture of their organization.

The accredited course provides the advanced hacking tools and techniques used by hackers and information security professionals.

Key Outcomes

- Thorough introduction to ethical hacking
- Exposure to threat vectors and counter measures
- Addresses emerging areas of cloud and mobile hacking
- Prepares you to combat Trojans, malware, backdoors and more
- Enables you to hack using mobile

Exam Information

- Number of questions: 125
- Test duration: 4 Hours
- Test format: Multiple choice
- Test delivery: ECC Exam, VUE
- Exam prefix: 312-50 (ECC Exam), 312-50 (VUE)

Course Outline

1. Introduction to ethical hacking
2. Footprinting and reconnaissance
3. Scanning networks
4. Enumeration
5. Vulnerability analysis
6. System hacking
7. Malware threats
8. Sniffing
9. Social engineering
10. Denial of service
11. Session hijacking
12. Evading IDS, Firewalls, and Honeypot
13. Hacking web servers
14. Hacking web applications
15. SQL injection
16. Hacking wireless networks
17. Hacking mobile platforms
18. IoT Hacking
19. Cloud computing
20. Cryptography

CEH Course Objecives

Module 01: Introduction to Ethical Hacking
1.1. Overview of Information Security
1.2. UnderstandingInformation Security Threats and Attack Vectors
1.3. Overview of Hacking Concepts, Types, and Phases
1.4. Understanding Ethical Hacking Concepts and Scope
1.5. Overview of Information Security Controls
1.6. Overview of Penetration Testing
1.7. Overview of Information Security Laws and Standards
Module 02: Footprinting and Reconnaissance
2.1. Understanding Footprinting Concepts
2.2. Footprinting through Search Engines
2.3. Footprinting through Web Services
2.4. Footprinting through Social Networking Sites
2.5. Understanding Different Techniques for Website Footprinting
2.6. Understanding Different Techniques for Email Footprinting
2.7. Understanding Different Techniques for Competitive Intelli-gence
2.8. Understanding Different Techniques for Whois Footprinting
2.9. Understanding Different Techniques for DNS Footprinting
2.10. Understanding Different Techniques for Network Footprinting
2.11. Footprinting through Social Engineering
2.12. Footprinting Tools
2.13. Footprinting Countermeasures
2.14. Overview of Footprinting Penetration Testing
Module 03: Scanning Networks
3.1. Overview of Network Scanning
3.2. Scanning Tools
3.3. Understanding Various Scanning Techniques
3.4. Understanding Various Techniques for Scanning Beyond IDS and Firewall
3.5. Understanding Banner Grabbing
3.6. Draw Network Diagrams
3.7. Overview of Scanning Penetration Testing
Module 04: Enumeration
4.1. Understanding Enumeration
4.2. Understanding Different Techniques for NetBIOS Enumeration
4.3. Understanding Different Techniques for SNMP Enumeration
4.4. Understanding Different Techniques for LDAP Enumeration
4.5. Understanding Different Techniques for NTP Enumeration
4.6. Understanding Different Techniques for SMTP and DNS Enumeration
4.7. Understanding IPsec, VoIP, RPC, and Linux Enumeration
4.8. Enumeration Countermeasures
4.9. Overview of Enumeration Penetration Testing

CEH Course Objecives

Module 05: Vulnerability Analysis
5.1. Understanding Vulnerability Assessment Concepts
5.2. Vulnerability Assessment Solutions
5.3. UnderstandingVulnerability Scoring Systems
5.4. Vulnerability Assessment Tools
5.5. UnderstandingVulnerability Assessment Reports
Module 06: System Hacking
6.1. Understanding System Hacking Concepts
6.2. Understanding Different Password Cracking Techniques to Gain Access to the System
6.3. Understanding Privilege Escalation Techniques
6.4. Understanding Techniques to Create and Maintain Remote Access to the System
6.5. Understanding Techniques to Hide Malicious Programs
6.6. Understanding Techniques to Hide the Evidence of Compromise
6.7. Overview of System Hacking Penetration Testing
Module 07: Malware Threats
7.1. Introduction to Malware and Malware Propagation Techniques
7.2. Overview of Trojans, Their Types, and How They Infect Systems
7.3. Overview of Viruses and Worm, Their Types, and How They Infect Files
7.4. Understanding Malware Analysis Process
7.5. Malware Countermeasures
7.6. Anti-Malware Software
7.7. Overview of Malware Penetration Testing
Module 08: Sniffing
8.1. Overview of Sniffing Concepts
8.2. Understanding MAC Attacks
8.3. Understanding DHCP Attacks
8.4. Understanding ARP Poisoning
8.5. Understanding MAC Spoofing Attacks
8.6. Understanding DNS Poisoning
8.7. Sniffing Tools
8.8. Sniffing Countermeasures
8.9. Understanding Various Techniques to Detect Sniff-ing
8.10. Overview of Sniffing Penetration Testing
Module 09: Social Engineering
9.1. Overview of Social Engineering Concepts
9.2. Understanding Various Social Engineering Techniques
9.3. Understanding Insider Threats
9.4. Understanding Impersonation on Social Networking Sites

CEH Course Objecives

9.5.Understanding Identity Theft
9.6.Social Engineering, Insider Threats, and Identity Theft Countermea-sures
9.7. Overview of Social Engineering Penetration Testing
Module 10: Denial-of-Service
10.1. Understanding DoS/DDoS Concepts
10.2.Understanding Different DoS/DDoS Attack Techniques
10.3.Understanding the Botnet Network
10.4. Overview of DDoS Case Study
10.5.Understanding Various DoS/DDoS Attack Tools
10.6.Understanding Different Techniques to Detect DoS/DDoS Attacks
10.7.DoS/DDoS Protection Tools
10.8.Overview of DoS Attack Penetration Testing
Module 11: Session Hijacking
11.1.Understanding Session Hijacking Concepts
11.2.Understanding Application Level Session Hijack-ing
11.3.Understanding Network Level Session Hijacking
11.4. Session Hijacking Tools
11.5. Session Hijacking Countermeasures
11.6.Overview of Session Hijacking Penetration Testing

Module 12: Evading IDS, Firewalls, and Honeypots
12.1.Understanding IDS, Firewall, and Honeypot Concepts
12.2. IDS, Firewall and Honeypot Solutions
12.3.Understanding Different Techniques to Bypass IDS
12.4.Understanding Different Techniques to Bypass Firewalls
12.5. IDS/Firewall Evading Tools
12.6.Understanding Different Techniques to Detect Honey-pots
12.7. IDS/Firewall Evasion Countermeasures
12.8.Overview of IDS and Firewall Penetration Testing
Module 13: Hacking Webservers
13.1.Understanding Web Server Concepts
13.2.Understanding Web Server Attacks
13.3.Understanding Web Server Attack Methodolo-gy
13.4. Web Server Attack Tools
13.5. Web Server Attack Countermeasures
13.6.Overview of Patch Management
13.7. Web Server Security Tools
13.8.Overview of Web Server Penetration Testing
Module 14: Hacking Web Applications
14.1.Understanding Web Application Concepts

14.2. Understanding Web Application Threats
14.3. Understanding Web Application Hacking Methodolo-gy
14.4. Web Application Hacking Tools
14.5. Web Application Countermeasures
14.6. Web Application Security Testing Tools
14.7. Overview of Web Application Penetration Testing
Module 15: SQL Injection
15.1. Understanding SQL Injection Concepts
15.2. Understanding Various Types of SQL Injection At-tacks
15.3. Understanding SQL Injection Methodology
15.4. SQL Injection Tools
15.5. Understanding Different IDS Evasion Techniques
15.6. SQL Injection Countermeasures
Module 16: Hacking Wireless Networks
16.1. Understanding Wireless Concepts
16.2. Understanding Different Wireless Encryption Algo-rithms
16.3. Understanding Wireless Threats
16.4. Understanding Wireless Hacking Methodology
16.5. Wireless Hacking Tools
16.6. Understanding Bluetooth Hacking Techniques
16.7. Wireless Hacking Countermeasures
16.8. Wireless Security Tools
16.9. Overview of Wireless Penetration Testing
Module 17: Hacking Mobile Platforms
17.1. Understanding Mobile Platform Attack Vectors
17.2. Understanding Various Android OS Threats and Attacks
17.3. Understanding Various iOS Threats and Attacks
17.4. Overview of Mobile Spyware
17.5. Understanding Mobile Device Management (MDM)
17.6. Mobile Security Guidelines and Tools
17.7. Overview of Mobile Penetration Testing
Module 18: IoT Hacking
18.1. Understanding IoT Concepts
18.2. Understanding IoT Attacks
18.3. Understanding IoT Hacking Methodolo-gy
18.4. IoT Hacking Tools
18.5. IoT Countermeasures
18.6. Overview of IoT Penetration Testing
Module 19: Cloud Computing
19.1. Understanding Cloud Computing Con-cepts

19.2. Understanding Cloud Computing Threats
19.3. Understanding Cloud Computing Attacks
19.4. Overview of Cloud Security
19.5. Cloud Computing Security Tools
19.6. Overview of Cloud Penetration Testing
Module 20: Cryptography
20.1. Understanding Cryptography Concepts
20.2. Overview of Encryption Algorithms
20.3. Cryptography Tools
20.4. Understanding Public Key Infrastructure (PKI)
20.5. Understanding Email Encryption
20.6. Understanding Disk Encryption
20.7. Understanding Cryptanalysis
20.8. Cryptographic Attacks Countermeasures

Certified Ethical Hacker (Practical)

Course Description

C|EH Practical is a six-hour, rigorous exam that requires you to demonstrate the application of ethical hacking techniques such as threat vector identification, network scanning, OS detection, vulnerability analysis, system hacking, web app hacking, etc. to solve a security audit challenge.

This is the next step after you have attained the highly acclaimed Certified Ethical Hacker certification.

Key Outcomes

- Mastery of Ethical Hacking skills.
- Demonstrate the application of the knowledge to find solutions to real-life challenges.
- Commitment to code of ethics.
- Validate essential skills required in the ethical hacking domains.

Exam Information

- Number of Practical Challenges: 20
- Duration: 6 hours
- Availability: Aspen – iLabs
- Test Format: iLabs Cyber Range
- Passing Score: 70%

Course Outline

- Demonstrate the understanding of attack vectors
- Perform network scanning to identify live and vulnerable machines in a network.
- Perform OS banner grabbing, service, and user enumeration.
- Perform system hacking, steganography, steganalysis attacks, and cover tracks.
- Identify and use viruses, computer worms, and malware to exploit systems.
- Perform packet sniffing.
- Conduct a variety of web server and web application attacks including directory traversal, parameter tampering, XSS, etc.
- Perform SQL injection attacks.
- Perform different types of cryptography attacks.
- Perform vulnerability analysis to identify security loopholes in the target organization's network, communication infrastructure, and end systems etc.

EC-Council Certified Security Analyst (ECSA)

ECSA™
EC-Council Certified Security Analyst

Course Description

ECSA is a globally accepted hacking and penetration testing program that covers the testing of modern infrastructures, operating systems, and application environments while teaching the students how to document and write a penetration testing report.

This program takes the tools and techniques covered in CEH to next level by utilizing EC-Council's published penetration testing methodology.

Key Outcomes

- Introduce to security analysis and penetration testing methodologies
- In-depth vulnerability analysis, network penetration testing from external and internal evading firewalls and ids
- Learn to own web applications and databases, and take over cloud services
- Analyze security of mobile devices and wireless networks
- Present findings in a structured actionable report

Exam Information

- Credit towards certification: ECSAv10
- Number of questions: 150
- Passing score: 70%
- Test duration: 4 hours

Course Outline

0. Penetration Testing Essential Concepts
1. Introduction to Penetration Testing and Methodologies
2. Penetration Testing Scoping and Engagement Methodology
3. Open-Source Intelligence (OSINT) Methodology
4. Social Engineering Penetration Testing Methodology
5. Network Penetration Testing Methodology – External
6. Network Penetration Testing Methodology – Internal
7. Network Penetration Testing Methodology – Perimeter Devices
8. Web Application Penetration Testing Methodology
9. Database Penetration Testing Methodology
10. Wireless Penetration Testing Methodology
11. Cloud Penetration Testing Methodology
12. Report Writing and Post Testing Actions

ECSA™

EC-Council Certified Security Analyst

ECSA Course Objecives

Module 01: Security Analysis and Penetration Testing Methodologies
1.1. Overview of Penetration Testing
1.2. Understanding Benefits of Conducting a Penetration Test
1.3. Understanding the Difference between Penetration Testing and Ethical Hacking
1.4. Understanding the Difference between Security Audit, Vulnerability Assessment, and Penetration Testing
1.5. Understanding Different Penetration Testing Types
1.6. Understanding Common Areas of Penetration Testing
1.7. Understanding Penetration Testing Process
1.8. Understanding Penetration Testing Phases
1.9. Understanding Penetration Testing Methodologies
1.10. Overview to LPT Penetration Testing Methodology
1.11. Understanding Ethics of Penetration Tester
Module 02: Penetration Testing Scoping and Engagement Methodology
2.1. Collecting the Penetration Testing Requirements from the Client
2.2. Preparing Response Requirements for Proposal Submission
2.3. Drafting Timeline and Quote for Penetration Testing
2.4. Starting Penetration Testing Engagement
2.5. Creating Rules of Engagement (ROE)
2.6. Identifying the Resources Required for the Penetration
2.7. Drafting a Penetration Testing Contracts
2.8. Creating a Pen Testing Agreement with the Client
2.9. Preparing Penetration Testing Team
2.10. Preparing a Penetrating Testing Test Plan
2.11. Obtaining Permissions for Penetration Testing
Module 03: Open Source Intelligence (OSINT) Methodology
3.1. Performing OSINT through World Wide Web (WWW)
3.2. Information Gathering through Advanced Google Hacking
3.3. Identifying the Key Email Addresses through Email
3.4. Performing OSINT through Website Analysis
3.5. Performing OSINT through DNS Interrogation
Module 04: Social Engineering Penetration Testing Methodology
4.1. Overview to Social Engineering Penetration Testing
4.2. Understanding the Skills Required to Perform Social Engineering Pen Test
4.3. Understanding the Common Targets of Social Engineering Pen Test
4.4. Performing Social Engineering Pen Testing using E-mail Attack Vector
4.5. Performing Social Engineering Pen Testing using Telephone Attack Vector
4.6. Performing Social Engineering Pen Testing using Physical Attack Vector
Module 05: Network Penetration Testing Methodology-External
5.1. Overview of External Penetration Testing
5.2. Performing Port Scanning on Target
5.3. Perform OS and Service Fingerprinting on Target
5.4. Conducting Vulnerability Research

ECSA™
EC-Council Certified Security Analyst

ECSA Course Objecives

5.5. Searching and Mapping the Target with the Associated Security Vulnerabilities
5.6. Finding out The Security Vulnerability Exploits
5.7. Performing Exploit Verification
Module 06: Network Penetration Testing Methodology-Internal
6.1. Overview of Internal Penetration Testing
6.2. Performing Footprinting on Internal Network
6.3. Performing Network Scanning on Internal Network
6.4. Performing OS and Service Fingerprinting on Internal Network
6.5. Applying Various Enumeration Techniques on Internal Network
6.6. Performing Vulnerability Assessment/ Scanning
6.7. Mapping the OS, Service, device with The Associated Security Vulnerabilities
6.8. Performing Windows Exploitation
6.9. Performing Unix/Linux Exploitation
6.10. Testing Interwork Network against Various Types of Attacks
6.11. Performing Post Exploitation activities
Module 07: Network Penetration Testing Methodology-Perimeter Devices
7.1. Performing Port Scanning and Locating Firewall
7.2. Performing Banner Grabbing
7.3. Enumerating Firewall Access Control List
7.4. Performing vulnerability Scanning
7.5. Attempting to Bypass Firewall using various Techniques/methods/attacks

7.6. Understanding the need of IDS Penetration Testing
7.7. Testing IDS using various Attacks
7.8. Overview to Router and Switches Penetration Testing
7.9. Testing for Router Misconfigurations Vulnerabilities
7.10. Testing for Switches Misconfigurations Vulnerabilities
Module 08: Web Application Penetration Testing Methodology
8.1. Overview of Web Application Penetration Testing
8.2. Discovering Web Application Default Content
8.3. Discovering Web Application Hidden Content
8.4. Performing Web Vulnerability Scanning
8.5. Identifying the Attack Surface Area
8.6. Testing for SQL Injection Vulnerabilities
8.7. Testing for XSS Vulnerabilities
8.8. Testing Security Misconfiguration Vulnerabilities
8.9. Testing for Broken the Authentication and Authorization Vulnerabilities
8.10. Testing Broken Session Management Vulnerabilities
8.11. Testing for Web Services Vulnerabilities
8.12. Testing for Business Logic Flaws
8.13. Testing for Web Server Vulnerabilities
8.14. Tests for Thick Clients Vulnerabilities
Module 09: Database Penetration Testing Methodology
9.1. Performing Database Information Reconnaissance

ECSA™
EC-Council Certified Security Analyst

ECSA Course Objecives

9.2. Performing Oracle Database Enumeration
9.3. Performing MS SQL Server Database Enumeration
9.4. Performing MySQL Database Enumeration
9.5. Database Vulnerability and Exploit Research
9.6. Performing Oracle Database Exploitation
9.7. Performing MS SQL Server Database Exploitation
9.8. Performing MySQL Database Exploitation
Module 10: Wireless Penetration Testing Methodology
10.1. Overview of Wireless Penetration Testing
10.2. Overview to Wireless Local Area Network (WLAN) Penetration Testing
10.3. Testing for Wireless Local Area Network (WLAN) Vulnerabilities
10.4. Overview to RFID Penetration Testing
10.5. Testing for RFID Penetration Vulnerabilities
10.6. Overview to NFC Penetration Testing
10.7. Testing for NFC Penetration Vulnerabilities
10.8. Overview to Mobile Device Penetration Testing
10.9. Testing for Mobile Device and Application Vulnerabilities
10.10. Overview to IoT Penetration Testing
Module 11: Cloud Penetration Testing Methodology
11.1. Understanding Cloud Computing Security and Concerns
11.2. Understanding Security Risks Involved in Cloud Computing
11.3. Understanding Role of Penetration Testing in Cloud Computing

11.4. Understanding the Scope of Cloud Pen Testing
11.5. Understanding Cloud Penetration Testing Limitations
11.6. Overview of Cloud Penetration Testing
11.7. Performing Cloud Reconnaissance
11.8. Understanding Provision of Penetration Testing for Different CSP
11.9. Obtaining Authorization for Penetration Testing from the CSP
11.10. Testing cloud for Cloud Specific Vulnerabilities
Module 12: Report Writing and Post Test Actions
12.1. Overview of Penetration Testing Deliverables
12.2. Understanding the Process of Writing Penetration Testing Report
12.3. Overview of Pen Testing Report Format
12.4. Understanding Penetration Testing Report Analysis
12.5. Understanding Post Testing Actions
12.6. Overview of Report Retention

EC-Council Certified Security Analyst (Practical)

Course Description

ECSA (Practical) is a 12-hour, rigorous practical exam built to test your penetration testing skills.

The candidates are required to demonstrate the application of the penetration testing methodology that is presented in the ECSA program, and are required to perform a comprehensive security audit of an organization, just like in the real world. You will start with challenges requiring you to perform advanced network scans beyond perimeter defenses, leading to automated and manual vulnerability analysis, exploit selection, customization, launch, and post exploitation maneuvers.

Key Outcomes

- Test your ability to perform threat and exploit research, understand exploits in the wild, write your own exploits, customize payloads, and make critical decisions
- Create a professional pen testing report with essential elements

Exam Information

- Number of challenges: 8
- Duration: 12 hours
- Availability: Aspen- iLabs
- Test Format: iLabs cyber range
- Passing Score: 5 out of 8 challenges and submission of an acceptable penetration testing report

Course Outline

- Perform advanced network scans beyond perimeter defenses, leading to automated and manual vulnerability analysis, exploit selection, customization, launch and post exploitation maneuvers.
- Customize payloads
- Make critical decisions at different phases of a pen-testing engagement
- Perform advanced network scans beyond perimeter defenses
- Perform automated and manual vulnerability analysis
- Customization, launch, and post exploitation maneuvers
- Perform a full fledged Penetration Testing engagement
- Create a professional pen-testing report
- Demonstrate the application of penetration testing methodology presented in the ECSA program

APT

Advanced Penetration Testing

Course Description

In the Advanced Penetration Testing Course, you are presented with minimal network information along with a Scope of Work (SOW). The course was created to provide you with advanced concepts that will help when it comes to attempting the LPT (Master) Certification exam.

The last module of the course includes an SOW for each of the various networks we have created for the course. This, combined with the composition of various ranges, mimics a professional penetration test. Time is limited and you will be required to identify the attack surface followed by the weaknesses of the machines that are on the network.

Key Outcomes

- Introduces a comprehensive process for a security test, producing findings and report for an enterprise class setting
- Complemented with Cyber Ranges that progresses in difficulty and reflect an enterprise level architecture, with defenses to defeat and challenges to overcome
- Exposure to evasion techniques

Exam Information

- Based on practical results
- 60 questions
- 75 minutes
- Open book, note and access to range is allowed during the test
- 70% minimum required to pass

Course Outline

1. Introduction to Vulnerability Assessment and Penetration Testing
2. Information Gathering Methodology
3. Scanning and Enumeration
4. Identify Vulnerabilities
5. Exploitation
6. Post Exploitation
7. Advanced Tips and Techniques
8. Preparing a Report
9. Practice Ranges

EC-Council Licensed Penetration Tester (LPT) - Master

Course Description

LPT (Master) credential is developed in collaboration with SMEs and practitioners around the world after a thorough job role, job task, and skills-gap analysis.

The LPT (Master) practical exam is the capstone to EC-Council's entire information security track, right from the CEH to the ECSA Program. The LPT (Master) exam covers the skill-sets, technical analysis and report writing, required to be a true professional penetration tester.

Key Outcomes

- Mastery of penetration testing skills
- Ability to perform repeatable methodology
- Commitment to code of ethics
- Ability to present analysed results through structured reports

Exam Information

- Live Online
- Fully Proctored
- 3 Levels
- 9 Challenges
- 18 Hours

Testimonials

"Converting fear into confidence with LPT(Master)"

by Adithya Naresh

"Proud to attain the LPT(Master) credential"

by Ali Isikli

"LPT(Master): Extremely challenging and one of the toughest exams"

by Mark Horvat

"Real-life penetration testing with LPT(Master)"

by Moustafa Mohamed Mohsen

EC-Council Certified Incident Handler (ECIH)

Course Description

ECIH program is designed to provide the fundamental skills to handle and respond to the computer security incidents in an information system. The course addresses various underlying principles and techniques for detecting and responding to current and emerging computer security threats.

The comprehensive training program will make students proficient in handling as well as responding to various security incidents such as network security incidents, malicious code incidents, and insider attack threats.

Key Outcomes

- Principals, processes and techniques for detecting and responding to security threats/breaches
- Liaison with legal and regulatory bodies
- Learn to handle incidents and conduct assessments
- Cover various incidents like malicious code, network attacks, and insider attacks

Exam Information

- Credit towards certification: ECIH 212-89
- Number of questions: 50
- Passing score: 70%
- Test duration: 2 hours
- Test format: Multiple choice
- Test delivery: ECC exam, VUE

Course Outline

1. Introduction to incident response and handling
2. Risk assessment
3. Incident response and handling steps
4. CSIRT
5. Handling network security incidents
6. Handling malicious code incidents
7. Handling insider threats
8. Forensic analysis and incident response
9. Incident reporting
10. Incident recovery
11. Security policies and laws

ECIH Course Objecives

Module 01: Introduction to Incident Response and Handling
1.1. Define computer security incident
1.2. Discuss the importance of data classification
1.3. Discuss information warfare
1.4. Discuss the key concepts of information security
1.5. Explain various vulnerability, threat, and attacks on information systems
1.6. Discuss types of computer security incidents with example
1.7. Explain different incident categories
1.8. Discuss incident prioritization issues
1.9. Explain incident response, incident handling and computer forensics
Module 02: Risk Assessment
2.1. Explain risk policy
2.2. Discuss the risk assessment methodology
2.3. Outline different steps to assess and mitigate risks at work place
2.4. Describe risk analysis
2.5. Discuss different risk mitigation strategies
2.6. Explain the importance of cost/benefit analysis in risk assessment process
2.7. Discuss various issues involved with control implementation
2.8. Explain the risk mitigation methodology
2.9. Discuss residual risk
2.10. List and explain various tools that may help in risk assessment

Module 03: Incident Response and Handling Steps
3.1. Explain the need for incident response
3.2. Describe the incident response process
3.3. Explain the incident response components
3.4. Describe incident response methodology
3.5. Explain various incident response and handling stages
3.6. Define the incident response plan
3.7. Outline the steps for incident response plan
3.8. Discuss the importance of training and awareness for incident response and handling
3.9. Provide security awareness and training checklists
3.10. Explain incident response policy
3.11. Discuss about incident management and the purpose of incident management
3.12. Explain about incident response team structure, personnel, team dependencies and team services
3.13. Define the relationship between incident response, incident handling, and incident management
3.14. Discuss about incident response best practices
Module 04: CSIRT
4.1. Discuss the need of an Incident Response Team (IRT)
4.2. Explain CSIRT goals and strategies
4.3. Explain CSIRT mission and vision
4.4. Explain CSIRT constituency

ECIH Course Objecives

4.5. Discuss about the CSIRT place in the organization
4.6. Explain the CSIRT relationship with peers
4.7. Define the types of CSIRT environments
4.8. Explain the best practices for creating a CSIRT
4.9. Explain the role of CSIRTs
4.10. Define the roles in an Incident Response Team
4.11. Illustrate different CSIRT services
4.12. Explain about CSIRT policies and procedures
4.13. Explain how CSIRT handles a case
Module 05: Handling Network Security Incidents
5.1. Define DoS and DDoS attacks
5.2. Explain incident handling preparation for DoS attacks
5.3. Discuss different types of unauthorized access incidents
5.4. Explain various stages involved in incident handling preparation for an unauthorized access incident
5.5. Discuss different types of inappropriate usage incidents
5.6. Explain different steps of incident handling preparation for inappropriate usage incidents
5.7. Discuss about the multiple component incidents
5.8. Explain steps involved in incident handling preparation for multiple component incidents
5.9. Discuss various network security assessment tools

Module 06: Handling Malicious Code Incidents
6.1. Explain about virus, worms, Trojans and spywares
6.2. Explain the incident handling preparation for malicious code incidents
6.3. Discuss about the incident prevention, detection and analysis of malicious code incidents
6.4. Explain the containment strategy for the t malicious code incidents
6.5. Explain the method of evidence gathering and handling the malicious code incidents
6.6. Define the method of eradication and recovery from the malicious code incidents
6.7. Explain various countermeasures for the malicious code incidents
Module 07: Handling Insider Threats
7.1. Define insider threats
7.2. Explain the anatomy of an insider attack
7.3. Explain different techniques for the insider threat detection
7.4. Explain the insider threats response
7.5. Describe the insider's threat incident response plan
7.6. Provide guidelines for overcoming insider threats
7.7. Demonstrate the use of various employee monitoring tools
Module 08: Forensic Analysis and Incident Response
8.1. Discuss computer forensics
8.2. Explain the objectives of forensics analysis

8.3. Discuss about the role of forensics analysis in incident response
8.4. Explain the types of computer forensics
8.5. Discuss about computer forensic investigator and other people involved in computer forensics
8.6. Define the computer forensics process
8.7. Explain about the forensic policies
8.8. Discuss about the forensics in the information system life cycle
8.9. Demonstrate various forensics analysis tools
Module 09: Incident Reporting
9.1. Define the incident reporting
9.2. Outline the details to be reported
9.3. Provide report formats
9.4. Discuss the information disclosure issues
9.5. Explain the issues involved in reporting work place incidents
9.6. Discuss about the federal agency's incident categories
9.7. Provide the incident reporting guidelines
Module 10: Incident Recovery
10.1. Define the incident recovery process
10.2. Explain the principles of incident recovery
10.3. List and explain the steps in incident recovery
10.4. Discuss about contingency/continuity of operations planning
10.5. Discuss about contingency/continuity of operations planning
10.6. Discuss about business continuity planning and business impact analysis
10.7. Describe the incident recovery plan
10.8. Discuss about the incident recovery planning team
10.9. Define the incident recovery testing
Module 11: Security Policies and Laws
11.1. Define the security policy
11.2. Explain the key elements of security policy
11.3. Describe the goals of a security policy
11.4. Explain the purpose of a security policy
11.5. Explain the characteristics of a security policy
11.6. Discuss about the implementation of security policies
11.7. Explain the access control policy and its importance
11.8. List and explain the various security policies
11.9. Provide the physical security guidelines
11.10. Discuss about the personnel security policies & guidance
11.11. Explain the role of laws in incident handling
11.12. Discuss about the legal issues when dealing with an incident
11.13. Discuss about the law enforcement agencies

Computer Hacking and Forensic Investigator (CHFI)

Course Description

CHFI is a comprehensive course covering major forensic investigation scenarios, enabling students to acquire hands-on experience.

The program provides a strong baseline knowledge of key concepts and practices in the digital forensic domains relevant to today's organizations. Moreover, CHFI provides firm grasp on the domains of digital forensics.

Key Outcomes

- Comprehensive forensics investigation process
- Forensics of file systems, operating systems, network and database, websites, and email systems
- Techniques for investigating on cloud, malware, and mobile
- Data acquisition and analysis as well as anti-forensic techniques
- Thorough understanding of chain of custody, forensic report, and presentation

Exam Information

- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 hours
- Test Format: Multiple choice
- Test Delivery: ECC Exam portal

Course Outline

1. Computer forensics in today's world
2. Computer forensics investigation process
3. Understanding hard disks and file systems
4. Defeating anti-forensics techniques
5. Operating system forensics
6. Network forensics
7. Investigating web attacks
8. Database forensics
9. Cloud forensics
10. Malware forensics
11. Investigating email crimes
12. Mobile forensics
13. Forensics report writing and presentation
14. Data Acquisition and Duplication

CHFI Course Objecives

Module 01: Computer Forensics in Today's World
1.1. Define computer forensics and understand its objectives
1.2. Understand and classify different types of cybercrimes
1.3. Understand different challenges cybercrimes present to investigators
1.4. Understand different types of cybercrime investigations and general rules of forensics
1.5. Understand Rules of Evidence and different types of digital evidence
1.6. Examine the role of computer forensics and forensics readiness in incident response plans
1.7. Understand need for forensic investigators and identify their roles and responsibilities
1.8. Review legal, privacy and code of ethics issues in computer forensics
Module 02: Computer Forensics Investigation Process
2.1. Understand the importance of computer forensics process
2.2. Describe the various phases of the computer forensics investigation process
2.3. Identify the requirements for building a computer forensics lab and an investigation team
2.4. Understand the roles of a First Responder
2.5. Perform search and seizure, evidence collection, management and preservation
2.6. Understand chain of custody and its importance
2.7. Discuss about data duplication, deleted data recovery and evidence examination
2.8. Write an investigative report and testify in a court room

Module 03: Understanding Hard Disks and File Systems
3.1. Describe the different types of disk drives and their characteristics
3.2. Understand the physical and logical structure of a hard disk
3.3. Identify the types of hard disk interfaces and discuss the various hard disk components
3.4. Describe hard disk partitions
3.5. Summarize Windows, Mac, and Linux boot Processes
3.6. Understand various Windows, Linux and Mac OS X file systems
3.7. Differentiate between various RAID storage systems
3.8. Demonstrate file system analysis
Module 04: Data Acquisition and Duplication
4.1. Understand data acquisition and its importance
4.2. Understand live data acquisition
4.3. Understand static data acquisition
4.4. Review data acquisition and duplication steps
4.5. Choose the steps required to keep the device unaltered
4.6. Determine the best acquisition method and select appropriate data acquisition tool
4.7. Perform the data acquisition on Windows and Linux Machines
4.8. Summarize data acquisition best practices

CHFI Course Objecives

Module 05: Defeating Anti-forensics Techniques
5.1. Define anti-forensics and list the goals of anti-forensics
5.2. Review anti-forensics techniques
5.3. Extract evidence from deleted files/partitions, password protected files, and stego material
5.4. Identify trial obfuscation, artifact wiping, data/metadata overwriting, and encryption
5.5. Identify encrypted network protocols, program packers, rootkits and detection methods
5.6. Examine different techniques attackers use to avoid detection during investigation
5.7. Interpret anti-forensics countermeasures
5.8. Understand challenges faced by Investigators to defeat anti-forensics
Module 06: Operating System Forensics (Windows, Mac, Linux)
6.1. Understand how to collect and examine volatile and non-volatile data in Windows machines
6.2. Perform windows memory and registry analysis
6.3. Examine the cache, cookie, and history recorded in web browsers
6.4. Examine Windows files and metadata
6.5. Analyze text based logs and Windows event logs
6.6. List various Linux based shell commands and log files
6.7. Collect and examine volatile and non-volatile information in Linux machines
6.8. Explain the need for Mac forensics and examine Mac forensics data and log files

Module 07: Network Forensics
7.1. Understand the importance of network forensics
7.2. Discuss the fundamental logging concepts
7.3. Summarize the event correlation concepts
7.4. Understand network forensic readiness and list the network forensics steps
7.5. Examine the Router, Firewall, IDS, DHCP and ODBC logs
7.6. Examine the network traffic
7.7. Document the evidence gathered on a network
7.8. Perform evidence reconstruction for investigation
Module 08: Investigating Web Attacks
8.1. Understand the importance of web application forensics
8.2. Illustrate the web application architecture and list the challenges in web application forensics
8.3. Indicate web attacks and define all the web application threats
8.4. Interpret the steps to investigate web attacks
8.5. Perform web attacks investigation on Windows-based servers
8.6. Describe IIS web server architecture and perform IIS logs investigation
8.7. Describe Apache web server architecture and perform Apache logs investigation
8.8. Investigate various attacks on web applications

CHFI Course Objecives

Module 09: Database Forensics
9.1. Understand database forensics and its importance
9.2. Perform MSSQL forensics
9.3. Determine the database evidence repositories and collect the evidence files
9.4. Examine evidence files using SQL Server Management Studio and ApexSQL DBA
9.5. Perform MySQL forensics
9.6. Understand architecture of MySQL and determine the structure of data directory
9.7. List MySQL utilities for performing forensic analysis
9.8. Perform MySQL forensics on WordPress web application database

Module 10: Cloud Forensics
10.1. Summarize cloud computing concepts
10.2. List all the cloud computing attacks
10.3. Understand the importance of cloud forensics
10.4. Interpret the usage of cloud forensics
10.5. Distinguish between the various types of cloud forensics
10.6. Understand the roles of stake holders in cloud forensics
10.7. Interpret the challenges faced by investigators while performing cloud forensics
10.8. Investigate the cloud storage services Dropbox and Google Drive

Module 11: Malware Forensics
11.1. Define a malware and list the different ways a malware can get into a system
11.2. Discuss techniques attackers use to spread malware, and list the basic malware components
11.3. Apply malware forensics concepts, identify and extract malware from live and dead systems
11.4. Understand the prominence of setting up a controlled malware analysis lab
11.5. Prepare Testbed for malware analysis
11.6. Identify the general rules to perform malware analysis
11.7. Perform Static and Dynamic malware analysis and analyze malicious documents
11.8. Understand the challenges faced while performing malware analysis

Module 12: Investigating Email Crimes
12.1. Understand Email System, Clients and Servers, and their characteristics
12.2. Understand the importance of electronic records management
12.3. List the email crimes and discuss the crimes committed via chat room
12.4. Describe the components of an Email message
12.5. List Common Headers and X-Headers
12.6. Review the steps to investigate email crimes and violations
12.7. List all the email forensics tools
12.8. Discuss about the U.S. Law against email crime: CAN-SPAM act and its characteristics

CHFI Course Objecives

Module 13: Mobile Phone Forensics
13.1. Discuss about mobile device forensics and understand why it is needed
13.2. Understand the role of mobile hardware and OS while conducting forensics on mobiles
13.3. Illustrate the architectural layers of mobile device environment
13.4. Illustrate Android architecture stack and demonstrate Android boot process
13.5. Illustrate iOS architecture stack and demonstrate iOS boot process
13.6. Determine the mobile storage and evidence locations
13.7. Understand what you should do before performing investigation
13.8. Perform mobile forensics
Module 14: Forensics Report Writing and Presentation
14.1. Understand the importance of forensic investigation reports
14.2. Understand the important aspects of a good report
14.3. Summarize the contents of a forensics investigation report template
14.4. Classify the investigation reports and review the guidelines for writing a report
14.5. Define an expert witness and describe the roles of an expert witness
14.6. Differentiate Technical Witness Vs. Expert Witness
14.7. Understand Daubert and Fyre Standards
14.8. Describe how to testify in a court and discuss the general ethics while testifying

Certified Application Security Engineer (CASE) .Net

Course Description

CASE professionals take software development up a notch by introducing security requirements across all stages of the software development life cycle (SDLC), as well as, secure coding practices, secure requirement gathering, robust application design, and handling security issues in both pre and post development phases of application development.

The hands-on training program is one of the most comprehensive certifications for secure software development in the market today. It's desired by software application engineers, analysts, testers globally, and respected by hiring authorities.

Key Outcomes

- Ensure that application security is no longer an afterthought but a foremost one.
- It lays the foundation required by all application developers and development organizations, to produce secure applications with greater stability and fewer security risks to the consumer.
- Ensure that organizations mitigate the risk of losing millions due to security compromises that may arise with every step of application development process.

Exam Information

- Number of questions: 50
- Passing score: 70%
- Test duration: 2 Hours
- Test format: Multiple choice
- Test delivery: EC-Council Exam center
- Exam prefix: 312-95

Course Outline

1. Understanding Application Security, Threats, and Attacks
2. Security Requirements Gathering
3. Secure Application Design and Architecture
4. Secure Coding Practices for Input Validation
5. Secure Coding Practices for Authentication and Authorization
6. Secure Coding Practices for Cryptography
7. Secure Coding Practices for Session Management
8. Secure Coding Practices for Error Handling
9. Static and Dynamic Application Security Testing (SAST & DAST)
10. Secure Deployment and Maintenance

CASE .Net Course Objecives

Module 01: Understanding Application Security, Threats, and Attacks
1.1. Understand the Need and Benefits of Application Security
1.2. Discuss the Most Common Application-level Attacks
1.3. Discuss the Common Reasons Behind the Existence of Application-level Vulnerabilities
1.4. Understand Various Components of Comprehensive Application Security
1.5. Understand the Need and Advantages of Integrating Security in SDLC
1.6. Differentiate Functional Vs Security Activities in SDLC
1.7. Discuss Microsoft Security Development Lifecycle (SDL)
1.8. Discuss Various Software Security Reference Standards, Models, and Frameworks
Module 02: Security Requirements Gathering
2.1. Understand the Importance of Gathering Security Requirements
2.2. Understand Security Requirement Engineering (SRE) and its Phases
2.3. Describe Abuse Cases and Abuse Case Modeling
2.4. Describe Security Use Cases and Security Use Case Modeling
2.5. Describe Abuser and Security Stories
2.6. Explain Security Quality Requirements Engineering (SQUARE) Model
2.7. Explain OCTAVE Model
Module 03: Secure Application Design and Architecture
3.1. Understand the Importance of Secure Application Design
3.2. Discuss Various Secure Design Principles
3.3. Understand Threat Modeling
3.4. Describe Threat Modeling Process
3.5. Discuss STRIDE and DREAD Model
3.6. Describe Secure Application Architecture Design
Module 04: Secure Coding Practices for Input Validation
4.1. Understand the Importance of Robust Input Validation
4.2. Discuss Secure Input Validation Techniques in Web Forms, ASP.NET Core, and MVC
4.3. Learn Defensive Coding Techniques against SQL Injection Attacks
4.4. Learn Defensive Coding Techniques against XSS Attacks
4.5. Learn Defensive Coding Techniques against Parameter Tampering Attacks
4.6. Learn Defensive Coding Techniques against Directory Traversing Attacks
4.7. Learn Defensive Coding Techniques against Open Redirect Vulnerabilities
Module 05: Secure Coding Practices for Authentication and Authorization
5.1. Understand Authentication and Authorization
5.2. Explain Authentication and Authorization in Web Forms
5.3. Explain Authentication and Authorization in ASP.NET Core
5.4. Explain Authentication and Authorization in MVC
5.5. Learn Authentication and Authorization Defensive Techniques in Web Forms
5.6. Learn Authentication and Authorization Defensive Techniques in ASP.NET Core
5.7. Learn Authentication and Authorization Defensive Techniques in MVC

CASE .Net Course Objecives

Module 06: Secure Coding Practices for Cryptography
6.1. Understand Cryptography in .NET
6.2. Explain Symmetric Encryption
6.3. Learn Defensive Coding Practices using Symmetric Encryption
6.4. Explain Asymmetric Encryption
6.5. Learn Defensive Coding Practices using Asymmetric Encryption
6.6. Explain Hashing
6.7. Explain Digital Signatures
6.8. Explain Digital Certificates
6.9. Learn ASP.NET Core Specific Secure Cryptography Practices
Module 07: Secure Coding Practices for Session Management
7.1. Understand Session Management Concepts
7.2. Discuss Various Session Management Techniques
7.3. Learn Defensive Coding Practices against Session Hijacking Attacks
7.4. Learn Defensive Coding Practices against Session Replay and Session Fixation Attacks
7.5. Learn How to Prevent Sessions from Cross-site Scripting, Client-side Scripts, and CSRF Attacks
7.6. Learn How to Prevent Session Attacks on ViewState
7.7. Learn ASP.NET Core Specific Secure Session Management Techniques
Module 08: Secure Coding Practices for Error Handling
8.1. Introduction to Error and Exception Handling
8.2. Discuss the Need of Secure Exception Handling
8.3. Learn Defensive Coding Practices against Information Disclosure
8.4. Learn Defensive Coding Practices against Improper Error Handling
8.5. Learn Secure Error Handling Practices in ASP.NET Core
8.6. Learn Secure Auditing and Logging Best Practices
Module 09 Static and Dynamic Application Security Testing (SAST & DAST)
9.1. Introduction to Static Application Security Testing (SAST)
9.2. Discuss Manual Secure Code Review Techniques for Most Common Vulnerabilities
9.3. Introduction to Dynamic Application Security Testing
9.4. Discuss DAST using Automated Application Vulnerability Scanning Tools
9.5. Discuss DAST using Proxy-based Security Testing Tools
Module 10: Secure Deployment and Maintenance
10.1. Understand the Importance of Secure Deployment
10.2. Discuss Security Practices at Host Level
10.3. Discuss Security Practices at Network Level
10.4. Discuss Security Practices at Application Level
10.5. Discuss Security Practices at IIS level
10.6. Discuss Security Practices at .NET Level
10.7. Discuss Security Practices at SQL Server Level
10.8. Discuss Securit y Maintenance and Monitoring Activities

Certified Application Security Engineer (CASE) Java

Course Description

The CASE Java is designed to be a hands-on, comprehensive application security training course that trains software developers on the critical security skills and knowledge required throughout a typical software development life cycle (SDLC), focusing on the importance of the implementation of secure methodologies and practices required in today's insecure operating environment.

CASE professionals can get the better of security challenges across all phases of SDLC to rise above the title of an ordinary developer. CASE professionals often become Project Managers, utilizing their learning in the SSDLC, making them unique and valuable resources.

Key Outcomes

- Testing and credentialing secure application development across all phases of the SDLC
- CASE Program maps to many Specialty Areas under Securely Provision category in the NICE 2.0 Framework
- Covers techniques such as Input Validation, Authentications and Authorizations, Cryptography, Error Handling, and Session Management techniques, among many others

Exam Information

- Number of questions: 50
- Passing score: 70%
- Test duration: 2 Hours
- Test format: Multiple choice
- Test delivery: EC-Council Exam center
- Exam prefix: 312-96

Course Outline

1. Understanding Application Security, Threats, and Attacks
2. Security Requirements Gathering
3. Secure Application Design and Architecture
4. Secure Coding Practices for Input Validation
5. Secure Coding Practices for Authentication and Authorization
6. Secure Coding Practices for Cryptography
7. Secure Coding Practices for Session Management
8. Secure Coding Practices for Error Handling
9. Static and Dynamic Application Security Testing (SAST & DAST)
10. Secure Deployment and Maintenance

CASE Java Course Objecives

Module 01: Understanding Application Security, Threats, and Attacks
1.1. Understand the Need and Benefits of Application Security
1.2. Discuss the Most Common Application-level Attacks
1.3. Discuss the Common Reasons Behind the Existence of Application-level Vulnerabilities
1.4. Understand Various Components of Comprehensive Application Security
1.5. Understand the Need and Advantages of Integrating Security in SDLC
1.6. Differentiate Functional Vs Security Activities in SDLC
1.7. Discuss Software Security Reference Standards, Models, and Frameworks
Module 02: Security Requirements Gathering
2.1. Understand the Importance of Gathering Security Requirements
2.2. Understand Security Requirement Engineering (SRE) and its Phases
2.3. Describe Abuse Cases and Abuse Case Modeling
2.4. Describe Security Use Cases and Security Use Case Modeling
2.5. Describe Abuser and Security Stories
2.6. Explain Security Quality Requirements Engineering (SQUARE) Model
2.7. Explain(OCTAVE Model
Module 03: Secure Application Design and Architecture
3.1. Understand the Importance of Secure Application Design
3.2. Discuss Various Secure Design Principles
3.3. Understand Threat Modeling
3.4. Describe Threat Modeling Process
3.5. Discuss STRIDE and DREAD Model
3.6. Describe Secure Application Architecture Design
Module 04: Secure Coding Practices for Input Validation
4.1. Understand the Need of Input Validation
4.2. Discuss Data Validation Techniques
4.3. Discuss Data Validation in Strut Framework
4.4. Discuss Data Validation in Spring Framework
4.5. Discuss Common Input Validation Errors
4.6. Learn Common Secure Coding Practices for Input Validation
Module 05: Secure Coding Practices for Authentication and Authorization
5.1. Understand Authentication Concepts
5.2. Discuss Authentication Implementation in Java
5.3. Discuss Authentication Weaknesses and Prevention
5.4. Understand Authorization Concepts
5.5. Discuss Access Control Model
5.6. Discuss EJB Authorization
5.7. Discuss Java Authentication and Authorization (JAAS)
5.8. Discuss Authorization Common Mistakes and Countermeasures
5.9. Discuss Java EE Security
5.10. Discuss Authentication and Authorization in Spring Security Framework
5.11. Learn Defensive Coding Practices for Broken Authentication and Authorization

CASE Java Course Objecives

Module 06: Secure Coding Practices for Cryptography
6.1. Understand Fundamental Concepts and Need of Cryptography in Java
6.2. Discuss Encryption and Secret Keys
6.3. Discuss Implementation of Cipher Class
6.4. Discuss Implementation of Digital Signatures
6.5. Discuss Implementation of Secure Socket Layer (SSL)
6.6. Discuss Secure Key Management
6.7. Discuss Implementation of Digital Certificates
6.8. Discuss Implementation of Hashing
6.9. Explain Java Card Cryptography
6.10. Explain Crypto Module in Spring Security
6.11. Learn Dos and Don'ts in Java Cryptography
Module 07: Secure Coding Practices for Session Management
7.1. Introduction to Session Management in Java
7.2. Discuss Session Management in Spring Framework
7.3. Discuss Session Vulnerabilities and their Mitigation Techniques
7.4. Best Practices and Guidelines for Secure Session Management
Module 08: Secure Coding Practices for Error Handling
8.1. Introduction to Exception and Error Handling in Java
8.2. Discuss Erroneous Exceptional Behaviors
8.3. Learn Dos and Don'ts in Error Handling
8.4. Discuss Spring MVC Error Handling

8.5. Discuss Exception Handling in Struts2
8.6. Learn Best Practices for Error Handling
8.7. Introduction to Logging in Java
8.8. Discuss Logging using Log4j
8.9. Learn Coding Techniques in Secure Logging
8.10. Learn Best Practices for Logging
Module 09 Static and Dynamic Application Security Testing (SAST & DAST)
9.1. Introduction to Static Application Security Testing (SAST)
9.2. Discuss Manual Secure Code Review Techniques for Most Common Vulnerabilities
9.3. Introduction to Dynamic Application Security Testing
9.4. Discuss DAST using Automated Application Vulnerability Scanning Tools
9.5. Discuss DAST using Proxy-based Security Testing Tools
Module 10: Secure Deployment and Maintenance
10.1. Understand the Importance of Secure Deployment
10.2. Discuss Security Practices at Host Level
10.3. Discuss Security Practices at Network Level
10.4. Discuss Security Practices at Application Level
10.5. Discuss Security Practices at Web Container Level (Tomcat)
10.6. Discuss Security Practices at Oracle Database Level
10.7. Discuss Security Maintenance and Monitoring Activities

Certified Chief Information Security Officer (C|CISO)

Course Description

C|CISO certification is an industry-leading program that recognizes the real-world experience necessary to succeed at the highest executive levels of information security. Bringing together all the components required for a C-Level positions, the C|CISO program combines audit management, governance, IS controls, human capital management, strategic program development, and the financial expertise vital for leading a highly successful IS program.

The C|CISO Training Program can be the key to a successful transition to the highest ranks of information security management.

Course Outline

1. Governance
2. Security risk management, controls, and audit management
3. Security program management and operations
4. Information security core concepts
5. Strategic planning, finance, and vendor management

Key Outcomes

- Establishes the role of CISO and models for governance
- Core concepts of information security controls, risk management, and compliance
- Builds foundation for leadership through strategic planning, program management, and vendor management

Exam Information

- Exam Format : Multiple Choice
- Total number of questions : 150
- Exam duration : 2.5 Hours
- Required passing score : 72%

CCISO Course Objecives

Domain 1: Governance (Policy, Legal, & Compliance) & Risk Management
1.1. Define, implement, manage and maintain an information security governance program that includes leadership, organizational structures and processes.
1.2. Align information security governance framework with organizational goals and governance, i.e., leadership style, philosophy, values, standards and policies.
1.3. Establish information security management structure.
1.4. Establish a framework for information security governance monitoring (considering cost/benefits analyses of controls and ROI).
1.5. Understand standards, procedures, directives, policies, regulations, and legal issues that affect the information security program.
1.6. Understand the enterprise information security compliance program and manage the compliance team.
1.7. Analyze all the external laws, regulations, standards, and best practices applicable to the organization.
1.8. Understand the various provisions of the laws that affect the organizational security such as Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act, Health Insurance Portability and Accountability Act [HIPAA], Federal Information Security
1.9. Management Act [FISMA], Clinger-Cohen Act, Privacy Act, Sarbanes-Oxley, etc.
1.10. Be familiar with the different standards such as ISO 27000 series, Federal Information Processing Standards [FIPS]
1.11. Understand the federal and organization specific published documents to manage operations in a computing environment
1.12. Assess the major enterprise risk factors for compliance
1.13. Coordinate the application of information security strategies, plans, policies, and procedures to reduce regulatory risk
1.14. Understand the importance of regulatory information security organizations and appropriate industry groups, forums, and stakeholders
1.15. Understand the information security changes, trends, and best practices
1.16. Manage enterprise compliance program controls
1.17. Understand the information security compliance process and procedures
1.18. Compile, analyze, and report compliance programs
1.19. Understand the compliance auditing and certification programs
1.20. Follow organizational ethics
Domain 2: IS Management Controls and Auditing Management
2.1. Information Security Management Controls
2.1.1. Identify the organization's operational process and objectives as well as risk tolerance level
2.1.2. Design information systems controls in alignment with the operational needs and goals and conduct testing prior to implementation to ensure e effectiveness and efficiency
2.1.3. Identify and select the resources required to effectively implement and maintain information systems controls. Such resources can include human capital, information, infrastructure, and architecture (e.g., platforms, operating systems, networks, databases, applications)

CCISO Course Objecives

2.1.4. Design and implement information systems controls to mitigate risk. Monitor and document the information systems control performance in meeting organizational objectives by identifying and measuring metrics and key performance indicators
2.1.5. Design and conduct testing of information security controls to ensure effectiveness, discover de¬ficiencies and ensure alignment with organization's policies, standards and procedures
2.1.6. Design and implement processes to appropriately remediate de¬ficiencies and evaluate problem management practices to ensure that errors are recorded, analyzed and resolved in a timely manner
2.1.7. Assess and implement tools and techniques to automate information systems control processes.
2.1.8. Produce information systems control status reports to ensure that the processes for information systems operations, maintenance and support meet the organization's strategies and objectives, and share with relevant stakeholders to support executive decision-making
2.2. Auditing Management
2.2.1. Understand the IT audit process and be familiar with IT audit standards
2.2.2. Apply information systems audit principles, skills and techniques in reviewing and testing information systems technology and applications to design and implement a thorough risk-based IT audit strategy
2.2.3. Execute the audit process in accordance with established standards and interpret results against defined criteria to ensure that the information systems are protected, controlled and effective in supporting organization's objectives
2.2.4. Effectively evaluate audit results, weighing the relevancy, accuracy, and perspective of conclusions against the accumulated audit evidence
2.2.5. Assess the exposures resulting from ineffective or missing control practices and formulate a practical and cost-effective plan to improve those areas
2.2.6. Develop an IT audit documentation process and share reports with relevant stakeholders as the basis for decision-making
2.2.7. Ensure that the necessary changes based on the audit findings are effectively implemented in a timely manner
Domain 3: Management – Projects and Operations (Projects, Technology & Operations)
3.1. For each information systems project develop a clear project scope statement in alignment with organizational objectives
3.2. Define activities needed to successfully execute the information systems program, estimate activity duration, and develop a schedule and staffing plan
3.3. Develop, manage and monitor the information systems program budget, estimate and control costs of individual projects
3.4. Identify, negotiate, acquire and manage the resources needed for successful design and implementation of the information systems program (e.g., people, infrastructure, and architecture)
3.5. Acquire, develop and manage information security project team
3.6. Assign clear information security personnel job functions and provide continuous training to ensure effective performance and accountability
3.7. Direct information security personnel and establish communications, and team activities, between the information systems team and other security-related personnel (e.g., technical support, incident management, security engineering)

CCISO Course Objecives

3.8. Resolve personnel and teamwork issues within time, cost, and quality constraints
3.9. Identify, negotiate and manage vendor agreement and community
3.10. Participate with vendors and stakeholders to review/assess recommended solutions; identify incompatibilities, challenges, or issues with proposed solutions
3.11. Evaluate the project management practices and controls to determine whether business requirements are achieved in a cost-effective manner while managing risks to the organization
3.12. Develop a plan to continuously measure the effectiveness of the information systems projects to ensure optimal system performance
3.13. Identify stakeholders, manage stakeholders' expectations and communicate effectively to report progress and performance
3.14. Ensure that necessary changes and improvements to the information systems processes are implemented as required
Domain 4: Information Security Core Competencies
4.1. Access Control
4.1.1. Identify the criteria for mandatory and discretionary access control, understand the different factors that help in implementation of access controls and design an access control plan
4.1.2. Implement and manage an access control plan in alignment with the basic principles that govern the access control systems such as need-to-know
4.1.3. Identify different access control systems such as ID cards and biometrics
4.1.4. Understand the importance of warning banners for implementing access rules
4.1.5. Develop procedures to ensure system users are aware of their IA responsibilities before granting access to the information systems
4.2. Social Engineering, Phishing Attacks, Identity Theft
4.2.1. Understand various social engineering concepts and their role in insider attacks and develop best practices to counter social engineering attacks
4.2.2. Design a response plan to identity theft incidences
4.2.3. Identify and design a plan to overcome phishing attacks
4.3. Physical Security
4.3.1. Identify standards, procedures, directives, policies, regulations and laws for physical security
4.3.2. Determine the value of physical assets and the impact if unavailable
4.3.3. Identify resources needed to effectively implement a physical security plan
4.3.4. Design, implement and manage a coherent, coordinated, and holistic physical security plan to ensure overall organizational security
4.3.5. Establish objectives for personnel security to ensure alignment with overall security goals for the enterprise
4.3.6. Design and manage the physical security audit and update issues
4.3.7. Establish a physical security performance measurement system
4.4. Risk Management
4.4.1. Identify the risk mitigation and risk treatment processes and understand the concept of acceptable risk
4.4.2. Identify resource requirements for risk management plan implementation

CCISO Course Objecives

4.4.3. Design a systematic and structured risk assessment process and establish, in coordination with stakeholders, an IT security risk management program based on standards and procedures and ensure alignment with organizational goals and objectives
4.4.4. Develop, coordinate and manage risk management teams
4.4.5. Establish relationships between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals)
4.4.6. Develop an incident management measurement program and manage the risk management tools and techniques
4.4.7. Understand the residual risk in the information infrastructure
4.4.8. Assess threats and vulnerabilities to identify security risks, and regularly update applicable security controls
4.4.9. Identify changes to risk management policies and processes and ensure the risk management program remains current with the emerging risk and threat environment and in alignment with the organizational goals and objectives
4.4.10. Determine if security controls and processes are adequately integrated into the investment planning process based on IT portfolio and security reporting
4.5. Disaster Recovery and Business Continuity Planning
4.5.1. Develop, implement and monitor business continuity plans in case of disruptive events and ensure alignment with organizational goals and objectives
4.5.2. Define the scope of the enterprise continuity of operations program to address business continuity, business recovery, contingency planning, and disaster recovery/related activities
4.5.3. Identify the resources and roles of different stakeholders in business continuity programs
4.5.4. Identify and prioritize critical business functions and consequently design emergency delegations of authority, orders of succession for key positions, the enterprise continuity of operations organizational structure and staffing model
4.5.5. Direct contingency planning, operations, and programs to manage risk
4.5.6. Understand the importance of lessons learned from test, training and exercise, and crisis events
4.5.7. Design documentation process as part of the continuity of operations program
4.5.8. Design and execute a testing and updating plan for the continuity of operations program
4.5.9. Understand the importance of integration of IA requirements into the Continuity of Operations Plan (COOP).
4.5.10. Identify the measures to increase the level of emergency preparedness such as backup and recovery solutions and design standard operating procedures for implementation during disasters
4.6. Firewall, IDS/IPS and Network Defense Systems
4.6.1. Identify the appropriate intrusion detection and prevention systems for organizational information security
4.6.2. Design and develop a program to monitor ¬firewalls and identify ¬firewall configuration issues
4.6.3. Understand perimeter defense systems such as grid sensors and access control lists on routers, ¬firewalls, and other network devices
4.6.4. Identify the basic network architecture, models, protocols and components such as routers and hubs that play a role in network security
4.6.5. Understand the concept of network segmentation

CCISO Course Objecives

4.6.6. Manage DMZs, VPN and telecommunication technologies such as PBX and VoIP
4.6.7. Identify network vulnerabilities and explore network security controls such as use of SSL and TLS for transmission security
4.6.8. Support, monitor, test, and troubleshoot issues with hardware and software
4.6.9. Manage accounts, network rights, and access to systems and equipment
4.7. Wireless Security
4.7.1. Identify vulnerability and attacks associated with wireless networks and manage different wireless network security tools
4.8. Virus, Trojans and Malware Threats
4.8.1. Assess the threat of virus, Trojan and malware to organizational security and identify sources and mediums of malware infection
4.8.2. Deploy and manage anti-virus systems
4.8.3. Develop process to counter virus, Trojan, and malware threats
4.9. Secure Coding Best Practices and Securing Web Applications
4.9.1. Develop and maintain software assurance programs in alignment with the secure coding principles and each phase of System Development Life Cycle (SDLC)
4.9.2. Understand various system-engineering practices
4.9.3. Configure and run tools that help in developing secure programs
4.9.4. Understand the software vulnerability analysis techniques
4.9.5. Install and operate the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards
4.9.6. Identify web application vulnerabilities and attacks and web application security tools to counter attacks

4.10. Hardening OS
4.10.1. Identify various OS vulnerabilities and attacks and develop a plan for hardening OS systems
4.10.2. Understand system logs, patch management process and configuration management for information system security
4.11. Encryption Technologies
4.11.1. Understand the concept of encryption and decryption, digital certificates, public key infrastructure and the key differences between cryptography and steganography
4.11.2. Identify the different components of a cryptosystem
4.11.3. Develop a plan for information security encryption techniques
4.12. Vulnerability Assessment and Penetration Testing
4.12.1. Design, develop and implement a penetration testing program based on penetration testing methodology to ensure organizational security
4.12.2. Identify different vulnerabilities associated with information systems and legal issues involved in penetration testing
4.12.3. Develop pre and post testing procedures
4.12.4. Develop a plan for pen test reporting and implementation of technical vulnerability corrections
4.12.5. Develop vulnerability management systems
4.13. Computer Forensics and Incident Response
4.13.1. Develop a plan to identify a potential security violation and take appropriate action to report the incident
4.13.2. Comply with system termination procedures and incident reporting requirements related to potential security incidents or actual breaches

4.13.3. Assess potential security violations to determine if the network security policies have been breached, assess the impact, and preserve evidence
4.13.4. Diagnose and resolve IA problems in response to reported incidents
4.13.5. Design incident response procedures
4.13.6. Develop guidelines to determine whether a security incident is indicative of a violation of law that requires specific legal action
4.13.7. Identify the volatile and persistent system information
4.13.8. Set up and manage forensic labs and programs
4.13.9. Understand various digital media devices, e-discovery principles and practices and different ¬file systems
4.13.10. Develop and manage an organizational digital forensic program
4.13.11. Establish, develop and manage forensic investigation teams
4.13.12. Design investigation processes such as evidence collection, imaging, data acquisition, and analysis
4.13.13. Identify the best practices to acquire, store and process digital evidence
4.13.14. Configure and use various forensic investigation tools
4.13.15. Design anti-forensic techniques
Domain 5: Strategic Planning and Finance
5.1. Strategic Planning
5.1.1. Design, develop and maintain enterprise information security architecture (EISA) by aligning business processes, IT software and hardware, local and wide area networks, people, operations, and projects with the organization's overall security strategy
5.1.2. Perform external analysis of the organization (e.g., analysis of customers, competitors, markets and industry environment) and internal analysis (risk management, organizational capabilities, performance measurement etc.) and utilize them to align information security program with organization's objectives
5.1.3. Identify and consult with key stakeholders to ensure understanding of organization's objectives
5.1.4. Define a forward-looking, visionary and innovative strategic plan for the role of the information security program with clear goals, objectives and targets that support the operational needs of the organization
5.1.5. Define key performance indicators and measure effectiveness on continuous basis
5.1.6. Assess and adjust IT investments to ensure they are on track to support organization's strategic objectives
5.1.7. Monitor and update activities to ensure accountability and progress
5.2. Finance
5.2.1. Analyze, forecast and develop the operational budget of the IT department
5.2.2. Acquire and manage the necessary resources for implementation and management of information security plan
5.2.3. Allocate ¬financial resources to projects, processes and units within information security program
5.2.4. Monitor and oversee cost management of information security projects, return on investment (ROI) of key purchases related to IT infrastructure and security and ensure alignment with the strategic plan
5.2.5. Identify and report financial metrics to stakeholders

5.2.6. Balance the IT security investment portfolio based on EISA considerations and enterprise security priorities
5.2.7. Understand the acquisition life cycle and determine the importance of procurement by performing Business Impact Analysis
5.2.8. Identify different procurement strategies and understand the importance of cost-benefit analysis during procurement of an information system
5.2.9. Understand the basic procurement concepts such as Statement of Objectives (SOO), Statement of Work (SOW), and Total Cost of Ownership (TCO)
5.2.10. Collaborate with various stakeholders (which may include internal client, lawyers, IT security professionals, privacy professionals, security engineers, suppliers, and others) on the procurement of IT security products and services
5.2.11. Ensure the inclusion of risk-based IT security requirements in acquisition plans, cost estimates, statements of work, contracts, and evaluation factors for award, service level agreements, and other pertinent procurement documents
5.2.12. Design vendor selection process and management policy
5.2.13. Develop contract administration policies that direct the evaluation and acceptance of delivered IT security products and services under a contract, as well as the security evaluation of IT and software being procured
5.2.14. Develop measures and reporting standards to measure and report on key objectives in procurements aligned with IT security policies and procedures
5.2.15. Understand the IA security requirements to be included in statements of work and other appropriate procurement documents

Certified EC-Council Instructor (CEI)

Course Description

The **CEI** program is designed for individuals who want to become certified to deliver EC-Council's suite of professional certification programs. The CEI program provides resources for individuals to become industry-recognized trainers specializing in the field of information security.

All of EC-Council instructor-led training combines lectures, technical demonstrations, and hands-on labs. Certified EC-Council Instructors are required to be technically proficient with good instructional skills. The instructors need to maintain a high standard of professionalism and teaching preparedness..

Key Outcomes

- Assure preparation of the instructional site.
- Establish and maintain instructor credibility.
- Manage the learning environment.
- Demonstrate effective communication skills.
- Demonstrate effective questioning skills and techniques
- Respond appropriately for learners' needs for clarification or feedback.

Exam Information

- Number of questions: 50
- Test duration: 2 hours
- Test format: Multiple choice
- Test delivery: ECC Exam portal

Course Outline

1. Introduction of EC-Council
2. Ethical and Legal Standards
3. Establishing and Maintaining Instructor Credibility
4. Analyzing Course Materials and Learners Information
5. Preparation of the Instructional Site
6. Planning for Instructional Methods
7. Stimulating and Sustaining Learner Motivation and Engagement
8. Effective Presentation Skills
9. Effective Facilitation Skills
10. Effective Questioning Skills
11. Instruction Clarification and Feedbacks
12. Knowledge and Skills Retention of Learners
13. Use of Media and Technology to Enhance Learning and Performance
14. Learning and Performance Assessment
15. Evaluating Instructional Effectiveness
16. Managing the Learning Environment
17. EC-Council Course Information
18. Delivering EC-Council Courses

CEI Course Objectives

Module 01: Introduction of EC-Council
1.1 Overview of International Council of E-Commerce Consultants (EC-Council)
1.2 Overview of EC-Council Certifications
1.3 Understanding EC-Council Security Matrix
1.4 Understanding EC-Council Education Courses
1.5 Understanding EC-Council Security Webinar Series
1.6 Overview of EC-Council Academy
1.7 Understanding EC-Council Evaluation System (EES)
1.8 Overview of EC-Council Accredited Training Center (ATC)
1.9 Overview of EC-Council Continuing Education (ECE)
Module 02: Ethical and Legal Standards
2.1 Understanding Code of Ethics
2.2 Understanding Legal Standards
Module 03: Establishing and Maintaining Instructor Credibility
3.1 Overview of Instructor Credibility
3.2 Maintaining Credibility
3.3 Overview of Instructor's Communication Skills
Module 04: Analyzing Course Materials and Learners Information
4.1 Analyzing Course Material and Learners
4.2 Overview of Learners Information
4.3 Checklist for Course Materials and Learners Information

Module 05: Preparation of the Instructional Site
5.1 Overview of Logistic Arrangements
5.2 Understanding Physical Environment Evaluation
5.3 Understanding Evaluation of the Training Site
Module 06: Planning for Instructional Methods
6.1 Overview of Instructional Methods
6.2 Understand How to choose Right Instructional Method
Module 07: Stimulating and Sustaining Learner Motivation and Engagement
7.1 Stimulating and Sustaining Learner Motivation and Engagement
Module 08: Effective Presentation Skills
8.1 Presenting a Topic
8.2 Preparing the Visuals
8.3 Preparing the Handouts
8.4 Rehearsing and Evaluating the Presentation
8.5 Checklist for Effective Presentation
Module 09: Effective Facilitation Skills
9.1 Overview of Facilitation Skills
9.2 Values of Facilitation
9.3 Overview of Learner Participation
9.4 Things to Avoid in Facilitation

CEI Course Objectives

Module 10: Effective Questioning Skills
10.1 Understanding the Levels of Learning
10.2 Understanding the Questioning Skills
Module 11: Instruction Clarification and Feedbacks
11.1 Understanding Different Types of Feedback
11.2 Analyzing Feedbacks
Module 12: Knowledge and Skills Retention of Learners
12.1 Knowledge and Skills Retention of Learners
Module 13: Use of Media and Technology to Enhance Learning and Performance
13.1 Overview of Media
13.2 Overview of Synchronous Media Devices
13.3 Overview of Asynchronous Media Devices
Module 14: Learning and Performance Assessment
14.1 Understanding Different Methods of Evaluation
Module 15: Evaluating Instructional Effectiveness
15.1 Overview of Elements of Evaluation
15.2 Creating the Evaluation

Module 16: Managing the Learning Environment
16.1 Managing the Learning Environment
16.2 Understand the Time Management
16.3 Motivating Learning
Module 17: EC-Council Course Information
17.1 Overview of Certified Ethical Hacker (CEH)
17.2 Overview of Computer Hacking Forensic Investigator (CHFI)
17.3 Overview of EC-Council Certified Security Analyst (ECSA)
17.4 Overview of EC-Council's Licensed Penetration Tester (LPT)
17.5 Understanding the Exam Process
17.6 Understanding the Training Guidelines
Module 18: Delivering EC-Council Courses
18.1 Overview of CEH Courseware Contents
18.2 Understand How to Teach the CEH Class
18.3 Overview of CHFI Courseware Contents
18.4 Understand How to Teach the CHFI Class
18.5 Overview of ECSA/LPT Courseware Contents
18.6 Understand How to Teach the ECSA/LPT Class

EC-Council | Disaster Recovery Professional™

EC-Council Disaster Recovery Professional (EDRP)

Course Description

The **EDRP** course identifies vulnerabilities and takes appropriate countermeasures to prevent and mitigate failure risks for an organization. It also provides the networking professional a foundation in disaster recovery course principles, including preparation of a disaster recovery plan, assessment of risks in the enterprise, development of policies and procedures, an understanding of the roles and relationships of various members of an organization, implementation of a plan, and recovering from a disaster.

Key Outcomes

- Introduction to business continuity, risk management, and disaster recovery
- Disasters and emergency management, and applicable regulations
- DR planning process, preparation, recovery of systems and facilities
- Incident response and liaison with public services and regulatory bodies
- Exposure to various services from government and other entities

Exam Information

- Number of questions: 150
- Test duration: 4 hours
- Test format: Multiple choice
- Test delivery: ECC Exam portal

Course Outline

1. Introduction to Disaster Recovery and Business Continuity
2. Business Continuity Management (BCM)
3. Risk Assessment
4. Business Impact Analysis (BIA)
5. Business Continuity Planning (BCP)
6. Data Backup Strategies
7. Data Recovery Strategies
8. Virtualization-Based Disaster Recovery
9. System Recovery
10. Centralized and Decentralized System Recovery
11. Disaster Recovery Planning Process
12. BCP Testing, Maintenance, and Training

CAST 614 – Advanced Network Defense

Center for Advanced Security Training

Course Description

The **CAST 614 – Advanced Network Defense** will enable you to evaluate advanced hacking methods of defense fortification, bringing you closer to establishing perfect security best practices and methodologies you can apply to secure environments. It will cover fundamental areas of fortifying your defenses by discovering methods of developing a secure baseline and hardening your enterprise architecture from the most advanced attacks.

Key Outcomes

- Get introduced to concepts of advanced firewall controls and hardening of systems
- Understand intrusions, detection and prevention
- Defending web applications, end points, and critical infrastructure systems

Exam Information

- Onsite workshop

Course Outline

1. Firewalls
2. Advanced filtering
3. Firewall configuration
4. Hardening: establishing a secure baseline
5. Intrusion detection and prevention
6. Protecting web applications
7. Memory analysis
8. Endpoint protection
9. Securing wireless

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Bachelor of Science in Cyber Security (BSCS)

Course Description

The **Bachelor of Science in Cyber Security (BSCS)** prepares students the knowledge for careers in cyber security and assurance. The program consists of topical areas dealing with computer security management, incident response, and security threat assessment, etc.

Key Outcomes

- Knowledge and hands-on experience on various foundational cyber security concepts
- Some of the key topics include security management and incident response, security threat assessment and risk management, legal and regulatory issues and compliance
- Cyber defense and cyber warfare, implementation of security controls, and auditing

Exam Information

- Completion of 60 credit hours of 300/400 level courses in which the candidate earned a cumulative GPA of 2.5 or better
- Satisfactory completion of the summative-capstone course
- All degree requirements must be completed within four years from the date the student enrolls in the University and begins the program

Course Outline

1. CIS 300 Fundamentals of Information Systems Security
2. CIS 301 Legal Issues in Cyber Security
3. CIS 302 Managing Risk in Information Systems
4. CIS 303 Security Policies and Implementation Issues
5. CIS 304 Auditing IT Infrastructures for Compliance
6. CIS 308 Access Control
7. CIS 401 Security Strategies in Windows Platforms and Applications
8. CIS 402 Security Strategies in Linux Platforms and Applications
9. CIS 403 Network Security, Firewalls, and VPNs
10. CIS 404 Hacker Techniques, Tools, and Incident Handling
11. CIS 405 Internet Security: How to Defend Against Online Attackers
12. CIS 406 System Forensics, Investigation, and Response
13. CIS 407 Cyberwarfare
14. CIS 408 Wireless and Mobile Device Security
15. CIS 410 Capstone Course
16. ENG 340 English Communications
17. MTH 350 Introduction to Statistics
18. PSY 360 Social Psychology
19. BIS 430 Ethics for the Business Professional
20. ECN 440 Principles of Microeconomics
21. MGT 450 Introduction to Project Management

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Graduate Certificate Programs

Course Description

EC-Council University's Graduate Certificate Program focuses on the competencies necessary for information assurance professionals to become managers, directors, and CIOs. Students will experience not only specialized technical training in a variety of IT security areas, but will also acquire an understanding of organizational structure and behavior, the skills to work within and across that organizational structure, and the ability to analyze and navigate its hierarchy successfully. Each certificate targets skills and understandings specific to particular roles in the IT security framework of an organization. The certificates can be taken singly or as a progressive set of five, each building on the one before it to move students from IT practitioner skill levels to IT executive skill levels.

Key Outcomes

- Establishes the role of CISO and models for governance
- Core concepts of information security controls, risk management, and compliance
- Builds foundation for leadership through strategic planning, program management, and vendor management

Exam Information

- Exam Format : Multiple Choice
- Total number of questions : 150
- Exam duration : 2.5 Hours
- Required passing score : 72%

Course Outline

- Information Security Professional
  - ECCU 500 Managing Secure Network Systems
  - ECCU 501 Ethical Hacking and Countermeasures
  - ECCU 505 Research and Writing for the IT Practitioner
  - Digital Forensics
  - Disaster Recovery
  - Executive Information Assurance
  - IT Analyst

EC-COUNCIL UNIVERSITY
ACCREDITED. FLEXIBLE. ONLINE.

Master of Science in Cyber Security (MSS)

Course Description

CHFI is a comprehensive course covering major forensic investigation scenarios, enabling students to acquire hands-on experience.

The program provides a strong baseline knowledge of key concepts and practices in the digital forensic domains relevant to today's organizations. Moreover, CHFI provides firm grasp on the domains of digital forensics.

Key Outcomes

- Comprehensive forensics investigation process
- Forensics of file systems, operating systems, network and database, websites, and email systems
- Techniques for investigating on cloud, malware, and mobile
- Data acquisition and analysis as well as anti-forensic techniques
- Thorough understanding of chain of custody, forensic report, and presentation

Exam Information

- Number of Questions: 150
- Passing Score: 70%
- Test Duration: 4 hours
- Test Format: Multiple choice
- Test Delivery: ECC Exam portal

Course Outline

1. ECCU 500 Managing Secure Network Systems
2. ECCU 501 Ethical Hacking and Countermeasures
3. ECCU 502 Investigating Network Intrusions & Computer Forensics
4. ECCU 503 Security Analysis and Vulnerability Assessment
5. ECCU 504 Foundations of Organizational Behavior
6. ECCU 505 Intro to Research and Writing for the IT Practitioner
7. ECCU 506 Conducting Penetration andSecurity Tests
8. Linux Networking and Security
9. ECCU 507 Securing Wireless Networks
10. ECCU 509 Secure Programming
11. ECCU 510 Beyond Business Continuity
12. ECCU 512 Project Management in IT Security
13. ECCU 515 Th e Hacker Mind: Profi ling the IT Criminal
14. ECCU 517 Cyber Law
15. ECCU 511 Global Business Leadership
16. ECCU 512 Beyond Business Continuity: Managing Organizational Change
17. ECCU 514 Quantum Leadership
18. MGMT 502 Business Essential
19. ECCU 506 Conducting Penetration and Security Tests Disaster Recovery
20. ECCU 513 Disaster Recovery
21. ECCU 515 Project Management in IT Security
22. ECCU 516 Th e Hacker Mind: Profi ling the IT Criminal
23. ECCU 517 Cyber Law
24. Final Course required ECCU 519 CAPSTONE

Mapping Methodology

Mapping Methodology

1. Identification of NICE Cybersecurity Workforce Framework (NCWF) cybersecurity work Categories, Speciality Areas and respective Job Roles
2. Analysis of Tasks, Knowledge, Skills and Abilities associated with each Job Roles
3. Analysis of Cybersecurity job roles and work role descriptions
4. Mapping NCWF Tasks and KSAs to Bloom's cognitive action verbs
5. Research on NICE proficiency description
6. Proximity search of EC-Council exam objective with relevance to each Tasks and KSAs of NCWF
7. Relationship of each Tasks and KSAs of NCWF and EC-Council certification exam objectives (with requisite knowledge & performance filters) to determine a correlation to ±5%
8. Validation of relevance of EC-Council exam objectives with reference to NCWF Tasks and KSAs based on SME reviews, student feedback, and industry acceptance of the trained workforce
9. Mapping the training proficiency level for each course with the NCWF Job Roles

Mapping References

- NCWF and United States Office of Personnel Management (OPM) Job Role Mapping
- Proficiency Descriptions
- Bloom's Taxonomy

Job Role Mapping

Categories	Specialty Areas	Work Role	NCWF ID	OPM Code
Securely Provision (SP)				
	Risk Management (RM)	Authorizing Official/Designating Representative	SP-RM-001	611
		Security Control Assessor	SP-RM-002	612
	Software Development (DEV)	Software Developer	SP-DEV-001	621
		Secure Software Assessor	SP-DEV-002	622
	Systems Architecture (ARC)	Enterprise Architect	SP-ARC-001	651
		Security Architect	SP-ARC-002	652
	Technology R&D (RD)	Research & Development Specialist	SP-RD-001	661
	Systems Requirements Planning (RP)	Systems Requirements Planner	SP-RP-001	641
	Test and Evaluation (TE)	System Testing and Evaluation Specialist	SP-TE-001	671
	Systems Development (SYS)	Information Systems Security Developer	SP-SYS-001	631
		Systems Developer	SP-SYS-002	632
Operate and Maintain (OM)				
	Data Administration (DA)	Database Administrator	OM-DA-001	421
		Data Analyst	OM-DA-002	422
	Knowledge Management (KM)	Knowledge Manager	OM-KM-001	431
	Customer Service and Technical Support (TS)	Technical Support Specialist	OM-TS-001	411
	Network Services (NET)	Network Operations Specialist	OM-NET-001	441
	Systems Administration (SA)	System Administrator	OM-SA-001	451
	Systems Analysis (AN)	Systems Security Analyst	OM-AN-001	461

Job Role Mapping

Categories	Specialty Areas	Work Role	NCWF ID	OPM Code
Oversee and Govern (OV)				
	Legal Advice and Advocacy (LG)	Cyber Legal Advisor	OV-LG-001	731
		Privacy Compliance Manager	OV-LG-002	732
	Training, Education, and Awareness (ED)	Cyber Instructional Curriculum Developer	OV-ED-001	711
		Cyber Instructor	OV-ED-002	712
	Cybersecurity Management (MG)	Information Systems Security Manager	OV-MG-001	722
		COMSEC Manager	OV-MG-002	723
	Strategic Planning and Policy (PL)	Cyber Workforce Developer and Manager	OV-PL-001	751
		Cyber Policy and Strategy Planner	OV-PL-002	752
	Executive Cybersecurity Leadership (EX)	Executive Cyber Leadership	OV-EX-001	901
	Acquisition and Program/Project Management (PM)	Program Manager	OV-PM-001	801
		IT Project Manager	OV-PM-002	802
		Product Support Manager	OV-PM-003	803
		IT Investment/Portfolio Manager	OV-PM-004	804
		IT Program Auditor	OV-PM-005	805
Protect and Defend (PR)				
	Cybersecurity Defense Analysis (DA)	Cyber Defense Analyst	PR-DA-001	511
	Cybersecurity Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	PR-INF-001	521
	Incident Response (IR)	Cyber Defense Incident Responder	PR-IR-001	531
	Vulnerability Assessment and Management (VA)	Vulnerability Assessment Analyst	PR-VA-001	541

Job Role Mapping

Categories	Specialty Areas	Work Role	NCWF ID	OPM Code
Analyze (AN)				
	Threat Analysis (TA)	Warning Analyst	AN-TA-001	141
	Exploitation Analysis (XA)	Exploitation Analyst	AN-XA-001	121
	All-Source Analysis (AN)	All-Source Analyst	AN-AN-001	111
		Mission Assessment Specialist	AN-AN-002	112
	Targets (TD)	Target Developer	AN-TD-001	131
		Target Network Analyst	AN-TD-002	132
	Language Analysis (LA)	Multi-Disciplined Language Analyst	AN-LA-001	151
Collect and Operate (CO)				
	Collection Operations (CL)	All Source-Collection Manager	CO-CL-001	311
		All Source-Collection Requirements Manager	CO-CL-002	312
	Cyber Operational Planning (PL)	Cyber Intel Planner	CO-PL-001	331
		Cyber Ops Planner	CO-PL-002	332
		Partner Integration Planner	CO-PL-003	333
	Cyber Operations (OP)	Cyber Operator	CO-OP-001	321
Investigate (IN)				
	Cyber Investigation (CI)	Cyber Crime Investigator	IN-CI-001	221
	Digital Forensics (FO)	Forensics Analyst	IN-FO-001	211
		Cyber Defense Forensics Analyst	IN-FO-002	212

Proficiency Levels

Level	Proficiency Category	Description
0	No Proficiency	This training is intended for someone with insufficient knowledge, skill, or ability level necessary for use in simple or routine work situations. Knowledge, skill, or ability level provided would be similar to the knowledge of a layperson. Considered "no proficiency" for purposes of accomplishing specialized, or technical, work.
1	Basic	This training is intended for individuals who need basic knowledge, skills, or abilities necessary for use and the application in simple work situations with specific instructions and/or guidance.
2	Intermediate	This training is intended for individuals who need intermediate knowledge, skills, or abilities for independent use and application in straightforward, routine work situations with limited need for direction.
3	Advanced	This training is intended for individuals who need advanced knowledge, skills, or abilities for independent use and application in complex or novel work situations.
4	Expert	This training is intended for individuals who need expert knowledge, skills, or abilities for independent use and application in highly complex, difficult, or ambiguous work situations, or the trainee is an acknowledged authority, advisor, or key resource.

Bloom's Taxonomy

Bloom's Taxonomy

Bloom's taxonomy is a classification of learning objectives within education. It is named for Benjamin Bloom, who chaired the committee of educators that devised the taxonomy. Bloom's taxonomy is considered to be a foundational and essential element within the education community.

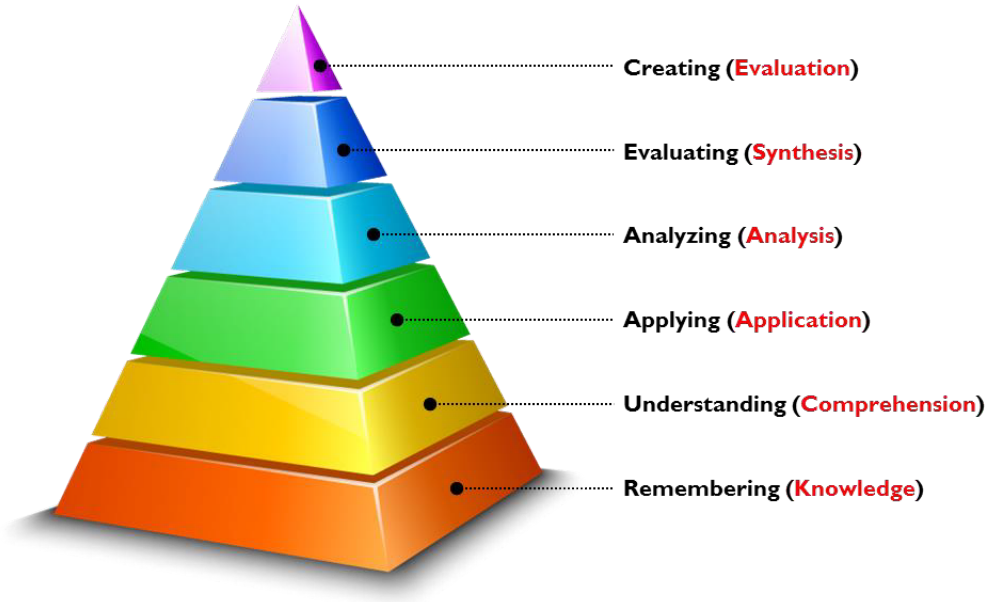
It divides educational objectives into three domains:

1. Cognitive - involves knowledge and the development of intellectual skills (Knowledge)
2. Affective - growth in feelings or emotional areas (Attitude or self)
3. Psychomotor - manual or physical skills (Skills)

Bloom's Taxonomy was revised in 2001by a group of cognitive psychologists, curriculum theorists and instructional researchers, and testing and assessment specialists led by Lorin Anderson, a former student of Bloom. This new taxonomy reflects a more active form of thinking and is considered more accurate by academicians.

The revised taxonomy points to a more dynamic conception of classification using verbs and gerunds to label their categories and subcategories (rather than the nouns of the original taxonomy). These "action words" describe the cognitive processes by which thinkers encounter and work with knowledge (Armstrong, P. Center for Teaching. Vanderbilt University. 2014).

Revised Bloom's Taxonomy for Cognitive Learning



Note: Parentheses contain the original taxonomy domains.

Bloom's Taxonomy

Revised Bloom's Taxonomy Categories, Definitions and Action Verbs

Bloom's Category	Definition	Action Verbs
Remembering	Recall previous learned information.	Arrange, Choose, Cite, Define, Describe, Duplicate, Enumerate, Group, Identify, Label, List, Listen, Locate, Match, Memorize, Name, Order, Outline, Quote, Recognize, Relate, Recall, Repeat, Reproduce, Read, Recite, Record, Review, Select, Show, Sort, State, Underline, Write
Understanding	Comprehend the meaning, translation, interpolation, and interpretation of instructions and problems. State a problem in one's own words.	Account for, Annotate, Associate, Classify, Convert, Defend, Define, Describe, Discuss, Distinguish, Estimate, Explain, Express, Extend, Generalized, Give example(s),Identify, Indicate, Infer, Interpret, Locate, Observe, Outline, Paraphrase, Predict, Recognize, Rewrite, Review, Reorganize, Report, Research, Restate, Retell, Select, Summarize, Translate
Applying	Apply rules, facts, concepts and ideas.	Adapt, Apply, Calculate, Change, Choose, Collect, Compute, Construct, Demonstrate, Discover, Dramatize, Draw, Employ, Exhibit, Generalize, Illustrate, Interpret, Interview, Make, Manipulate, Modify, Operate, Paint, Practice, Predict, Prepare, Produce, Relate, Schedule, Sequence, Show, Sketch, Solve, Translate, Use, Write
Analyzing	Separate material or concepts into component parts so that its organizational structure may be understood. Distinguish between facts and inferences.	Analyze, Appraise, Arrange, Breakdown, Calculate, Categorize, Compare, Contrast, Criticize, Debate, Detect, Diagram, Differentiate, Discriminate, Dissect, Distinguish, Examine, Experiment, Group, Identify, Illustrate, Infer, Inquire, Inspect, Investigate, Model, Order, Outline, Point out, Probe, Question, Relate, Research, Scrutinize, Select, Separate, Sequence, Sift, Subdivide, Summarize, Survey, Test
Evaluating	Make judgments about the value of ideas or materials.	Appraise, Argue, Assess, Choose, Compare, Conclude, Criticize, Critique, Debate, Decide, Deduce, Defend, Determine, Differentiate, Discriminate, Evaluate, Infer, Judge, Justify, Measure, Predict, Prioritize, Probe, Rank, Rate, Recommend, Revise, Score, Select, Validate, Value
Creating	Build a structure or pattern from diverse elements. Put parts together to form a whole, with emphasis on creating a new meaning or structure.	Act, Assemble, Blend, Combine, Compile, Compose, Concoct, Construct, Create, Design, Develop, Devise, Formulate, Forecast, Generate, Hypothesize, Imagine, Invent, Organize, Originate, Predict, Plan, Prepare, Propose, Produce, Set up

Mapping Summary

NCWF Categories	Specialty Areas	Work Role	NCWF ID	EC-Council Certification	Proficiency Match (0-4)
Securely Provision (SP)					
	Risk Management (RM)	Authorizing Official/Designating Representative	SP-RM-001	CCISO	4
		Security Control Assessor	SP-RM-002	CCISO	3
	Software Development (DEV)	Software Developer	SP-DEV-001	CASE	3
		Secure Software Assessor	SP-DEV-002	CASE	3
	Systems Architecture (ARC)	Enterprise Architect	SP-ARC-001	CND	3
		Security Architect	SP-ARC-002	CND	3
	Technology R&D (RD)	Research & Development Specialist	SP-RD-001	CEH	3
	Systems Requirements Planning (RP)	Systems Requirements Planner	SP-RP-001	CND	3
	Test and Evaluation (TE)	System Testing and Evaluation Specialist	SP-TE-001	CND	3
	Systems Development (SYS)	Information Systems Security Developer	SP-SYS-001	CND	3
		Systems Developer	SP-SYS-002	CND	3
Operate and Maintain (OM)					
	Data Administration (DA)	Database Administrator	OM-DA-001	N/A	
		Data Analyst	OM-DA-002	N/A	
	Knowledge Management (KM)	Knowledge Manager	OM-KM-001	N/A	
	Customer Service and Technical Support (TS)	Technical Support Specialist	OM-TS-001	CND	3
	Network Services (NET)	Network Operations Specialist	OM-NET-001	CND	3
	Systems Administration (SA)	System Administrator	OM-SA-001	CND	3
	Systems Analysis (AN)	Systems Security Analyst	OM-AN-001	CND	3

Mapping Summary

NCWF Categories	Specialty Areas	Work Role	NCWF ID	EC-Council Certification	Proficiency Match (0-4)
Oversee and Govern (OV)					
	Legal Advice and Advocacy (LG)	Cyber Legal Advisor	OV-LG-001	CCISO	3
		Privacy Compliance Manager	OV-LG-002	CCISO	4
	Training, Education, and Awareness (ED)	Cyber Instructional Curriculum Developer	OV-ED-001	CEI	4
		Cyber Instructor	OV-ED-002	CEI	4
	Cybersecurity Management (MG)	Information Systems Security Manager	OV-MG-001	CCISO	4
		COMSEC Manager	OV-MG-002	CCISO	4
	Strategic Planning and Policy (PL)	Cyber Workforce Developer and Manager	OV-PL-001	CCISO	3
		Cyber Policy and Strategy Planner	OV-PL-002	CCISO	4
	Executive Cybersecurity Leadership (EX)	Executive Cyber Leadership	OV-EX-001	CCISO	4
	Acquisition and Program/Project Management (PM)	Program Manager	OV-PM-001	CCISO	3
		IT Project Manager	OV-PM-002	CCISO	3
		Product Support Manager	OV-PM-003	CCISO	3
		IT Investment/Portfolio Manager	OV-PM-004	CCISO	3
		IT Program Auditor	OV-PM-005	CCISO	4
Protect and Defend (PR)					
	Cybersecurity Defense Analysis (DA)	Cyber Defense Analyst	PR-DA-001	CEH	3
	Cybersecurity Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	PR-INF-001	CND	3
	Incident Response (IR)	Cyber Defense Incident Responder	PR-IR-001	ECIH	3

Mapping Summary

NCWF Categories	Specialty Areas	Work Role	NCWF ID	EC-Council Certification	Proficiency Match (0-4)
	Vulnerability Assessment and Management (VA)	Vulnerability Assessment Analyst	PR-VA-001	CEH	3
Analyze (AN)					
	Threat Analysis (TA)	Warning Analyst	AN-TA-001	CEH	3
	Exploitation Analysis (XA)	Exploitation Analyst	AN-XA-001	ECSA	4
	All-Source Analysis (AN)	All-Source Analyst	AN-AN-001	ECSA	3
		Mission Assessment Specialist	AN-AN-002	ECSA	3
	Targets (TD)	Target Developer	AN-TD-001	ECSA	4
		Target Network Analyst	AN-TD-002	ECSA	4
	Language Analysis (LA)	Multi-Disciplined Language Analyst	AN-LA-001	ECSA	4
Collect and Operate (CO)					
	Collection Operations (CL)	All Source-Collection Manager	CO-CL-001	ECSA	3
		All Source-Collection Requirements Manager	CO-CL-002	ECSA	3
	Cyber Operational Planning (PL)	Cyber Intel Planner	CO-PL-001	ECSA	3
		Cyber Ops Planner	CO-PL-002	ECSA	3
		Partner Integration Planner	CO-PL-003	ECSA	3
	Cyber Operations (OP)	Cyber Operator	CO-OP-001	ECSA	4
Investigate (IN)					
	Cyber Investigation (CI)	Cyber Crime Investigator	IN-CI-001	CHFI	4
	Digital Forensics (FO)	Forensics Analyst	IN-FO-001	CHFI	3
		Cyber Defense Forensics Analyst	IN-FO-002	CHFI	3

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

SECURELY PROVISION (SP)

Specialty areas responsible for conceptualizing, designing, and building secure information technology (IT) systems, with responsibility for aspects of systems and/or networks development.

Risk Management (RM)

Oversees, evaluates, and supports the documentation, validation, assessment, and authorization processes necessary to assure that existing and new IT systems meet the organization's cybersecurity and risk requirements. Ensures appropriate treatment of risk, compliance, and assurance from internal and external perspectives.

Software Development (DEV)

Develops and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs following software assurance best practices.

Systems Architecture (ARC)

Develops system concepts and works on the capabilities phases of the systems development lifecycle; translates technology and environmental conditions (e.g., law and regulation) into system and security designs and processes.

Technology Research and Development (RD)

Conducts technology assessment and integration processes; provides and supports a prototype capability and/or evaluates its utility.

Systems Requirements Planning (RP)

Consults with customers to gather and evaluate functional requirements and translates these requirements into technical solutions. Provides guidance to customers about applicability of information systems to meet business needs.

Test and Evaluation (TE)

Develops and conducts tests of systems to evaluate compliance with specifications and requirements by applying principles and methods for cost-effective planning, evaluating, verifying, and validating of technical, functional, and performance characteristics (including interoperability) of systems or elements of systems incorporating information technology (IT).

Systems Development (SYS)

Works on the development phases of the systems development lifecycle.

NCWF JOB ROLE

Authorizing Official/Designating Representative

Job Role Description: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an Authorizing Official. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .6 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0145	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Synthesis, Evaluation	1.5 to 1.10	4	60% or .6
T0221	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Synthesis, Evaluation	2.1, 4.4	4	70% or .7
T0371	Establish acceptable limits for the software application, network, or system.	Analyze, Synthesis	2.1	3	50% or .5
T0495	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Synthesis, Evaluation	1.5 to 1.10	4	60% or .6
	Summary			**4**	**60% or .6**

NCWF JOB ROLE

Authorizing Official/Designating Representative

Job Role Description: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an Authorizing Official. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .6 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0013	Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities.	2.1.7, 4.1.2, 4.7.1, 4.9.6	4	95% or .95
K0019	Knowledge of cryptography and cryptographic key management concepts.	4.11	4	60% or .60
K0027	Knowledge of organization's enterprise information security architecture system.	2.1	3	65% or .65
K0028	Knowledge of organization's evaluation and validation requirements.	3.11	3	60% or .60
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	4.4	3	65% or .65
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	4.12	3	95% or .95
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	4.1 to 4.12	4	95% or .95
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	4	95% or .95
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	4.6	4	90% or .9
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	2.1,2.2	3	65% or .65

NCWF JOB ROLE

Authorizing Official/Designating Representative

Job Role Description: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an Authorizing Official. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .6 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	5.1		
K0084	Knowledge of structured analysis principles and methods.	1.1, 1.3,5.1	3	60% or .60
K0085	Knowledge of system and application security threats and vulnerabilities.	4.9	3	60% or .60
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	4.10, 4.13.4	3	60% or .60
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	5.1	4	100% or 1
K0146	Knowledge of the organization's core business/mission processes.	3.1 to 3.14	4	100% or 1
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	1.7 to 1.10	4	100% or 1
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	4	100% or 1
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	3.12	3	60% or .60
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	4.6	3	100% or 1
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	5.1	4	100% or 1
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	5.1	4	100% or 1
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	1.7 to 1.10	4	100% or 1
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	1.7 to 1.10	4	100% or 1
K0262	Knowledge of Personal Health Information (PHI) data security standards.	1.7 to 1.10	4	100% or 1

NCWF JOB ROLE

Authorizing Official/Designating Representative

Job Role Description: Senior official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an Authorizing Official. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .6 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	1.7 to 1.10	4	100% or 1
K0295	Knowledge of confidentiality, integrity, and availability principles.	4.1	4	100% or 1
K0322	Knowledge of embedded systems.	NA		
K0342	Knowledge of penetration testing principles, tools, and techniques.	4.12	3	80% or .80
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	2.1.3	3	80% or .80
	Summary		**4**	**90% or .9**

NCWF JOB ROLE

Security Control Assessor

Job Role Description: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Security Control Assessor. CCISO maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0032	Conduct Privacy Impact Assessments (PIA) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Synthesis, Evaluation	2.2.2	4	80% or .80
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Synthesis, Evaluation	4.4.3	**3**	60% or .60
T0079	Develop specifications to ensure risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level.	Synthesis, Evaluation	4.4.1 to 4.4.10	4	80% or .80
T0083	Draft statements of preliminary or residual security risks for system operation.	Synthesis, Evaluation	4.4.7	4	80% or .80
T0141	Maintain information systems assurance and accreditation materials.	Application, Evaluation	5.1.1	4	80% or .80
T0150	Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements.	Synthesis, Evaluation	1.4	**3**	60% or .60
T0183	Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks.	Synthesis, Evaluation	2.2.3,2.2.4	4	80% or .80
T0184	Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.	Synthesis, Evaluation	4.1.1 to 4.1.5	3	60% or .60
T0197	Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant cybersecurity compliances.	Synthesis, Evaluation	2.2.4	3	60% or .60
T0218	Recommend new or revised security, resilience, and dependability measures based on the results of reviews.	Application, Analysis	2.2.7	3	60% or .60
T0221	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Application, Analysis	2.1.5	2	40% or .40

NCWF JOB ROLE

Security Control Assessor

Job Role Description: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Security Control Assessor. CCISO maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0244	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.	Application, Analysis	2.2.3,2.2.4	3	60% or .60
T0245	Verify that the software application/network/system accreditation and assurance documentation is current.	Application, Analysis	2.2.2,2.2.3	3	60% or .60
T0251	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).	Synthesis, Evaluation	2.2.1 to 2.2.7	3	60% or .60
T0301	Develop and Implement cybersecurity independent audit processes for application software/networks/systems and oversee ongoing independent audits to ensure that operational and Research and Design (R&D) processes and procedures are in compliance with organizational and mandatory cybersecurity requirements and accurately followed by Systems Administrators and other cybersecurity staff when performing their day-to-day activities.	Application, Analysis, Synthesis, Evaluation	2.2.1 to 2.2.7	3	60% or .60
	Summary			**3**	**65% or .65**

NCWF JOB ROLE

Security Control Assessor

Job Role Description: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Security Control Assessor. CCISO maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0013	Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities.	2.1.7, 4.1.2, 4.7.1, 4.9.6	4	95% or .95
K0019	Knowledge of cryptography and cryptographic key management concepts.	4.11	4	60% or .60
K0027	Knowledge of organization's enterprise information security architecture system.	2.1	3	65% or .65
K0028	Knowledge of organization's evaluation and validation requirements.	3.11	3	60% or .60
K0037	Knowledge of the Security Assessment and Authorization process.	4.1, 4.12	3	60% or .60
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	4.4	3	65% or .65
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	4.12	3	95% or .95
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	4.1 to 4.12	4	95% or .95
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	4	95% or .95
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	4.6	4	90% or .9

NCWF JOB ROLE

Security Control Assessor

Job Role Description: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Security Control Assessor. CCISO maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	2.1,2.2	3	65% or .65
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	5.1		
K0084	Knowledge of structured analysis principles and methods.	1.1, 1.3,5.1	3	60% or .60
K0085	Knowledge of system and application security threats and vulnerabilities.	4.9	3	60% or .60
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	4.10, 4.13.4	3	60% or .60
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	5.1	4	100% or 1
K0146	Knowledge of the organization's core business/mission processes.	3.1 to 3.14	4	100% or 1
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	1.7 to 1.10	4	100% or 1
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	4	100% or 1
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	3.12	3	60% or .60
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	4.6	3	100% or 1
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	5.1	4	100% or 1
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	5.1	4	100% or 1
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	1.7 to 1.10	4	100% or 1

NCWF JOB ROLE

Security Control Assessor

Job Role Description: Conducts independent comprehensive assessments of the management, operational, and technical security controls and control enhancements employed within or inherited by an information technology (IT) system to determine the overall effectiveness of the controls (as defined in NIST SP 800-37).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Security Control Assessor. CCISO maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	1.7 to 1.10	4	100% or 1
K0262	Knowledge of Personal Health Information (PHI) data security standards.	1.7 to 1.10	4	100% or 1
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	1.7 to 1.10	4	100% or 1
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	4.1	4	100% or 1
K0322	Knowledge of embedded systems.	NA		
K0342	Knowledge of penetration testing principles, tools, and techniques.	4.12	3	80% or .80
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	4.4.8, 4.6.7, 4.7.1, 4.9.6, 4.10.1, 4.12.4, 4.12.5	4	100% or 1
S0006	Skill in applying confidentiality, integrity, and availability principles.	4.1 - 4.13	4	100% or 1
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	5.1.2	3	80% or .80
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	2.1.3	3	80% or .80
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	2.1.4	4	80% or .80
S0086	Skill in evaluating the trustworthiness of the supplier and/or product.	5.2.10	4	80% or .80
	Summary		**4**	**90% or .9**

NCWF JOB ROLE

Software Developer

Job Role Description: A Software Developer develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Software Developer. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
T0009	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.	Analysis	NA		
T0011	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.	Analysis	NA		
T0013	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	Application	9.11,9.12	1	20% or .2
T0014	Apply secure code documentation.	Application, Synthesis	1 - 9	4	90% or .9
T0022	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	Identify, Analysis	NA		
T0026	Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.	Record	NA		
T0034	Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.	Discuss, Analysis	NA		
T0040	Consult with engineering staff to evaluate interface between hardware and software.	Evaluate	NA		
T0046	Correct errors by making appropriate changes and rechecking the program to ensure desired results are produced.	Examine, Analysis	7.7 to 7.12	3	60% or .6
T0057	Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.	Design, Synthesis	NA		
T0077	Develop secure code and error handling.	Create, Synthesis	1 - 9	4	95% or .95

NCWF JOB ROLE

Software Developer

Job Role Description: A Software Developer develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Software Developer. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
T0100	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	Evaluation, Synthesis	NA		
T0111	Identify basic common coding flaws at a high level.	Evaluation	1 - 9	4	90% or .9
T0117	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development.	Identify, Analysis	NA		
T0118	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.	Identify, Analysis	NA		
T0171	Perform integrated quality assurance testing for security functionality and resiliency attack.	Application	9.1	1	20% or .2
T0176	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.	Application, Evaluation	1 - 9	4	95% or .95
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Application	1.9	2	40% or .4
T0189	Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language.	Prepare	NA		
T0217	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Locate	NA		
T0228	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Evaluate	NA		

NCWF JOB ROLE

Software Developer

Job Role Description: A Software Developer develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Software Developer. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
T0236	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.	Convert	NA		
T0267	Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.	Design, Synthesis	1 - 9	4	95% or .95
T0303	Identify and leverage the enterprise-wide version control system while designing and developing secure applications.	Identify	NA		
T0311	Consult with customers about software system design and maintenance.	Evaluate	NA		
T0324	Direct software programming and development of documentation.	Prepare	NA		
T0337	Supervise and assign work to programmers, designers, technologists and technicians and other engineering and scientific personnel.	Operate	NA		
T0416	Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.	Application	6.1 to 6.12	1	25% or .25
T0417	Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Anti-Virus solution) when appropriate.	Identify	NA		
T0436	Conduct trial runs of programs and software applications to ensure the desired information is produced and instructions and security levels are correct.	Employ	NA		
T0455	Develop software system testing and validation procedures, programming, and documentation.	Develop	NA		
T0500	Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.	Modify	NA		
T0553	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Application	4.1 to 4.7, 6.1 to 6.12	3	70% or .7

NCWF JOB ROLE

Software Developer

Job Role Description: A Software Developer develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Software Developer. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
T0554	Determine and document software patches or the extent of releases that would leave software vulnerable.	Identify, Analysis	NA		
	Summary			**3**	**20% or .2**

NCWF JOB ROLE

Software Developer

Job Role Description: A Software Developer develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Software Developer. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

KSA

ID	Statement	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	NA		
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	NA		
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	NA		
K0004	* Knowledge of cybersecurity principles.	4.1 to 4.9		
K0005	* Knowledge of cyber threats and vulnerabilities.	1.6,1.7	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.5	4	90% or .9
K0014	Knowledge of complex data structures.	NA		
K0016	Knowledge of computer programming principles such as object-oriented design.	NA		
K0027	Knowledge of organization's enterprise information security architecture system.	NA		
K0028	Knowledge of organization's evaluation and validation requirements.	NA		
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	4.1 to 4.9	1	20% or .2
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	4.1 to 4.9	1	20% or .2
K0051	Knowledge of low-level computer languages (e.g., assembly languages).	NA		
K0060	Knowledge of operating systems.	NA		
K0066	Knowledge of Privacy Impact Assessments.	NA		
K0068	Knowledge of programming language structures and logic.	NA		
K0073	Knowledge of secure configuration management techniques.	9.1 - 9.9	4	95% or .95
K0079	Knowledge of software debugging principles.	NA		
K0080	Knowledge of software design tools, methods, and techniques.	1 - 9	3	80% or .8
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	NA		

NCWF JOB ROLE

Software Developer

Job Role Description: A Software Developer develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Software Developer. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

KSA

ID	Statement	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
K0082	Knowledge of software engineering.	NA		
K0084	Knowledge of structured analysis principles and methods.	NA		
K0085	Knowledge of system and application security threats and vulnerabilities.	1.6,1.7	4	95% or .95
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	NA		
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	NA		
K0139	Knowledge of interpreted and compiled computer languages.	NA		
K0140	Knowledge of secure coding techniques.	1 - 9	4	100% or 1
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	NA		
K0153	Knowledge of software quality assurance process.	NA		
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	NA		
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	NA		
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	NA		
K0202	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).	NA		
K0219	Knowledge of local area network (LAN) and wide area network (WAN) principles.	NA		

NCWF JOB ROLE

Software Developer

Job Role Description: A Software Developer develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Software Developer. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

KSA

ID	Statement	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	NA		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	NA		
K0262	Knowledge of Personal Health Information (PHI) data security standards.	NA		
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	NA		
K0322	Knowledge of embedded systems.	NA		
K0331	Knowledge of network protocols (e.g., Transmission Critical Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP)), and directory services (e.g., Domain Name System (DNS)).	NA		
K0342	Knowledge of penetration testing principles, tools, and techniques.	NA		
K0343	Knowledge of root cause analysis techniques.	NA		
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	9.10 - 9.12	2	20%or 0.2
S0014	Skill in conducting software debugging.	NA		
S0017	Skill in creating and utilizing mathematical or statistical models.	NA		
S0019	Skill in creating programs that validate and process multiple inputs including command line arguments, environmental variables, and input streams.	3.1 - 3.12	1	10% or .1
S0022	Skill in designing countermeasures to identified security risks.	1 - 9		
S0031	Skill in developing and applying security system access controls.	6.4,6.5	2	20% or .2
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	NA		
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	NA		
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	NA		
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	6.1 - 6.12	3	80% or .8
S0149	Skill in developing applications that can log and handle errors, exceptions, and application faults and logging.	7.7 - 7.12	3	90% or .9

NCWF JOB ROLE

Software Developer

Job Role Description: A Software Developer develops, creates, maintains, and writes/codes new (or modifies existing) computer applications, software, or specialized utility programs.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Software Developer. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

KSA

ID	Statement	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
S0174	Skill in using code analysis tools.	9.12	1	30% or .3
S0175	Skill in performing root cause analysis.	NA		
A0007	Ability to tailor code analysis for application-specific concerns.	9.10 - 9.12	1	30% or .3
A0021	Ability to use and understand complex mathematical concepts (e.g., discrete math).	NA		
A0047	Ability to develop secure software according to secure software deployment methodologies, tools, and practices.	1 - 9	4	100% or 1
	Summary		**3**	**20% or .2**

NCWF JOB ROLE

Secure Software Assessor

Job Role Description: A Secure Software Assessor analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Secure Software Assessor. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
T0013	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	Application, Synthesis	1 - 9	4	90% or .9
T0014	Apply secure code documentation.	Application, Synthesis	1 - 9	4	100% or 1
T0022	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	Analysis	NA		
T0038	Develop threat model based on customer interviews and requirements.	Application, Synthesis	1.9	3	75% to .75
T0040	Consult with engineering staff to evaluate interface between hardware and software.	Evaluation	NA		
T0100	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	Evaluation	NA		
T0111	Identify basic common coding flaws at a high level.	Identify, Evaluation	1 - 9	4	90% or .9
T0117	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprises computer systems in software development.	Analysis	NA		
T0118	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.	Analysis	NA		
T0171	Perform integrated quality assurance testing for security functionality and resiliency attack.	Analysis	1.1	2	20% or .2
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Analysis	1.9	3	50% or .5

NCWF JOB ROLE

Secure Software Assessor

Job Role Description: A Secure Software Assessor analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Secure Software Assessor. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
T0217	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Application	NA		
T0228	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Application	NA		
T0236	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.	Analysis	1.9	3	50% or .5
T0266	Perform penetration testing as required for new or updated applications.	Analysis, Evaluation	NA		
T0311	Consult with customers about software system design and maintenance.	Analysis, Evaluation	NA		
T0324	Direct software programming and development of documentation.	Analysis, Evaluation	NA		
T0337	Supervise and assign work to programmers, designers, technologists and technicians and other engineering and scientific personnel.	Analysis, Evaluation	NA		
T0424	Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.	Analysis, Evaluation	NA		
T0428	Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.	Analysis, Evaluation	NA		
T0436	Conduct trial runs of programs and software applications to ensure the desired information is produced and instructions and security levels are correct.	Analysis, Evaluation	NA		
T0456	Develop secure software testing and validation procedures.	Application	1.1	2	30% or.3
T0457	Develop system testing and validation procedures, programming, and documentation.	Application	NA		

NCWF JOB ROLE

Secure Software Assessor

Job Role Description: A Secure Software Assessor analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Secure Software Assessor. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
T0516	Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.	Evaluation	1 - 9	4	100% or 1
T0554	Determine and document software patches or the extent of releases that would leave software vulnerable.	Analysis	NA		
	Summary			**3**	**20% or .2**

NCWF JOB ROLE

Secure Software Assessor

Job Role Description: A Secure Software Assessor analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Secure Software Assessor. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

KSA

ID	Statement	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	NA		
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.9	1	20% or .2
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	NA		
K0004	* Knowledge of cybersecurity principles.	1.1	1	20% or .2
K0005	* Knowledge of cyber threats and vulnerabilities.	1.6,1.7	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	NA		
K0014	Knowledge of complex data structures.	NA		
K0016	Knowledge of computer programming principles such as object-oriented design.	NA		
K0027	Knowledge of organization's enterprise information security architecture system.	NA		
K0028	Knowledge of organization's evaluation and validation requirements.	NA		
K0039	Knowledge of cybersecurity principles and methods that apply to software development.	1 - 9	3	75% or 0.75
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	1.1	1	20% or .2
K0051	Knowledge of low-level computer languages (e.g., assembly languages).	NA		
K0060	Knowledge of operating systems.	NA		
K0066	Knowledge of Privacy Impact Assessments.	NA		
K0068	Knowledge of programming language structures and logic.	NA		
K0073	Knowledge of secure configuration management techniques.	9.1 - 9.9	3	80% or .8
K0079	Knowledge of software debugging principles.	NA		
K0080	Knowledge of software design tools, methods, and techniques.	NA		
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	NA		

NCWF JOB ROLE

Secure Software Assessor

Job Role Description: A Secure Software Assessor analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Secure Software Assessor. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

KSA

ID	Statement	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
K0082	Knowledge of software engineering.	NA		
K0084	Knowledge of structured analysis principles and methods.	NA		
K0085	Knowledge of system and application security threats and vulnerabilities.	1.6,1.7	4	100% or 1
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	9.12	3	50% or .5
K0105	Knowledge of web services, including service-oriented architecture, Simple Object Access Protocol, and web service description language.	NA		
K0139	Knowledge of interpreted and compiled computer languages.	NA		
K0140	Knowledge of secure coding techniques.	1 - 9	4	100% or 1
K0152	Knowledge of software related information technology (IT) security principles and methods (e.g., modularization, layering, abstraction, data hiding, simplicity/minimization).	1.11	2	20% or .2
K0153	Knowledge of software quality assurance process.	1.1	1	20% or .2
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	NA		
K0178	Knowledge of secure software deployment methodologies, tools, and practices.	1 - 9	3	80% or .8
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	NA		
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	NA		
K0202	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).	NA		

NCWF JOB ROLE

Secure Software Assessor

Job Role Description: A Secure Software Assessor analyzes the security of new or existing computer applications, software, or specialized utility programs and provides actionable results.

Maps To: Certified Application Security Engineer (CASE)

Mapping Summary: Performance-based learning and evaluation in CASE imparts specific KSAs that should be demonstrated by a Secure Software Assessor. CASE maps to this job role at a Specialist level (level 3) with a correlation coefficient of .2 on the Framework tasks and a correlation coefficient of .2 on the KSA proficiency descriptions.

KSA

ID	Statement	CASE Exam Objectives	NICE Proficiency	Relational Coefficient
K0219	Knowledge of local area network (LAN) and wide area network (WAN) principles.	NA		
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	NA		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	NA		
K0262	Knowledge of Personal Health Information (PHI) data security standards.	NA		
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	NA		
K0322	Knowledge of embedded systems.	NA		
K0342	Knowledge of penetration testing principles, tools, and techniques.	NA		
K0343	Knowledge of root cause analysis techniques.	NA		
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	NA		
S0022	Skill in designing countermeasures to identified security risks.	1 - 9	3	80% or .8
S0031	Skill in developing and applying security system access controls.	8.11	2	20% or .2
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	NA		
S0083	Skill in integrating black box security testing tools into quality assurance process of software releases.	NA		
S0135	Skill in secure test plan design (e. g. unit, integration, system, acceptance).	1.1	1	20% or .2
S0138	Skill in using Public-Key Infrastructure (PKI) encryption and digital signature capabilities into applications (e.g., S/MIME email, SSL traffic).	6.1 - 6.12	3	90% or .9
S0174	Skill in using code analysis tools.	9.12	2	30% or 0.3
S0175	Skill in performing root cause analysis.	NA		
A0021	Ability to use and understand complex mathematical concepts (e.g., discrete math).	NA		
	Summary		**2**	**20% or .2**

NCWF JOB ROLE

Enterprise Architect

Job Role Description: An Enterprise Architect develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Enterprise Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .6 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0051	Define appropriate levels of system availability based on critical system functions and ensure system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	Analysis, Define	13.1 to 13.10	3	75% or .75
T0084	Employ secure configuration management processes.	Employ	6.1 to 6.13, 7.1 to 7.12, 8.1 to 8.10, 9.1 to 9.11	4	100% or 1
T0090	Ensure acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.	Comply	6.1 to 6.13	3	95% or .95
T0108	Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Identify	1- 14	2	40% or .4
T0196	Provide advice on project costs, design concepts, or design changes.	Explain	NA		
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Explain, Analysis	12.2 to 12.5	3	80% or .8
T0307	Analyze candidate architectures, allocate security services, and select security mechanisms.	Analyze, Evaluate	1- 14	4	100% or 1
T0314	Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	Develop, Synthesis	6.1, 6.2	3	95% or .95
T0328	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.	Evaluate	5.9, 6.3, 9.10, 10.12, 12.6,13.9	3	80% or .8
T0338	Write detailed functional specifications that document the architecture development process.	Analyze, Synthesis	NA		

NCWF JOB ROLE

Enterprise Architect

Job Role Description: An Enterprise Architect develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Enterprise Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .6 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0427	Analyze user needs and requirements to plan architecture.	Analyze	NA		
T0440	Captures and integrates essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Identify, Application	13.1	2	20% or .2
T0448	Develop enterprise architecture or system components required to meet user needs.	Develop, Synthesis	NA		
T0473	Document and update as necessary all definition and architecture activities.	Application, Analysis	1- 14	2	20% or .2
T0517	Integrate results regarding the identification of gaps in security architecture.	Application, Analysis	NA		
T0521	Plan implementation strategy to ensure enterprise components can be integrated and aligned.	Analysis, Synthesis	1- 14	3	60% or .6
T0542	Translate proposed capabilities into technical requirements.	Translate	NA		
T0555	Document how the implementation of a new system or new interface between systems impacts the current and target environment including but not limited to security posture.	Analysis	NA		
T0557	Integrate key management functions as related to cyberspace.	Application, Analysis	1- 14	3	40% or .4
	Summary			**3**	**60% or .6**

NCWF JOB ROLE

Enterprise Architect

Job Role Description: An Enterprise Architect develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Enterprise Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .6 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.1, 1.2, 1.3	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.2, 12.3	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	1.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.1 - 2.7	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1, 2.2	3	95% or .95
K0024	Knowledge of database systems.	NA		
K0027	Knowledge of organization's enterprise information security architecture system.	1.6, 1.7, 1.8	3	60% or .6
K0028	Knowledge of organization's evaluation and validation requirements.	NA		
K0030	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware.	NA		
K0035	Knowledge of how system components are installed, integrated, and optimized.	NA		
K0037	Knowledge of the Security Assessment and Authorization process.	3.4, 12.6	2	50% or .5
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	1- 14	4	100% or 1
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	1.1, 3.1	4	100% or 1
K0052	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics.	NA		
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	3.2, 3.3, 3.4, 3.5	4	100% or 1
K0060	Knowledge of operating systems.	6.1, 6.2, 6.3, 6.6	2	25% or .25
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	1.1, 1.2, 1.3	4	100% or 1

NCWF JOB ROLE

Enterprise Architect

Job Role Description: An Enterprise Architect develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Enterprise Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .6 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0063	Knowledge of parallel and distributed computing concepts.	NA		
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	6.4	3	80% or .8
K0075	Knowledge of security system design tools, methods, and techniques.	1 - 14	4	100% or 1
K0082	Knowledge of software engineering.	NA		
K0091	Knowledge of systems testing and evaluation methods.	NA		
K0093	Knowledge of key telecommunications concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers).	NA		
K0102	Knowledge of the systems engineering process.	NA		
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	NA		
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1.1 - 1.7	4	100% or 1
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	1- 14	4	100% or 1
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	NA		
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	4.6	2	35% or .35
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	NA		
K0207	Knowledge of circuit analysis.	NA		
K0211	Knowledge of confidentiality, integrity, and availability requirements.	3.1	4	100% or 1
K0212	Knowledge of cybersecurity-enabled software products.	1 - 14	3	80% or .8

NCWF JOB ROLE

Enterprise Architect

Job Role Description: An Enterprise Architect develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Enterprise Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .6 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0214	Knowledge of the Risk Management Framework Assessment Methodology.	12.2 - 12.4	3	90% or .9
K0227	Knowledge of various types of computer architectures.	NA		
K0240	Knowledge of multi-level/security cross domain solutions.	1 - 14	3	65% or .65
K0264	Knowledge of program protection planning to include information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements.	NA		
K0275	Knowledge of configuration management techniques.	1 - 14	4	100% or 1
K0286	Knowledge of N-tiered typologies including server and client operating systems.	1.2	2	80% or .8
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	13.1	2	25% or .25
K0291	Knowledge of the enterprise information technology (IT) architectural concepts and patterns to include baseline and target architectures.	6.1, 6.2, 6.3	2	50% or .5
K0293	Knowledge of integrating the organization's goals and objectives into the architecture.	NA		
K0299	Knowledge in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	5.1 - 5.7	2	35% or .35
K0322	Knowledge of embedded systems.	NA		
K0323	Knowledge of system fault tolerance methodologies.	NA		
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	NA		
K0326	Knowledge of cybersecurity methods, such as firewalls, demilitarized zones, and encryption.	3.2, 3.5, 7.1 - 7.12,	4	100% or 1
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	1.3	4	100% or 1
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs.	1 - 14	3	95% or .95

NCWF JOB ROLE

Enterprise Architect

Job Role Description: An Enterprise Architect develops and maintains business, systems, and information processes to support enterprise mission needs; develops information technology (IT) rules and requirements that describe baseline and target architectures.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Enterprise Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .6 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
S0005	Skill in applying and incorporating information technologies into proposed solutions.	1- 14	3	60% or .6
S0024	Skill in designing the integration of hardware and software solutions.	1- 14	2	50% or .5
S0050	Skill in design modeling and building use cases (e.g., unified modeling language).	NA		
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	NA		
S0099	Skill in determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes.	5.1 - 5.7	2	50% or .5
S0122	Skill in the use of design methods.	1- 14	2	80% or .8
A0008	Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).	1 - 14	3	80% or .8
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	6.4, 12.6	4	95% or .95
A0027	Ability to apply an organization's goals and objectives to develop and maintain architecture.	1 - 14	3	80% or .8
A0038	Ability to optimize systems to meet enterprise performance requirements.	6.1 - 6.3	3	50% or .5
A0051	Ability to execute technology integration processes.	1 - 14	3	50% or .5
A0060	Ability to build architectures and frameworks.	1 - 14	3	50% or .5
	Summary		**3**	**50% or .5**

NCWF JOB ROLE

Security Architect

Job Role Description: A Security Architect designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Security Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .7 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0050	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Define, Application	13.9,13.10	2	30% or .3
T0051	Define appropriate levels of system availability based on critical system functions and ensure system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	Define, Application	13.1 to 13.10	2	50% or .5
T0071	Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).	Develop, Evaluation, Synthesis	5.5, 13.1	4	100% or 1
T0082	Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition lifecycle.	Write, Analysis	1- 14	3	75% or .75
T0084	Employ secure configuration management processes.	Employ, Evaluation, Synthesis	1- 14	4	100% or 1
T0090	Ensure acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.	Compare, Analysis	1- 14	3	80% or .8
T0108	Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Identify, Application	1- 14	2	50% or .5
T0177	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Compile, Analysis	12.2	3	90% or .9
T0196	Provide advice on project costs, design concepts, or design changes.	Tell, Analysis	1- 14	3	50% or .5
T0203	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.	Tell, Application	1- 14	2	35% or .35

NCWF JOB ROLE

Security Architect

Job Role Description: A Security Architect designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Security Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .7 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Tell, Application	12.1 to 12.3	2	30% or .3
T0268	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.	Define, Application	2.1, 6.1 to 6.10	2	25% or .25
T0307	Analyze candidate architectures, allocate security services, and select security mechanisms.	Analyze, Evaluation, Synthesis	1- 14	4	80% or .8
T0314	Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	Develop, Evaluation, Synthesis	6.1, 6.2	4	95% or .95
T0328	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.	Evaluate, Evaluation, Synthesis	5.9, 6.3, 9.10, 10.12, 12.6,13.9	4	100% or 1
T0338	Write detailed functional specifications that document the architecture development process.	Write	NA		
T0427	Analyze user needs and requirements to plan architecture.	Analyze	NA		
T0448	Develop enterprise architecture or system components required to meet user needs.	Develop	NA		
T0473	Document and update as necessary all definition and architecture activities.	Write, Analysis	1- 14	3	80% or .8
T0484	Document the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.	Write, Evaluation, Synthesis	1- 14	4	100% or 1
T0542	Translate proposed capabilities into technical requirements.	Translate	NA		
T0556	Assess and design security management functions as related to cyberspace.	Assess, Evaluation, Synthesis	1- 14	4	100% or 1
	Summary			**3**	**70% or .7**

NCWF JOB ROLE

Security Architect

Job Role Description: A Security Architect designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Security Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .7 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.1, 1.2, 1.3	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.2,12.3	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	1.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.1 to 2.7	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1, 2.2	3	95% or .95
K0015	Knowledge of computer algorithms.	NA		
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	3.5	4	95% or .95
K0019	Knowledge of cryptography and cryptographic key management concepts.	3.5	4	95% or .95
K0024	Knowledge of database systems.	NA		
K0027	Knowledge of organization's enterprise information security architecture system.	1.6,1.7,1.8	3	90% or .9
K0030	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware.	NA		
K0035	Knowledge of how system components are installed, integrated, and optimized.	NA		
K0036	Knowledge of human-computer interaction principles.	NA		
K0037	Knowledge of the Security Assessment and Authorization process.	3.4,12.6	3	90% or .9
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	1- 14	3	80% or .8
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	1.1,3.1	4	80% or .8
K0052	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics.	NA		
K0055	Knowledge of microprocessors.	NA		

NCWF JOB ROLE

Security Architect

Job Role Description: A Security Architect designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Security Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .7 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	3.2, 3.3,3.4,3.5	4	100% or 1
K0060	Knowledge of operating systems.	6.1,6.2,6.3, 6.6	3	30% or .3
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	1.1,1.2,1.3	3	90% or .9
K0063	Knowledge of parallel and distributed computing concepts.	NA		
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	6.4	3	50% or .5
K0082	Knowledge of software engineering.	NA		
K0091	Knowledge of systems testing and evaluation methods.	NA		
K0092	Knowledge of technology integration processes.	NA		
K0093	Knowledge of key telecommunications concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers).	NA		
K0102	Knowledge of the systems engineering process.	NA		
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	NA		
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	1- 14	4	100% or 1
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	NA		
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	4.6	3	80% or .8
K0207	Knowledge of circuit analysis.	NA		
K0211	Knowledge of confidentiality, integrity, and availability requirements.	3.1	4	100% or 1

NCWF JOB ROLE

Security Architect

Job Role Description: A Security Architect designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Security Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .7 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0212	Knowledge of cybersecurity-enabled software products.	1- 14	3	50% or .5
K0214	Knowledge of the Risk Management Framework Assessment Methodology.	12.2 to 12.4	2	75% or .75
K0227	Knowledge of various types of computer architectures.	NA		
K0240	Knowledge of multi-level/security cross domain solutions.	1- 14	4	100% or 1
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	4.6	2	30% or .3
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	4.6	2	50% or .5
K0262	Knowledge of Personal Health Information (PHI) data security standards.	NA		
K0264	Knowledge of program protection planning to include information technology (IT) supply chain security/risk management policies, anti-tampering techniques, and requirements.	NA		
K0275	Knowledge of configuration management techniques.	1- 14	4	100% or 1
K0286	Knowledge of N-tiered typologies including server and client operating systems.	1.2	2	25% or .25
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	5.5, 13.1	3	70% or .7
K0291	Knowledge of the enterprise information technology (IT) architectural concepts and patterns to include baseline and target architectures.	6.1,6.2,6.3	4	70% or .7
K0293	Knowledge of integrating the organization's goals and objectives into the architecture.	NA		
K0320	Knowledge of organization's evaluation and validation criteria.	NA		
K0322	Knowledge of embedded systems.	NA		
K0323	Knowledge of system fault tolerance methodologies.	NA		
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	NA		
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	1.3	4	100% or 1

NCWF JOB ROLE

Security Architect

Job Role Description: A Security Architect designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Security Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .7 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs.	1- 14	4	100% or 1
K0336	Knowledge of access authentication methods.	3.4, 5.4	4	100% or 1
S0005	Skill in applying and incorporating information technologies into proposed solutions.	1- 14	4	80% or .8
S0024	Skill in designing the integration of hardware and software solutions.	1- 14	3	60% or .6
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	5.1 to 5.7	3	50% or .5
S0050	Skill in design modeling and building use cases (e.g., unified modeling language).	NA		
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	NA		
S0099	Skill in determining how a security system should work and how changes in conditions, operations, or the environment will affect these outcomes.	5.1 to 5.7	3	50% or .5
S0116	Skill in designing multi-level security/cross domain solutions.	1- 14	4	80% or .8
S0122	Skill in the use of design methods.	1- 14	3	55% or .55
S0139	Skill in applying security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	NA		
S0152	Skill in translating operational requirements into protection needs (i.e., security controls).	1- 14	4	100% or 1
S0168	Skill in applying cybersecurity methods, such as firewalls, demilitarized zones, and encryption.	3.2, 3.5, 7.1 to 7.12,	4	100% or 1
A0008	Ability to apply the methods, standards, and approaches for describing, analyzing, and documenting an organization's enterprise information technology (IT) architecture (e.g., Open Group Architecture Framework [TOGAF], Department of Defense Architecture Framework [DoDAF], Federal Enterprise Architecture Framework [FEAF]).	1- 14	3	70% or .7
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	12.6	4	100% or 1
A0027	Ability to apply an organization's goals and objectives to develop and maintain architecture.	1- 14	3	80% or .8
A0038	Ability to optimize systems to meet enterprise performance requirements.	6.1 to 6.3	3	50% or .5

NCWF JOB ROLE

Security Architect

Job Role Description: A Security Architect designs enterprise and systems security throughout the development life cycle; translates technology and environmental conditions (e.g., law and regulation) into security designs and processes.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Security Architect. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .7 on the Framework tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
A0048	Ability to apply network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1.1 to 1.7	4	100% or 1
A0049	Ability to apply secure system design tools, methods and techniques.	1- 14	4	100% or 1
A0050	Ability to apply system design tools, methods, and techniques, including automated systems analysis and design tools.	1- 14	4	100% or 1
A0061	Ability to design architectures and frameworks.	1- 14	4	80% or .8
	Summary		**3**	**50% or .5**

NCWF JOB ROLE

Research & Development Specialist

Job Role Description: A Research & Development Specialist conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Research & Development Specialist. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .75 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
T0064	Review and validate data mining and data warehousing programs, processes, and requirements.	Validate	N/A		
T0249	Research current technology to understand capabilities of required system or network.	Identify, Analyze	1.1	3	90% or .9
T0250	Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.		N/A		
T0283	Collaborate with stakeholders to identify and/or develop appropriate solutions technology.	Identify	6.7, 16.2	3	90% or .9
T0284	Design and develop new tools/technologies as related to cybersecurity.	Design	2.12, 3.4, 6.7, 7.7, 8.6, 9.6, 11.7, 12.6, 13.7, 14.8, 15.6, 15.7, 16.2, 17.5	4	100% or 1
T0327	Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.	Evaluate	1.10, 3.7	3	90% or .9
T0329	Follow software and systems engineering life cycle standards and processes.		N/A		
T0409	Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases.		N/A		
T0410	Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities.	Identify	1.6, 1.10	3	90% or .9
T0411	Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.	Identify	1.10, 3.7	3	90% or .9
T0413	Develop data management capabilities (e.g., cloud based, centralized cryptographic key management) to include support to the mobile workforce.	Develop, Synthesis	17.1, 17.4, 17.5, 18.4, 18.5, 15.6, 15.7	4	100% or 1
T0547	Research and evaluate available technologies and standards to meet customer requirements.	Evaluate	1.1, 1.11	3	90% or .9
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

Research & Development Specialist

Job Role Description: A Research & Development Specialist conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Research & Development Specialist. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .75 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	3 - 18	3	80% or .8
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.9	2	60% or .6
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	100% or 1
K0004	* Knowledge of cybersecurity principles.	1.2	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	100% or 1
K0009	Knowledge of application vulnerabilities.	1.1	4	100% or 1
K0019	Knowledge of cryptography and cryptographic key management concepts.	18.1	4	100% or 1
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	1.1	4	100% or 1
K0090	Knowledge of system life cycle management principles, including software security and usability.	N/A		
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	1.9	2	60% or .6
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	1.6	3	90% or .9
K0171	Knowledge of hardware reverse engineering techniques.	N/A		
K0172	Knowledge of middleware (e.g., enterprise service bus and message queuing).	N/A		
K0173	Withdrawn – Integrated into K0499			
K0174	Knowledge of networking protocols.	3 - 18	3	80% or .8
K0175	Knowledge of software reverse engineering techniques.	N/A		
K0176	Knowledge of Extensible Markup Language (XML) schemas.	12.1, 12.3	3	90% or .9

NCWF JOB ROLE

Research & Development Specialist

Job Role Description: A Research & Development Specialist conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Research & Development Specialist. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .75 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1.2, 1.6	3	90% or .9
K0202	Knowledge of the application firewall concepts and functions (e.g., Single point of authentication/audit/policy enforcement, message scanning for malicious content, data anonymization for PCI and PII compliance, data loss protection scanning, accelerated cryptographic operations, SSL security, REST/JSON processing).	16.1, 16.2	3	90% or .9
K0209	Knowledge of covert communication techniques.	5.6, 5.7	3	90% or .9
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	1.7, 1.11	4	100% or 1
K0268	Knowledge of forensic footprint identification.	2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11	4	100% or 1
K0269	Knowledge of mobile communications architecture.	15.2, 15.3, 15.4, 15.5	4	100% or 1
K0271	Knowledge of operating system structures and internals (e.g., process management, directory structure, installed applications).	N/A		
K0272	Knowledge of network analysis tools used to identify software communications vulnerabilities.	1.10, 3.7, 12.6, 14.8	4	100% or 1
K0288	Knowledge of industry standard security models.	NA		
K0296	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	11.2	3	90% or .9
K0310	Knowledge of hacking methodologies.	1.4	4	100% or 1
K0314	Knowledge of industry technologies and how differences affect exploitation/vulnerabilities.	1.10	4	100% or 1
K0321	Knowledge of engineering concepts as applied to computer architecture and associated computer hardware/ software.	N/A		

NCWF JOB ROLE

Research & Development Specialist

Job Role Description: A Research & Development Specialist conducts software and systems engineering and software systems research in order to develop new capabilities, ensuring cybersecurity is fully integrated. Conducts comprehensive technology research to evaluate potential vulnerabilities in cyberspace systems.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Research & Development Specialist. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .75 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0342	Knowledge of penetration testing principles, tools, and techniques.	1.10, 2.14, 3.11, 4.8, 5.8, 6.8, 7.10, 8.7, 9.7, 10.6, 11.8, 12.7, 14.9, 15.8, 16.8, 17.6	4	100% or 1
S0005	Skill in applying and incorporating information technologies into proposed solutions.	1.1, 1.6, 1.11	4	100% or 1
S0017	Skill in creating and utilizing mathematical or statistical models.	1.6	4	100% or 1
S0072	Skill in using scientific rules and methods to solve problems.	1.6	4	100% or 1
S0140	Skill in applying the systems engineering process.	N/A		
S0148	Skill in designing the integration of technology processes and solutions, including legacy systems and modern programming languages.	2.12, 3.4, 6.7, 7.7, 8.6, 9.6, 11.7, 12.6, 13.7, 14.8, 15.6, 15.7, 16.2, 17.5	4	100% or 1
S0172	Skill in applying secure coding techniques.	13.1, 13.3	4	100% or 1
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	1.10, 3.7	4	100% or 1
A0018	Ability to prepare and present briefings.	1 - 18	4	100% or 1
A0019	Ability to produce technical documentation.	1 - 18	4	100% or 1
	Summary		**4**	**75% or .75**

NCWF JOB ROLE

Systems Requirements Planner

Job Role Description: A Systems Requirements Planner consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Requirements Planner. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and .6 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0033	Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.	Create	12.1 - 12.4	2	40% or .4
T0039	Consult with customers to evaluate functional requirements.	Evaluate	NA		
T0045	Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions.	Discuss	NA		
T0052	Define project scope and objectives based on customer requirements.	Define	NA		
T0062	Develop and document requirements, capabilities, and constraints for design procedures and processes.	Develop	1 - 14	2	30% or .3
T0127	Integrate and align information security and/or cybersecurity policies to ensure system analysis meets security requirements.	Apply	4.1 - 4.4	4	80% or .8
T0156	Oversee and make recommendations regarding configuration management.	Inspect	1 - 14	4	85% or .85
T0174	Perform needs analysis to determine opportunities for new and improved business process solutions.	Compile	1 - 14	2	40% or .4
T0191	Prepare use cases to justify the need for specific information technology (IT) solutions.	Compile	NA		
T0235	Translate functional requirements into technical solutions.	Translate	NA		
T0273	Develop and document supply chain risks for critical system elements, as appropriate.	Develop	NA		
T0300	Develop and document User Experience (UX) requirements including information architecture and user interface requirements.	Develop	NA		
T0313	Design and document quality standards.	Design	4.6	2	30% or .3
T0325	Document a system's purpose and preliminary system security concept of operations.	Write	6.1 - 6.13	4	80% or .8

NCWF JOB ROLE

Systems Requirements Planner

Job Role Description: A Systems Requirements Planner consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Requirements Planner. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and .6 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0334	Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware).	Integrate	1 - 14	4	70% or .7
T0454	Define baseline security requirements in accordance with applicable guidelines.	Define	6.1 - 6.3	4	95% or .95
T0463	Develop cost estimates for new or modified system(s).	Develop	NA		
T0497	Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements.	Manage	NA		
	Summary			**3**	**30% or .3**

NCWF JOB ROLE

Systems Requirements Planner

Job Role Description: A Systems Requirements Planner consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Requirements Planner. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and .6 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.1 - 1.3	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.2 - 12.4	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	3.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.1 - 2.7	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1	3	95% or .95
K0008	Knowledge of applicable business processes and operations of customer organizations.	NA		
K0012	Knowledge of capabilities and requirements analysis.	NA		
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	3.5	4	95% or .95
K0019	Knowledge of cryptography and cryptographic key management concepts.	3.5	4	95% or .95
K0032	Knowledge of fault tolerance.	NA		
K0035	Knowledge of how system components are installed, integrated, and optimized.	1 - 14	4	90% or .9
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	1 - 14	4	95% or .95
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	4.6	4	90% or .9
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	3.1	4	90% or .9
K0045	Knowledge of information security systems engineering principles.	NA		
K0047	Knowledge of information technology (IT) architectural concepts and frameworks.	1 - 14	3	45% or .45
K0055	Knowledge of microprocessors.	NA		

NCWF JOB ROLE

Systems Requirements Planner

Job Role Description: A Systems Requirements Planner consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Requirements Planner. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and .6 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	3.1 - 3.5	4	100% or 1
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	1 - 14	4	80% or .8
K0060	Knowledge of operating systems.	6.1 - 6.6	2	35% or .35
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	1.1 - 1.3	4	95% or .95
K0063	Knowledge of parallel and distributed computing concepts.	NA		
K0066	Knowledge of Privacy Impact Assessments.	2.1		
K0067	Knowledge of process engineering concepts.	NA		
K0073	Knowledge of secure configuration management techniques.	1 - 14	4	95% or .95
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	1 - 14	4	95% or .95
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	1 - 14	4	95% or .95
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	4.6	3	55% or .55
K0090	Knowledge of system life cycle management principles, including software security and usability.	6.11	3	50% or .5
K0091	Knowledge of systems testing and evaluation methods.	6.1 - 6.5	3	35% or .35
K0093	Knowledge of key telecommunications concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers).	NA		
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	1.1 - 1.8, 3.1 - 3.8	3	65% or .65
K0102	Knowledge of the systems engineering process.	NA		
K0163	Knowledge of critical information technology (IT) procurement requirements.	NA		

NCWF JOB ROLE

Systems Requirements Planner

Job Role Description: A Systems Requirements Planner consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Requirements Planner. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and .6 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0164	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	NA		
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	4.6	3	65% or .65
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	NA		
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	6.1 - 6.10	3	35% or .35
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	1 - 14	4	100% or 1
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	1 - 14	4	90% or .9
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	4.6	4	90% or .9
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	5.5,13.1	3	45% or .45
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	NA		
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	1.3	4	100% or 1
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs.	1 - 14	4	100% or 1
S0005	Skill in applying and incorporating information technologies into proposed solutions.	1 - 14	4	90% or .9
S0006	Skill in applying confidentiality, integrity, and availability principles.	3.1	4	100% or 1

NCWF JOB ROLE

Systems Requirements Planner

Job Role Description: A Systems Requirements Planner consults with customers to evaluate functional requirements and translate functional requirements into technical solutions.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Requirements Planner. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and .6 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
S0008	Skill in applying organization-specific systems analysis principles and techniques.	6.1 - 6.10	4	95% or .95
S0010	Skill in conducting capabilities and requirements analysis.	NA		
S0050	Skill in design modeling and building use cases (e.g., unified modeling language).	NA		
S0134	Skill in conducting reviews of systems.	6.1 - 6.10	4	90% or .9
A0064	Ability to interpret and translate customer requirements into operational capabilities.	NA		
	Summary		**3**	**60% or .6**

NCWF JOB ROLE

System Testing and Evaluation Specialist

Job Role Description: A System Testing and Evaluation Specialist plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a System Testing and Evaluation Specialist. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .1 on the framework Tasks and .45 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0058	Determine level of assurance of developed capabilities based on test results.	Determine	NA		
T0080	Develop test plans to address specifications and requirements.	Develop	NA		
T0143	Make recommendations based on test results.	Recommend	12.6	3	30% or .3
T0257	Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated.	Determine	NA		
T0274	Create auditable evidence of security measures.	Create	NA		
T0393	Validate specifications and requirements for testability.	Test	NA		
T0426	Analyze the results of software, hardware, or interoperability testing.	Analyze	NA		
T0511	Perform developmental testing on systems under development.	Perform	NA		
T0512	Perform interoperability testing on systems exchanging electronic information with other systems.	Perform	NA		
T0513	Perform operational testing.	Perform	NA		
T0539	Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.	Test	6.1 - 6.4,12.6	4	95% or .95
T0540	Record and manage test data.	Record	12.6	3	30% or .3
	Summary			**3**	**10% or .1**

NCWF JOB ROLE

System Testing and Evaluation Specialist

Job Role Description: A System Testing and Evaluation Specialist plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a System Testing and Evaluation Specialist. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .1 on the framework Tasks and .45 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.1 - 1.3	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.2 - 12.4	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	3.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.1,2.2,2.3	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1	3	95% or .95
K0027	Knowledge of organization's enterprise information security architecture system.	1 - 14	4	90% or .9
K0028	Knowledge of organization's evaluation and validation requirements.	NA		
K0037	Knowledge of the Security Assessment and Authorization process.	3.4, 12.6	4	90% or .9
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	3.1	4	100% or 1
K0057	Knowledge of network hardware devices and functions.	3.7	4	100% or 1
K0088	Knowledge of systems administration concepts.	1.4, 6.1 - 6.10	4	50% or .5
K0102	Knowledge of the systems engineering process.	NA		
K0139	Knowledge of interpreted and compiled computer languages.	NA		
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	NA		
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	6.1 - 6.10	3	50% or .5
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1 - 14	4	100% or 1
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	1.1 - 1.8	3	50% or .5

NCWF JOB ROLE

System Testing and Evaluation Specialist

Job Role Description: A System Testing and Evaluation Specialist plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a System Testing and Evaluation Specialist. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .1 on the framework Tasks and .45 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	NA		
K0212	Knowledge of cybersecurity-enabled software products.	1 - 14	3	80% or .8
K0250	Knowledge of Test & Evaluation processes.	1 - 14	3	50% or .5
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	NA		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	4.6	4	60% or .6
K0262	Knowledge of Personal Health Information (PHI) data security standards.	NA		
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	5.5	3	45% or .45
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	1.3	4	100% or 1
S0015	Skill in conducting test events.	6.2, 12.6	2	35% or .35
S0021	Skill in designing a data analysis structure (i.e., the types of data your test must generate and how to analyze those data).	NA		
S0026	Skill in determining an appropriate level of test rigor for a given system.	6.2	2	25% or .25
S0030	Skill in developing operations-based testing scenarios.	NA		
S0048	Skill in systems integration testing.	NA		
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	NA		
S0061	Skill in writing test plans.	NA		
S0082	Skill in evaluating test plans for applicability and completeness.	NA		
S0104	Skill in conducting Test Readiness Reviews.	NA		
S0107	Skill in designing and documenting overall program Test & Evaluation strategies.	NA		
S0110	Skill in identifying Test & Evaluation infrastructure (people, ranges, tools, instrumentation) requirements.	NA		

NCWF JOB ROLE

System Testing and Evaluation Specialist

Job Role Description: A System Testing and Evaluation Specialist plans, prepares, and executes tests of systems to evaluate results against specifications and requirements as well as analyze/report test results.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a System Testing and Evaluation Specialist. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .1 on the framework Tasks and .45 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
S0112	Skill in managing test assets, test resources, and test personnel to ensure effective completion of test events.	NA		
S0115	Skill in preparing Test & Evaluation reports.	12.6	3	75% or .75
S0117	Skill in providing Test & Evaluation resource estimate.	NA		
A0026	Ability to analyze test data.	12.6	3	75% or .75
A0030	Ability to collect, verify, and validate test data.	12.6	3	75% or .75
A0040	Ability to translate data and test results into evaluative conclusions.	12.6	3	75% or .75
	Summary		**3**	**45% or .45**

NCWF JOB ROLE

Information Systems Security Developer

Job Role Description: An Information Systems Security Developer designs, develops, tests, and evaluates information system security throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Information Systems Security Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .35 on the framework Tasks and .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0012	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider lifecycle support.	Analyze	NA		
T0015	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Apply	NA		
T0018	Assess the effectiveness of cybersecurity measures utilized by system(s).	Assess	6.1 - 6.10	3	80% or .80
T0019	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	Assess	2.1 - 2.7	4	90% or .90
T0021	Build, test, and modify product prototypes using working models or theoretical models.	Build	NA		
T0032	Conduct Privacy Impact Assessments (PIA) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Conduct	NA		
T0053	Design and develop cybersecurity or cybersecurity-enabled products.	Design	NA		
T0055	Design hardware, operating systems, and software applications to adequately address cybersecurity requirements.	Design	1 -14	4	100% or 1
T0056	Design or integrate appropriate data backup capabilities into overall system designs, and ensure appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Design	13.1 - 13.7	4	95% or .95
T0061	Develop and direct system testing and validation procedures and documentation.	Develop	6.1 - 6.4, 12.6	2	35% or .35
T0069	Develop detailed security design documentation for component and interface specifications to support system design and development.	Develop	NA		
T0070	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Develop	13.9,13.10	2	30% or .30

NCWF JOB ROLE

Information Systems Security Developer

Job Role Description: An Information Systems Security Developer designs, develops, tests, and evaluates information system security throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Information Systems Security Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .35 on the framework Tasks and .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0076	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.	Develop	12.1 - 12.4	3	60% or .60
T0078	Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications.	Develop	6.1 - 6.10, 12.1 - 12.4	4	75% or .75
T0105	Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements.	Identify	1 -14	3	50% or .50
T0107	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable).	Identify	1.4	2	20% or .20
T0109	Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.	Identify	NA		
T0119	Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.	Identify	1 -14	3	80% or .80
T0122	Implement security designs for new or existing system(s).	Implement	1 -14	3	60% or .60
T0124	Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).	Implement	12.5,12.6	4	60% or .60
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Perform	12.2 - 12.4	4	60% or .60
T0201	Provide guidelines for implementing developed systems to customers or installation teams.	Provide	NA		

NCWF JOB ROLE

Information Systems Security Developer

Job Role Description: An Information Systems Security Developer designs, develops, tests, and evaluates information system security throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Information Systems Security Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .35 on the framework Tasks and .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Provide	12.2 - 12.4	3	45% or .45
T0228	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Operate	NA		
T0231	Provide support to security/certification test and evaluation activities.	Provide	NA		
T0242	Utilize models and simulations to analyze or predict system performance under different operating conditions.	Analyze	NA		
T0269	Design and develop key management functions (as related to cybersecurity).	Design	NA		
T0270	Analyze user needs and requirements to plan and conduct system security development.	Analyze	NA		
T0271	Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	Develop	5.1 - 5.8	3	80% or .80
T0272	Ensure security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.	Write	1 -14	3	55% or .55
T0304	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	Implement	NA		
T0326	Employ configuration management processes.	Employ	1 -14	4	85% or .85
T0359	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	Design	1 -14	2	35% or .35
T0446	Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.	Design	3.1	3	75% or .75

NCWF JOB ROLE

Information Systems Security Developer

Job Role Description: An Information Systems Security Developer designs, develops, tests, and evaluates information system security throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Information Systems Security Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .35 on the framework Tasks and .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0449	Design to security requirements to ensure requirements are met for all systems and/or applications.	Design	NA		
T0466	Develop mitigation strategies to address cost, schedule, performance, and security risks.	Develop	1 -14	2	30% or .30
T0509	Perform an information security risk assessment.	Perform	12.1 - 12.4	4	60% or .60
T0518	Perform security reviews and identify security gaps in architecture.	Perform	1 -14	3	45% or .45
T0527	Provide input to implementation plans and standard operating procedures as they relate to information systems security.	Provide	1 -14	3	45% or .45
T0541	Trace system requirements to design components and perform gap analysis.	Evaluate	NA		
T0544	Verify stability, interoperability, portability, and/or scalability of system architecture.	Test	NA		
	Summary			**3**	**35% or .35**

NCWF JOB ROLE

Information Systems Security Developer

Job Role Description: An Information Systems Security Developer designs, develops, tests, and evaluates information system security throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Information Systems Security Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .35 on the framework Tasks and .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.1 - 1.4	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.1 - 12.4	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	3.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.1 - 2.4	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1	3	95% or .95
K0015	Knowledge of computer algorithms.	NA		
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	3.5	4	70% or .70
K0024	Knowledge of database systems.	NA		
K0027	Knowledge of organization's enterprise information security architecture system.	1 -14	4	70% or .70
K0028	Knowledge of organization's evaluation and validation requirements.	NA		
K0030	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware.	NA		
K0032	Knowledge of fault tolerance.	NA		
K0035	Knowledge of how system components are installed, integrated, and optimized.	1 -14	3	80% or .80
K0036	Knowledge of human-computer interaction principles.	NA		
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	3.1	4	95% or .95
K0045	Knowledge of information security systems engineering principles.	NA		
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	3.2 - 3.5	4	100% or 1

NCWF JOB ROLE

Information Systems Security Developer

Job Role Description: An Information Systems Security Developer designs, develops, tests, and evaluates information system security throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Information Systems Security Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .35 on the framework Tasks and .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	1.1 - 1.4	4	100% or 1
K0052	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics.	NA		
K0055	Knowledge of microprocessors.	NA		
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	3.2 - 3.5	4	100% or 1
K0060	Knowledge of operating systems.	6.1 - 6.5	3	25% or .25
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	1.1 - 1.5	4	100% or 1
K0063	Knowledge of parallel and distributed computing concepts.	NA		
K0065	Knowledge of policy-based and risk adaptive access controls.	3.3	4	100% or 1
K0066	Knowledge of Privacy Impact Assessments.	2.1	3	85% or .85
K0067	Knowledge of process engineering concepts.	NA		
K0073	Knowledge of secure configuration management techniques.	1 -14	4	90% or .90
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	NA		
K0082	Knowledge of software engineering.	NA		
K0084	Knowledge of structured analysis principles and methods.	NA		
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	1 -14	3	85% or .85
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	1 -14	3	85% or .85
K0090	Knowledge of system life cycle management principles, including software security and usability.	NA		
K0091	Knowledge of systems testing and evaluation methods.	NA		

NCWF JOB ROLE

Information Systems Security Developer

Job Role Description: An Information Systems Security Developer designs, develops, tests, and evaluates information system security throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Information Systems Security Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .35 on the framework Tasks and .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0093	Knowledge of key telecommunications concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers).	NA		
K0102	Knowledge of the systems engineering process.	NA		
K0139	Knowledge of interpreted and compiled computer languages.	NA		
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	NA		
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	6.1 - 6.10	3	60% or .60
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1.1 - 1.8	4	100% or 1
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	1 -14	4	85% or .85
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	1 -14	3	60% or .60
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	NA		
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	NA		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	4.6	3	70% or .70
K0262	Knowledge of Personal Health Information (PHI) data security standards.	NA		
K0276	Knowledge of security management.	1 -14	4	85% or .85
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	5.5	3	45% or .45
K0297	Knowledge of countermeasure design for identified security risks.	1 -14	4	80% or .80
K0308	Knowledge of cryptology.	3.5	4	80% or .80

NCWF JOB ROLE

Information Systems Security Developer

Job Role Description: An Information Systems Security Developer designs, develops, tests, and evaluates information system security throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by an Information Systems Security Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .35 on the framework Tasks and .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0322	Knowledge of embedded systems.	NA		
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	NA		
K0331	Knowledge of network protocols (e.g., Transmission Critical Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP)), and directory services (e.g., Domain Name System (DNS)).	1.3	4	80% or .80
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs.	1 -14	3	70% or .70
K0336	Knowledge of access authentication methods.	3.3,3.4	4	85% or .85
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	6.1 - 6.5,12.6	4	100% or 1
S0022	Skill in designing countermeasures to identified security risks.	1 -14	4	85% or .85
S0023	Skill in designing security controls based on cybersecurity principles and tenets.	1 -14	4	85% or .85
S0024	Skill in designing the integration of hardware and software solutions.	1 -14	4	85% or .85
S0031	Skill in developing and applying security system access controls.	3.1 - 3.4	4	85% or .85
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	1 -14	4	85% or .85
S0036	Skill in evaluating the adequacy of security designs.	1 -14	4	85% or .85
S0085	Skill in conducting audits or reviews of technical systems.	1 -14	4	85% or .85
S0145	Skill in integrating and applying policies that meet system security objectives.	4.1 - 4.4	4	85% or .85
S0160	Skill in the use of design modeling (e.g., unified modeling language).	NA		
	Summary		**4**	**50% or .5**

NCWF JOB ROLE

Systems Developer

Job Role Description: A Systems Developer designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0012	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider lifecycle support.	Analyze	1 - 14	2	25% or .25
T0021	Build, test, and modify product prototypes using working models or theoretical models.	Build	NA		
T0053	Design and develop cybersecurity or cybersecurity-enabled products.	Design	NA		
T0056	Design or integrate appropriate data backup capabilities into overall system designs, and ensure appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Design	13.1 - 13.8	4	95% or .95
T0061	Develop and direct system testing and validation procedures and documentation.	Develop	NA		
T0067	Develop architectures or system components consistent with technical specifications.	Develop	1 - 14	3	60% or .6
T0070	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Develop	NA		
T0107	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable).	Identify	NA		
T0109	Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.	Identify	13.9,13.10	2	30% or .3
T0119	Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.	Identify	1 - 14	3	75% or .75
T0181	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Perform	12.2 - 12.6	4	80% or .8

NCWF JOB ROLE

Systems Developer

Job Role Description: A Systems Developer designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0201	Provide guidelines for implementing developed systems to customers or installation teams.	Provide	NA		
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Provide	12.2 - 12.4	3	45% or .45
T0228	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Manipulate	NA	3	45% or .45
T0242	Utilize models and simulations to analyze or predict system performance under different operating conditions.	Analyze	NA		
T0304	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	Implement	NA		
T0326	Employ configuration management processes.	Employ	1 - 14	4	85% or .85
T0350	Conduct a market analysis to identify, assess, and recommend commercial, GOTS, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.	Conduct	NA		
T0358	Design and develop system administration and management functionality for privileged access users.	Design	1 - 14	3	45% or .45
T0359	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	Design	1 - 14	3	45% or .45
T0378	Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle).	Implement	12.1 - 12.4	3	35% or .35
T0406	Ensure design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.	Write	NA		
T0447	Design hardware, operating systems, and software applications to adequately address requirements.	Design	1 - 14	3	60% or .6

NCWF JOB ROLE

Systems Developer

Job Role Description: A Systems Developer designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0449	Design to security requirements to ensure requirements are met for all systems and/or applications.	Design	1 - 14	3	30% or .3
T0464	Develop detailed design documentation for component and interface specifications to support system design and development.	Develop	NA		
T0466	Develop mitigation strategies to address cost, schedule, performance, and security risks.	Develop	NA		
T0480	Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements.	Identify	NA		
T0488	Implement designs for new or existing system(s).	Implement	NA		
T0518	Perform security reviews and identify security gaps in architecture.	Perform	1 - 14	3	80% or .8
T0528	Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials	Provide	NA		
T0538	Provide support to test and evaluation activities.	Provide	NA		
T0541	Trace system requirements to design components and perform gap analysis.	Validate	1 - 14	2	30% or .3
T0544	Verify stability, interoperability, portability, and/or scalability of system architecture.	Test	1 - 14	3	50% or .5
T0558	Analyze user needs and requirements to plan and conduct system development.	Analyze	NA		
T0559	Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations.	Develop	5.1 - 5.7	4	60% or .6
T0560	Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/ processing of multiple classification levels, and processing Sensitive Compartmented Information).	Support	5.1 - 5.7	4	60% or .6
	Summary			**3**	**30% or .3**

NCWF JOB ROLE

Systems Developer

Job Role Description: A Systems Developer designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.1 - 1.4	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.2 - 12.5	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	3.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.1 - 2.4	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1	3	95% or .95
K0015	Knowledge of computer algorithms.	NA		
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	3.5	4	80% or .8
K0024	Knowledge of database systems.	NA		
K0027	Knowledge of organization's enterprise information security architecture system.	1 - 14	4	60% or .6
K0028	Knowledge of organization's evaluation and validation requirements.	NA		
K0030	Knowledge of electrical engineering as applied to computer architecture, including circuit boards, processors, chips, and associated computer hardware.	NA		
K0032	Knowledge of fault tolerance.	NA		
K0035	Knowledge of how system components are installed, integrated, and optimized.	1 - 14	4	50% or .5
K0036	Knowledge of human-computer interaction principles.	NA		
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	3.1	4	90% or .9
K0045	Knowledge of information security systems engineering principles.	NA		
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	3.2 - 3.5	4	90% or .9

NCWF JOB ROLE

Systems Developer

Job Role Description: A Systems Developer designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	1.2	4	90% or .9
K0052	Knowledge of mathematics, including logarithms, trigonometry, linear algebra, calculus, and statistics.	NA		
K0055	Knowledge of microprocessors.	NA		
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	3.1 - 3.5	4	90% or .9
K0060	Knowledge of operating systems.	6.1 - 6.5	2	30% or .3
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	1.3	4	90% or .9
K0063	Knowledge of parallel and distributed computing concepts.	NA		
K0065	Knowledge of policy-based and risk adaptive access controls.	3.3	4	90% or .9
K0066	Knowledge of Privacy Impact Assessments.	3.1	3	80% or .8
K0067	Knowledge of process engineering concepts.	NA		
K0073	Knowledge of secure configuration management techniques.	1 - 14	4	80% or .8
K0081	Knowledge of software development models (e.g., Waterfall Model, Spiral Model).	NA		
K0082	Knowledge of software engineering.	NA		
K0084	Knowledge of structured analysis principles and methods.	NA		
K0086	Knowledge of system design tools, methods, and techniques, including automated systems analysis and design tools.	1 - 14	3	60% or .6
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	4.6	3	40% or .4
K0090	Knowledge of system life cycle management principles, including software security and usability.	NA		
K0091	Knowledge of systems testing and evaluation methods.	NA		

NCWF JOB ROLE

Systems Developer

Job Role Description: A Systems Developer designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0093	Knowledge of key telecommunications concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers).	NA		
K0102	Knowledge of the systems engineering process.	NA		
K0139	Knowledge of interpreted and compiled computer languages.	NA		
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	NA		
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	6.1 - 6.10	3	50% or .5
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1 - 14	4	90% or .9
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	1 - 14		
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	1 - 14	3	50% or .5
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	NA		
K0207	Knowledge of circuit analysis.	NA		
K0212	Knowledge of cybersecurity-enabled software products.	1 - 14	3	50% or .5
K0227	Knowledge of various types of computer architectures.	NA		
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	NA		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	4.6	4	50% or .5
K0262	Knowledge of Personal Health Information (PHI) data security standards.	NA		
K0276	Knowledge of security management.	1 - 14	4	90% or .9

NCWF JOB ROLE

Systems Developer

Job Role Description: A Systems Developer designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	5.5	3	50% or .5
K0297	Knowledge of countermeasure design for identified security risks.	1 - 14	4	90% or .9
K0308	Knowledge of cryptology.	3.5	4	90% or .9
K0322	Knowledge of embedded systems.	NA		
K0325	Knowledge of Information Theory (e.g., source coding, channel coding, algorithm complexity theory, and data compression).	NA		
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	1.3	4	90% or .9
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs.	1 - 14	4	90% or .9
K0336	Knowledge of access authentication methods.	3.3,3.4	4	90% or .9
S0018	Skill in creating policies that reflect system security objectives.	4.1 - 4.6	4	90% or .9
S0022	Skill in designing countermeasures to identified security risks.	1 - 14	4	90% or .9
S0023	Skill in designing security controls based on cybersecurity principles and tenets.	1 - 14	4	90% or .9
S0024	Skill in designing the integration of hardware and software solutions.	1 - 14	4	90% or .9
S0031	Skill in developing and applying security system access controls.	3.3,3.4	4	90% or .9
S0034	Skill in discerning the protection needs (i.e., security controls) of information systems and networks.	1 - 14	4	90% or .9
S0036	Skill in evaluating the adequacy of security designs.	1 - 14	4	90% or .9
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	NA		
S0085	Skill in conducting audits or reviews of technical systems.	1 - 14	4	90% or .9
S0097	Skill in applying security controls.	1 - 14	4	90% or .9
S0098	Skill in detecting host and network based intrusions via intrusion detection technologies.	8.1 - 8.10	4	90% or .9

NCWF JOB ROLE

Systems Developer

Job Role Description: A Systems Developer designs, develops, tests, and evaluates information systems throughout the systems development life cycle.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Developer. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .3 on the framework Tasks and a correlation coefficient of .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
S0136	Skill in network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	1 - 14	4	90% or .9
S0145	Skill in integrating and applying policies that meet system security objectives.	4.1 - 4.6	4	90% or .9
S0146	Skill in creating policies that enable systems to meet performance objectives (e.g. traffic routing, SLA's, CPU specifications).	4.1 - 4.6	4	90% or .9
S0160	Skill in the use of design modeling (e.g., unified modeling language).	NA		
	Summary		**4**	**50% or .5**

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

OPERATE AND MAINTAIN (OM)

Specialty areas responsible for providing support, administration, and maintenance necessary to ensure effective and efficient information technology (IT) system performance and security.

Data Administration (DA)

Develops and administers databases and/or data management systems that allow for the storage, query, and utilization of data.

Knowledge Management (KM)

Manages and administers processes and tools that enable the organization to identify, document, and access Intellectual capital and information content.

Customer Service and Technical Support (TS)

Addresses problems and installs, configures, troubleshoots, and provides maintenance and training in response to customer requirements or inquiries (e.g., tiered-level customer support).

Network Services (NET)

Installs, configures, tests, operates, maintains, and manages networks and their firewalls, including hardware (e.g., hubs, bridges, switches, multiplexers, routers, cables, proxy servers, and protective distributor systems) and software that permit the sharing and transmission of all spectrum transmissions of information to support the security of information and information systems.

System Administration (SA)

Installs, configures, troubleshoots, and maintains server configurations (hardware and software) to ensure their confidentiality, integrity, and availability. Also manages accounts, firewalls, and patches. Responsible for access control, passwords, and account creation and administration.

Systems Security Analysis (AN)

Conducts the integration/testing, operations, and maintenance of systems security.

NCWF JOB ROLE

Technical Support Specialist

Job Role Description: Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Technical Support Specialist. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .5 on the framework tasks and a correlation coefficient of .6 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0237	Troubleshoot system hardware and software.	Implement	1.4	3	60% or .6
T0308	Analyze incident data for emerging trends.	Analyze	11.1 - 11.9,14.1,14.2	3	80% or .8
T0315	Develop and deliver technical training to educate others or meet customer needs.	Develop	**5.8**	**2**	40% or .4
T0331	Maintain incident tracking and solution database.	Maintain	**14.1, 14.2**	**2**	40% or .4
T0468	Diagnose and resolve customer reported system incidents, problems, and events.	Examine	**1.4**	**2**	40% or .4
T0482	Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.	Recommend	**1 - 14**	**2**	40% or .4
T0491	Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.	Implement	**1 - 14**	**4**	50% or .5
T0494	Administer accounts, network rights, and access to systems and equipment.	Administer	**3.1 - 3.4, 6.1 - 6.10**	**4**	60% or .6
T0496	Perform asset management/inventory of information technology (IT) resources.	Perform	**10.9 - 10.12**	**3**	40% or .4
T0502	Monitor and report client-level computer system performance.	Monitor	**6.1 - 6.10**	**3**	40% or .4
T0530	Develop a trend analysis and impact report.	Develop	**12.6**	**3**	40% or .4
	Summary			**3**	**50% or .5**

NCWF JOB ROLE

Technical Support Specialist

Job Role Description: Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Technical Support Specialist. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .5 on the framework tasks and a correlation coefficient of .6 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.1 - 1.3,3.1 - 3.5	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.2 - 12.4	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	3.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.2 - 2.4	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1	3	95% or .95
K0053	Knowledge of measures or indicators of system performance and availability.	6.1 - 6.10	3	60% or .6
K0088	Knowledge of systems administration concepts.	1.4	3	60% or .6
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems [GPSs]).	1 - 14	2	40% or .4
K0237	Knowledge of industry best practices for service desk.	5.6	2	40% or .4
K0242	Knowledge of organizational security policies.	4.1 - 4.5	4	60% or .6
K0247	Knowledge of remote access processes, tools, and capabilities related to customer support.	NA		
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	NA		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	4.6	4	40% or .4
K0262	Knowledge of Personal Health Information (PHI) data security standards.	NA		
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	5.5	3	35% or .35
K0292	Knowledge of the operations and processes for incident, problem, and event management.	14.1 - 14.3	3	35% or .35
K0294	Knowledge of IT system operation, maintenance, and security needed to keep equipment functioning properly.	1 - 14	4	60% or .6
K0302	Knowledge of the basic operation of computers.	1.4	2	60% or .6

NCWF JOB ROLE

Technical Support Specialist

Job Role Description: Provides technical support to customers who need assistance utilizing client-level hardware and software in accordance with established or approved organizational process components (i.e., Master Incident Management Plan, when applicable).

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Technical Support Specialist. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .5 on the framework tasks and a correlation coefficient of .6 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0306	Knowledge of basic physical computer components and architectures	1.1	4	60% or .6
K0317	Knowledge of procedures used for documenting and querying reported incidents, problems, and events.	14.1 - 14.3	3	35% or .35
K0330	Knowledge of successful capabilities to identify the solutions to less common and more complex system problems.	1 - 14	3	60% or .6
S0039	Skill in identifying possible causes of degradation of system performance or availability and initiating actions needed to mitigate this degradation.	6.1 - 6.10	3	35% or .35
S0058	Skill in using the appropriate tools for repairing software, hardware, and peripheral equipment of a system.	NA		
S0142	Skill in conducting research for troubleshooting novel client-level problems.	1 - 14	3	35% or .35
S0159	Skill in configuring and validating network workstations and peripherals in accordance with approved standards and/or specifications.	1 - 14	4	90% or .9
A0025	Ability to accurately define incidents, problems, and events in the trouble ticketing system.	14.1 - 14.3	3	35% or .35
A0034	Ability to develop, update, and/or maintain standard operating procedures (SOPs).	1 - 14	3	35% or .35
	Summary		**3**	**60% or .6**

NCWF JOB ROLE

Network Operations Specialist

Job Role Description: A Network Operations Specialist plans, implements, and operates network services/systems, to include hardware and virtual environments.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Network Operations Specialist. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0035	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).	Configure, Apply	6.9	3	60% or .6
T0065	Develop and implement network backup and recovery procedures.	Develop, Synthesize	13.1 - 13.10	4	100% or 1
T0081	Diagnose network connectivity problem.	Examine, Analyze, Evaluate	**1.4**	**4**	100% or 1
T0121	Implement new system design procedures, test procedures, and quality standards.	Implement, Apply, Analyze	**1 - 14**	**3**	45% or .45
T0125	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Install, Apply, Analyze	**6.1 - 6.9**	**3**	70% or .7
T0126	Install or replace network hubs, routers, and switches.	Install, Apply, Analyze	**6.9**	**2**	30% oe .3
T0129	Integrate new systems into existing network architecture.	Install, Apply, Analyze	**1 - 14**	**3**	70% or .7
T0153	Monitor network capacity and performance.	Monitor, Analyze, Evaluate	**11.7 - 11.9**	**4**	70% or .7
T0160	Patch network vulnerabilities to ensure information is safeguarded against outside parties.	Apply, Evaluate	**6.4, 12.6**	**4**	70% or .7
T0200	Provide feedback on network requirements, including network architecture and infrastructure.	Provide, Analysis	**1 - 14**	**3**	30% or .3
T0232	Test and maintain network infrastructure including software and hardware devices.	Test, Evaluate	**1 - 14**	**4**	60% or .6
	Summary			**3**	**65% or .65**

NCWF JOB ROLE

Network Operations Specialist

Job Role Description: A Network Operations Specialist plans, implements, and operates network services/systems, to include hardware and virtual environments.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Network Operations Specialist. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.1 - 1.4	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.2 - 12.4	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	3.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.1 - 2.4	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1	3	95% or .95
K0010	Knowledge of communication methods, principles, and concepts (e.g., crypto, dual hubs, time multiplexers) that support the network infrastructure.	1.2	2	30% or .3
K0011	Knowledge of capabilities and applications of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	3.7,6.8,6.9	3	70% or .7
K0029	Knowledge of organization's LAN/WAN pathways.	1.2	3	60% or .6
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	3.1	4	60% or .6
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	3.5,3.7	4	95% or .95
K0050	Knowledge of local area and wide area networking principles and concepts including bandwidth management.	1.2	4	95% or .95
K0053	Knowledge of measures or indicators of system performance and availability.	6.1 - 6.9	4	70% or .7
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	1.2	4	95% or .95
K0071	Knowledge of remote access technology concepts.	9.1 - 9.11	3	60% or .6
K0076	Knowledge of server administration and systems engineering theories, concepts, and methods.	6.8	2	60% or .6

NCWF JOB ROLE

Network Operations Specialist

Job Role Description: A Network Operations Specialist plans, implements, and operates network services/systems, to include hardware and virtual environments.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Network Operations Specialist. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0093	Knowledge of key telecommunications concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers).	NA		
K0104	Knowledge of Virtual Private Network (VPN) security.	9.1 - 9.11	4	95% or .95
K0108	Knowledge of basic concepts, terminology, and operations of a wide range of communications media (computer and telephone networks, satellite, fiber, wireless).	1.8 - 1.5, 10.1 - 10.15	3	60% or .6
K0113	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	1.1,1.2	4	95% or .95
K0135	Knowledge of web filtering technologies.	3.7	4	95% or .95
K0136	Knowledge of the capabilities of different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	6.8	2	30% or .3
K0137	Knowledge of the range of existing networks (e.g., PBX, LANs, WANs, WIFI, SCADA).	1.1,1.2,10.1 - 10.15	3	60% or .6
K0138	Knowledge of Wi-Fi.	10.1 - 10.8	4	95% or .95
K0159	Knowledge of Voice over IP (VoIP).	NA		
K0160	Knowledge of the common attack vectors on the network layer.	2.1 - 2.7	4	95% or .95
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1 - 14	4	95% or .95
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	1 - 14	4	95% or .95
K0181	Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi]. paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.	10.1 - 10.15	4	60% or .6
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	1 - 14	3	60% or .6
K0201	Knowledge of symmetric key rotation techniques and concepts.	3.5	4	95% or .95
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	NA		

NCWF JOB ROLE

Network Operations Specialist

Job Role Description: A Network Operations Specialist plans, implements, and operates network services/systems, to include hardware and virtual environments.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Network Operations Specialist. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	NA		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	4.6	4	95% or .95
K0262	Knowledge of Personal Health Information (PHI) data security standards.	NA		
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	5.5	3	35% or .35
K0307	Knowledge of common network tools (e.g., ping, traceroute, nslookup).	1.4	4	100% or 1
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	1.3	4	95% or .95
S0004	Skill in analyzing network traffic capacity and performance characteristics.	11.1 - 11.9	3	100% or 1
S0035	Skill in establishing a routing schema.	1.1 - 1.5	3	30% or .3
S0040	Skill in implementing, maintaining, and improving established network security practices.	1 - 14	3	100% or 1
S0041	Skill in installing, configuring, and troubleshooting LAN and WAN components such as routers, hubs, and switches.	1 - 14	3	60% or .6
S0056	Skill in using network management tools to analyze network traffic patterns (e.g., simple network management protocol).	11.1 - 11.9	3	100% or 1
S0077	Skill in securing network communications.	3.8	3	60% or .6
S0079	Skill in protecting a network against malware.	6.1 - 6.6	3	95% or .95
S0084	Skill in configuring and utilizing network protection components (e.g., Firewalls, VPNs, network intrusion detection systems).	7.1 - 7.12, 8.1 - 8.10, 9.1 - 9.11	3	95% or .95
S0150	Skill in implementing and testing network infrastructure contingency and recovery plans.	13.1 - 13.10	3	95% or .95
S0162	Skill in sub-netting.	1.5	3	95% or .95
S0170	Skill in configuring and utilizing computer protection components (e.g., hardware firewalls, servers, routers, as appropriate).	1 - 14	3	95% or .95

NCWF JOB ROLE

Network Operations Specialist

Job Role Description: A Network Operations Specialist plans, implements, and operates network services/systems, to include hardware and virtual environments.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Network Operations Specialist. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .65 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
A0052	Ability to operate network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	1 - 14	3	60% or .6
A0055	Ability to operate common network tools (e.g., ping, traceroute, nslookup).	1.4	4	100% or 1
A0058	Ability to execute OS command line (e.g., ipconfig, netstat, dir, nbtstat).	1.4,6.1 - 6.8	4	100% or 1
A0059	Ability to operate the organization's LAN/WAN pathways.	1.2	3	60% or .6
A0062	Ability to monitor measures or indicators of system performance and availability.	6.1 - 6.8	3	60% or .6
A0063	Ability to operate different electronic communication systems and methods (e.g., e-mail, VOIP, IM, web forums, Direct Video Broadcasts).	6.8	3	60% or .6
A0065	Ability to monitor traffic flows across the network.	11.1 - 11.9	3	100% or 1
	Summary		**3**	**80% or .8**

NCWF JOB ROLE

System Administrator

Job Role Description: A System Administrator installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a System Administrator. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .7 on the framework tasks and a correlation coefficient of .85 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0029	Conduct functional and connectivity testing to ensure continuing operability.	Conduct	1.4	2	40% or .4
T0054	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	Design	3.3,6.3	3	40% or .4
T0063	Develop and document systems administration standard operating procedures.	Develop	1.4	2	40% or .4
T0136	Maintain baseline system security according to organizational policies.	Maintain	6.1 ,6.2	4	95% or .95
T0144	Manage accounts, network rights, and access to systems and equipment.	Manage	6.1 - 6.3	4	95% or .95
T0186	Plan, execute, and verify data redundancy and system recovery procedures.	Plan	13.9,13.10	3	40% or .4
T0207	Provide ongoing optimization and problem solving support.	Provide	1 - 14	3	40% or .4
T0418	Install, update, and troubleshoot systems/servers.	Install	6.1 - 6.9	4	80% or .8
T0431	Check system hardware availability, functionality, integrity, and efficiency.	Test	6.1 - 6.9	4	50% or .5
T0435	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	Conduct	6.1 - 1.9	3	40% or .4
T0458	Comply with organization systems administration standard operating procedures.	Comply	1.4,4.1 - 4.4	3	40% or .4
T0461	Implement and enforce local network usage policies and procedures.	Implement	4.4	4	100% or 1
T0498	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	Manage	6.1 - 6.9	4	95% or .95
T0501	Monitor and maintain system/server configuration.	Monitor	6.1 - 6.9	4	100% or 1
T0507	Oversee installation, implementation, configuration, and support of system components.	Support	6.1 - 6.9	4	100% or 1
T0514	Diagnose faulty system/server hardware.	Examine	1.4, 6.1 - 6.9	4	100% or 1
T0515	Perform repairs on faulty system/server hardware.	Perform	1.4, 6.1 - 6.9	3	40% or .4
T0531	Troubleshoot hardware/software interface and interoperability problems.	Troubleshoot	1.4	4	95% or .95
	Summary			**3**	**70% or .7**

NCWF JOB ROLE

System Administrator

Job Role Description: A System Administrator installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a System Administrator. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .7 on the framework tasks and a correlation coefficient of .85 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.1 - 1.4	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.2 - 12.4	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	3.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.2 - 2.4	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1	3	95% or .95
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	3.5,3.7	4	100% or 1
K0053	Knowledge of measures or indicators of system performance and availability.	6.1 - 6.9	4	100% or 1
K0064	Knowledge of performance tuning tools and techniques.	11.9	4	100% or 1
K0077	Knowledge of server and client operating systems.	6.2	4	100% or 1
K0088	Knowledge of systems administration concepts.	1.4	4	100% or 1
K0100	Knowledge of the enterprise information technology (IT) architecture.	1.6	4	95% or .95
K0103	Knowledge of the type and frequency of routine maintenance needed to keep equipment functioning properly.	1.4	3	95% or .95
K0104	Knowledge of Virtual Private Network (VPN) security.	9.1 - 9.11	4	100% or 1
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	6.2,6.3	3	95% or .95
K0130	Knowledge of virtualization technologies and virtual machine development and maintenance.	6.13	4	95% or .95
K0158	Knowledge of organizational information technology (IT) user security policies (e.g., account creation, password rules, access control).	4.4	4	95% or .95
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	1.4,6.2,6.3	4	100% or 1

NCWF JOB ROLE

System Administrator

Job Role Description: A System Administrator installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a System Administrator. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .7 on the framework tasks and a correlation coefficient of .85 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1 - 14	4	100% or 1
K0181	Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification [RFID], Infrared Networking [IR], Wireless Fidelity [Wi-Fi]. paging, cellular, satellite dishes), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.	10.1 - 10.8	4	60% or .6
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	NA		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	4.6	4	95% or .95
K0262	Knowledge of Personal Health Information (PHI) data security standards.	NA		
K0280	Knowledge of systems engineering theories, concepts, and methods.	NA		
K0289	Knowledge of system/server diagnostic tools and fault identification techniques.	6.1 - 6.10	4	95% or .95
K0318	Knowledge of operating system command line/prompt.	1.4, 6.2,6.3,6.6.	3	95% or .95
K0327	Knowledge of local area network (LAN), wide area network (WAN) and enterprise principles and concepts, including bandwidth management.	1.2	4	95% or .95
K0331	Knowledge of network protocols (e.g., Transmission Critical Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP)), and directory services (e.g., Domain Name System (DNS)).	1.3	4	95% or .95
K0346	Knowledge of principles and methods for integrating system components.	1 - 14	3	40% or .4
S0016	Skill in configuring and optimizing software.	1 - 14	3	40% or .4
S0033	Skill in diagnosing connectivity problems.	1.4	4	95% or .95
S0043	Skill in maintaining directory services.	6.1 - 6.10	3	40% or .4
S0073	Skill in using virtual machines.	6.13	3	40% or .4
S0076	Skill in configuring and utilizing software-based computer protection tools (e.g., software firewalls, anti-virus software, anti-spyware).	6.1 - 6.10	4	95% or .95
S0111	Skill in interfacing with customers.	NA		

NCWF JOB ROLE

System Administrator

Job Role Description: A System Administrator installs, configures, troubleshoots, and maintains hardware and software, and administers system accounts.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a System Administrator. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .7 on the framework tasks and a correlation coefficient of .85 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
S0143	Skill in conducting system/server planning, management, and maintenance.	6.1 - 6.10	4	95% or .95
S0144	Skill in correcting physical and technical problems that impact system/server performance.	5.1 - 5.7, 6.1 - 6.10	4	95% or .95
S0151	Skill in troubleshooting failed system components (i.e., servers)	14, 6.8	3	40% or .4
S0153	Skill in identifying and anticipating system/server performance, availability, capacity, or configuration problems.	14, 6.8	3	40% or .4
S0154	Skill in installing system and component upgrades.	6.1 - 6.10	4	95% or .95
S0155	Skill in monitoring and optimizing system/server performance.	6.1 - 6.10	4	95% or .95
S0157	Skill in recovering failed systems/servers.	6.1 - 6.10	3	40% or .4
S0158	Skill in operating system administration.	6.1 - 6.10	3	40% or .4
	Summary		**4**	**85% or .85**

NCWF JOB ROLE

Systems Security Analyst

Job Role Description: A Systems Security Analyst is responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Security Analyst. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .5 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0015	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Apply	4.4	3	40% or .4
T0016	Apply security policies to meet security objectives of the system.	Apply	4.4	4	75% or .75
T0017	Apply service oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.	Apply	1 - 14	4	75% or .75
T0085	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	Verify	1 - 14	3	60% or .6
T0086	Ensure application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.	Verify	6.4	3	40% or .4
T0088	Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Verify	12.2	4	60% or .6
T0123	Implement specific cybersecurity countermeasures for systems and/or applications.	Implement	6.1 - 6.12	4	60% or .6
T0128	Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.	Integrate	6.4	4	60% or .6
T0169	Perform cybersecurity testing of developed applications and/or systems.	Perform	NA		
T0177	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Perform	12.2	4	60% or .6
T0187	Plan and recommend modifications or adjustments based on exercise results or system environment.	Plan	6.1 - 6.12	4	60% or .6
T0194	Properly document all systems security implementation, operations and maintenance activities and update as necessary.	Write	6.1 - 6.12	3	60% or .6

NCWF JOB ROLE

Systems Security Analyst

Job Role Description: A Systems Security Analyst is responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Security Analyst. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .5 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0202	Provide cybersecurity guidance to leadership.	Provide	NA		
T0205	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Provide	12.2, 12.3	3	40% or .4
T0243	Verify and update security documentation reflecting the application/system security design features.	Verify	6.1 - 6.12	3	40% or .4
T0309	Assess the effectiveness of security controls.	Assess	1 - 14	4	60% or .6
T0344	Assess all the configuration management (change configuration/release management) processes.	Assess	1 - 14	4	60% or .6
T0462	Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements.	Develop	6.1 - 6.12	3	40% or .4
T0469	Analyze and report organizational security posture trends.	Analyze	1 - 14	3	40% or .4
T0470	Analyze and report system security posture trends.	Analyze	6.1 - 6.12	3	40% or .4
T0475	Assess adequate access controls based on principles of least privilege and need-to-know.	Assess	3.3,3.4	3	40% or .4
T0477	Ensure the execution of disaster recovery and continuity of operations.	Verify	13.1 - 13.10	4	60% or .6
T0485	Implement security measures to resolve vulnerabilities, mitigate risks and recommend security changes to system or system components as needed.	Implement	1 - 14	4	60% or .6
T0489	Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.	Implement	1 - 14	4	60% or .6
T0492	Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment.	Verify	NA		

NCWF JOB ROLE

Systems Security Analyst

Job Role Description: A Systems Security Analyst is responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Security Analyst. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .5 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0499	Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.	Mitigate	12.2,12.3	3	40% or .4
T0504	Assess and monitor cybersecurity related to system implementation and testing practices.	Assess	6.1 - 6.12	3	40% or .4
T0508	Verify minimum security requirements are in place for all applications.	Verify	6.11	3	40% or .4
T0526	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Provide	1 - 14	3	40% or .4
T0545	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Resolve	14.1 - 14.3	3	40% or .4
T0548	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	Provide	13.1 - 13.10	3	40% or .4
	Summary			**3**	**50% or .5**

NCWF JOB ROLE

Systems Security Analyst

Job Role Description: A Systems Security Analyst is responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Security Analyst. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .5 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.1 - 1.4	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.2 - 12.4	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	3.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.2 - 2.4	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1	3	95% or .95
K0015	Knowledge of computer algorithms.	NA		
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	3.5	4	95% or .95
K0019	Knowledge of cryptography and cryptographic key management concepts.	3.5	4	95% or .95
K0024	Knowledge of database systems.	NA		
K0035	Knowledge of how system components are installed, integrated, and optimized.	1 - 14	3	40% or .4
K0036	Knowledge of human-computer interaction principles.	1 - 14	3	40% or .4
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	2.2	3	40% or .4
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	3.1	3	95% or .95
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	3.5,3.7	4	95% or .95
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	3.3, 3.4,3.5	4	95% or .95
K0060	Knowledge of operating systems.	6.2	3	40% or .4

NCWF JOB ROLE

Systems Security Analyst

Job Role Description: A Systems Security Analyst is responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Security Analyst. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .5 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	1.2,1.3	4	95% or .95
K0063	Knowledge of parallel and distributed computing concepts.	NA		
K0075	Knowledge of security system design tools, methods, and techniques.	1 - 14	4	95% or .95
K0082	Knowledge of software engineering.	NA		
K0093	Knowledge of key telecommunications concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers).	NA		
K0102	Knowledge of the systems engineering process.	NA		
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1 - 14	4	95% or .95
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	1 - 14	4	95% or .95
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	1 - 14	4	95% or .95
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	NA		
K0227	Knowledge of various types of computer architectures.	NA		
K0232	Knowledge of critical protocols (e.g., IPSEC, AES, GRE, IKE).	3.8	3	40% or .4
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	NA		
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	4.6	4	95% or .95
K0262	Knowledge of Personal Health Information (PHI) data security standards.	NA		
K0263	Knowledge of information technology (IT) risk management policies, requirements, and procedures.	4.3,4.4	3	40% or .4
K0266	Knowledge of how to evaluate the trustworthiness of the supplier and/or product.	8.8	3	40% or .4

NCWF JOB ROLE

Systems Security Analyst

Job Role Description: A Systems Security Analyst is responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Security Analyst. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .5 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	4.6	4	95% or .95
K0275	Knowledge of configuration management techniques.	1 - 14	4	95% or .95
K0276	Knowledge of security management.	1 - 14	4	95% or .95
K0281	Knowledge of information technology (IT) service catalogues.	1 - 14	3	40% or .4
K0284	Knowledge of developing and applying user credential management system.	3.4	3	40% or .4
K0285	Knowledge of implementing enterprise key escrow systems to support data-at-rest encryption.	6.12	3	40% or .4
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	5.5	3	40% or .4
K0290	Knowledge of systems security testing and evaluation methods.	6.1 - 6.8	3	40% or .4
K0297	Knowledge of countermeasure design for identified security risks.	1 - 14	4	95% or .95
K0322	Knowledge of embedded systems.	NA		
K0329	Knowledge of statistics.	NA		
K0333	Knowledge of network design processes, to include understanding of security objectives, operational objectives, and tradeoffs.	1 - 14	4	95% or .95
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	12.6	4	95% or .95
S0024	Skill in designing the integration of hardware and software solutions.	1 - 14	3	40% or .4
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	5.7,6.1 - 6.8	3	40% or .4
S0031	Skill in developing and applying security system access controls.	1 - 14	4	95% or .95
S0036	Skill in evaluating the adequacy of security designs.	1 - 14	4	95% or .95
S0060	Skill in writing code in a currently supported programming language (e.g., Java, C++).	NA		
S0141	Skill in assessing security systems designs.	1 - 14	4	95% or .95

NCWF JOB ROLE

Systems Security Analyst

Job Role Description: A Systems Security Analyst is responsible for the analysis and development of the integration, testing, operations, and maintenance of systems security.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Systems Security Analyst. CND maps to this job role at an Specialist level (level 3) with a correlation coefficient of .5 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
S0147	Skill in assessing security controls based on cybersecurity principles and tenets.	1 - 14	4	95% or .95
S0167	Skill in recognizing vulnerabilities in security systems.	12.6	4	95% or .95
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	12.6	4	95% or .95
	Summary		**4**	**80% or .8**

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

OVERSEE AND GOVERN (OV)

Specialty areas providing leadership, management, direction, and/or development and advocacy so that individuals and organizations may effectively conduct cybersecurity work.

Legal Advice and Advocacy

Provides legally sound advice and recommendations to leadership and staff on a variety of relevant topics within the pertinent subject domain. Advocates legal and policy changes and makes a case on behalf of client via a wide range of written and oral work products, including legal briefs and proceedings.

Strategic Planning and Policy (PL)

Develops policies and plans and/or advocates for changes in policy that supports organizational cyberspace initiatives or required changes/enhancements.

Executive Cybersecurity Leadership (EX)

Supervises, manages, and/or leads work and workers performing cybersecurity work.

Training, Education, and Awareness (ED)

Conducts training of personnel within pertinent subject domain. Develops, plans, coordinates, delivers, and/or evaluates training courses, methods, and techniques as appropriate.

Acquisition and Program/Project Management (PM)

Applies knowledge of data, information, processes, organizational interactions, skills, and analytical expertise, as well as systems, networks, and information exchange capabilities to manage acquisition programs. Executes duties governing hardware, software, and information system acquisition programs and other program management policies. Provides direct support for acquisitions that use IT (including National Security Systems), applying IT-related laws and policies, and provides IT-related guidance throughout the total acquisition life-cycle.

Cybersecurity Management (MG)

Oversees the cybersecurity program of an information system or network; including managing information security implications within the organization, specific program, or other area of responsibility, to include strategic, personnel, infrastructure, requirements, policy enforcement, emergency planning, security awareness, and other resources.

NCWF JOB ROLE

Cyber Legal Advisor

Job Role Description: A Cyber Legal Advisor provides legal advice and recommendations on relevant topics related to cyber law.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Legal Advisor. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .5 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0006	Advocate organization's official position in legal and legislative proceedings.	Synthesis, Evaluation	1.5	4	60% or .6
T0098	Evaluate contracts to ensure compliance with funding, legal, and program requirements.	Synthesis, Evaluation	5.2.11	3	80% or .8
T0102	Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.	Synthesis, Evaluation	2.1.5	4	80% or .8
T0131	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.	Analysis, Evaluation	1.5 to 1.10	3	60% or .6
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Analysis, Evaluation	1.5 to 1.12	3	60% or .6
T0419	Acquire and maintain a working knowledge of constitutional issues relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.	Synthesis, Evaluation	1.5 to 1.10	4	80% or .8
T0434	Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.	Analysis, Evaluation	1.12	3	30% or .3
T0465	Develop guidelines for implementation.	Analysis, Evaluation	1.17,1.18	3	30% or .3
T0474	Provide legal analysis and decisions to inspector generals, privacy officers, oversight and compliance personnel with regard to compliance with cybersecurity policies and relevant legal and regulatory requirements.	Analysis, Evaluation	1.13,1.14	3	30% or .3
T0476	Evaluate the impact of changes to laws, regulations, policies, standards, or procedures.	Analysis, Evaluation	**2.1.5**	**3**	30% or .3
T0478	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.	Analysis, Evaluation	1.14,1.19	3	30% or .3
T0487	Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures.	Analysis, Evaluation	1.13	**3**	30% or .3

NCWF JOB ROLE

Cyber Legal Advisor

Job Role Description: A Cyber Legal Advisor provides legal advice and recommendations on relevant topics related to cyber law.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Legal Advisor. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .5 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0522	Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).	Analysis, Evaluation	1.18	3	60% or .6
	Summary			**3**	**50% or .5**

NCWF JOB ROLE

Cyber Legal Advisor

Job Role Description: A Cyber Legal Advisor provides legal advice and recommendations on relevant topics related to cyber law.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Legal Advisor. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .5 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0017	Knowledge of concepts and practices of processing digital forensic data.	4.13	3	90% or .9
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	5.1	3	60% or .6
K0107	Knowledge of and experience in Insider Threat investigations, reporting, investigative tools and laws/ regulations.	4.13	3	90% or .9
K0157	Knowledge of cyber defense policies, procedures, and regulations.	1.5 to 1.10	3	95% or .95
K0312	Knowledge of intelligence principles, policies, and procedures including legal authorities and restrictions.	1.5 to 1.10	3	95% or .95
K0316	Knowledge of business or military operation plans, concept operation plans, orders, policies, and standing rules of engagement.	5.1	3	70% or .7
K0341	Knowledge of foreign disclosure policies and import/export control regulations as related to cybersecurity.	5.2	3	70% or .7
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Synthesis, Evaluation	4.4	4	90% or .9
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, and systems, and elements.	Synthesis, Evaluation	5.2	4	90% or .9
T0032	Conduct Privacy Impact Assessments (PIA) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Analysis	4.9.1	3	90% or .9
T0066	Develop and maintain strategic plans.	Analysis, Evaluation	5.1	4	100% or 1
T0098	Evaluate contracts to ensure compliance with funding, legal, and program requirements.	Analysis, Evaluation	5.2.11	3	90% or .9
T0099	Evaluate cost benefit, economic, and risk analysis in decision making process.	Synthesis, Evaluation	5.2.8	4	90% or .9
T0131	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.	Analysis, Evaluation	1.1 to 1.19	4	80% or .8
T0133	Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	Analysis, Evaluation	1.1 to 1.19	4	80% or .8
T0188	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.	Analysis, Evaluation	2.2.3 to 2.2.6	4	80% or .8
T0381	Present technical information to technical and non-technical audiences.	Analysis	5.1	3	90% or .9
T0384	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Analysis, Evaluation	5.1	3	90% or .9
T0478	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.	Synthesis, Evaluation	1.1 to 1.19	4	90% or .9
T0861	Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations.	Analysis	1.8, 1.9	3	90% or .9

NCWF JOB ROLE

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0862	Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.	Analysis	1.8, 1.10	3	90% or .9
T0863	Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.	Analysis	1.1 to 1.19	3	90% or .9
T0864	Liaise with regulatory and accrediting bodies.	Analysis	1.1 to 1.19		90% or .9
T0865	Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.	Analysis	1.7 - 1.14	3	90% or .9
T0866	Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.	Analysis	1.1 to 1.19	3	80% or .8
T0867	Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.	Analysis	1.7 - 1.14	3	80% or .9
T0868	Work with business teams and senior management to ensure awareness of "best practices" on privacy and data security issues.	Analysis	1.7	3	90% or .9
T0869	Work with organization senior management to establish an organization-wide Privacy Oversight Committee	Analysis	5.1	3	90% or .9
T0870	Serve in a leadership role for Privacy Oversight Committee activities	Analysis	5.1	3	90% or .9
T0871	Collaborate on cyber privacy and security policies and procedures	Analysis	5.1	3	90% or .9
T0872	Collaborate with cyber security personnel on the security risk assessment process to address privacy compliance and risk mitigation	Analysis	4.4	3	80% or .8

NCWF JOB ROLE

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0873	Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations	Synthesis, Evaluation	5.1	4	80% or .8
T0874	Provide strategic guidance to corporate officers regarding information resources and technology	Synthesis, Evaluation	5.1	4	80% or .8
T0875	Assist the Security Officer with the development and implementation of an information infrastructure	Analysis	2.1	3	90% or .9
T0876	Coordinate with the Corporate Compliance Officer re: procedures for documenting and reporting self-disclosures of any evidence of privacy violations.	Analysis	1.1 to 1.19	3	90% or .9
T0877	Work cooperatively with applicable organization units in overseeing consumer information access rights	Analysis	4.1	3	90% or .9
T0878	Serve as the information privacy liaison for users of technology systems	Analysis	3.1 to 3.14	3	90% or .9
T0879	Act as a liaison to the information systems department	Analysis	3.1 to 3.14	3	90% or .9
T0880	Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations	Synthesis, Evaluation	3.6	4	90% or .9
T0881	Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties	Synthesis, Evaluation	3.6	4	90% or .9
T0882	Conduct on-going privacy training and awareness activities	Analysis	3.6	3	90% or .9
T0883	Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security	Analysis	1.14	3	90% or .10

NCWF JOB ROLE

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0884	Work with organization administration, legal counsel and other related parties to represent the organization's information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard.	Analysis	1.14	3	90% or .11
T0885	Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee	Analysis, Evaluation	2.1.8	4	80% or .80
T0886	Work with External Affairs to respond to press and other inquiries with regard to concern over consumer and employee data	Analysis, Evaluation	1.14	3	90% or .11
T0887	Provide leadership for the organization's privacy program	Analysis, Evaluation	1.1	4	80% or .80
T0888	Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization	Analysis	3.7	3	80% or .80
T0889	Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce and for all business associates in cooperation with Human Resources, the information security officer, administration and legal counsel as applicable	Analysis	1.1 to 1.19	3	90% or .9
T0890	Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures	Synthesis, Evaluation	1.1 to 1.19	4	90% or .9
T0891	Resolve allegations of non-compliance with the corporate privacy policies or notice of information practices	Analysis, Evaluation	1.1 to 1.19	3	90% or .9
T0892	Develop and coordinate a risk management and compliance framework for privacy	Synthesis, Evaluation	4.4	4	80% or .80

NCWF JOB ROLE

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0893	Undertake a comprehensive review of the company's data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies.	Analysis, Evaluation	5.1.2	3	90% or .9
T0894	Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations	Synthesis, Evaluation	3.1 to 3.14	4	90% or .9
T0895	Establish a process for receiving, documenting, tracking, investigating and taking action on all complaints concerning the organization's privacy policies and procedures	Synthesis, Evaluation	3.1 to 3.14	4	90% or .9
T0896	Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity	Synthesis, Evaluation	3.1 to 3.14	4	90% or .9
T0897	Provide leadership in the planning, design and evaluation of privacy and security related projects	Analysis, Evaluation	2.1.1 to 2.1.8	3	90% or .9
T0898	Establish an internal privacy audit program	Synthesis, Evaluation	2.2	4	90% or .9
T0899	Periodically revise the privacy program in light of changes in laws, regulatory or company policy	Analysis, Evaluation	1.1 to 1.19	3	90% or .9
T0900	Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel	Analysis, Evaluation	1.1 to 1.19	3	90% or .9
T0901	Assure that the use of technologies maintain, and do not erode, privacy protections on use, collection and disclosure of personal information	Analysis, Evaluation	2.1	3	90% or .9

NCWF JOB ROLE

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0902	Monitor systems development and operations for security and privacy compliance	Analysis, Evaluation	1.1 to 1.19	3	90% or .9
T0903	Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected	Analysis, Evaluation	4.13.3	3	90% or .9
T0904	Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions	Analysis, Evaluation	4.5.5	3	90% or .9
T0905	Review all system-related information security plans to ensure alignment between security and privacy practices	Analysis, Evaluation	3.12	4	80% or .80
T0906	Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization's policies, procedures and legal requirements	Analysis, Evaluation	2.1.5	4	80% or .80
T0907	Account for and administer individual requests for release or disclosure of personal and/or protected information	Analysis	NA		
T0908	Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements	Synthesis, Evaluation	1.1 to 1.19	4	90% or .9
T0909	Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed	Analysis	1.1 to 1.19	3	90% or .9
T0910	Act as, or work with, counsel relating to business partner contracts	Analysis	NA	3	90% or .9
T0911	Mitigate effects of a use or disclosure of personal information by employees or business partners	Analysis	2.1.6	3	90% or .9
T0912	Develop and apply corrective action procedures	Synthesis, Evaluation	2.1	4	90% or .9

NCWF JOB ROLE

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0913	Administer action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel	Analysis	NA		
T0914	Support the organization's privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations	Analysis	1.16 to 1.19	3	90% or .9
T0915	Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations	Analysis, Evaluation	1.12	3	90% or .9
T0916	Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units	Analysis, Evaluation	4.4.6	3	90% or .9
T0917	Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices	Analysis, Evaluation	1.15	3	90% or .9
T0918	Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations	Synthesis, Evaluation	1.1 to 1.19	4	90% or .9
T0919	Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials	Analysis, Evaluation	1.11, 2.1	3	80% or .8
Summary				4	**90% or .9**

NCWF JOB ROLE

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0008	Knowledge of applicable business processes and operations of customer organizations.	3.1 to 3.14	4	95% or .95
K0066	Knowledge of Privacy Impact Assessments.	4.13.3	3	95% or .95
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	1.1 to 1.19	3	95% or .95
K0606	Knowledge of transcript development processes and techniques (e.g., verbatim, gists, summaries).	NA		
K0607	Knowledge of translation processes and techniques.	NA		
K0608	Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).	4.1	3	40% or .4
K0609	Knowledge of virtual machine technologies.	NA		
K0610	Knowledge of virtualization products (VMware, Virtual PC).	NA		
K0611	Withdrawn – Integrated into K0131	NA		
K0612	Knowledge of what constitutes a "threat" to a network.	NA		
K0613	Knowledge of who the organization's operational planners are, how and where they can be contacted, and what are their expectations.	3.1 to 3.14	4	95% or .95

NCWF JOB ROLE

Privacy Compliance Manager

Job Role Description: A Privacy Compliance Manager develops and oversees privacy compliance program and privacy program staff, supporting privacy compliance needs of privacy and security executives and their teams.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Privacy Compliance Manager. CCISO maps to this job role at an Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.	4.7	3	95% or .95
S0354	Skill in creating policies that reflect the business's core privacy objectives.	1.1 to 1.19	3	95% or .95
S0355	Skill in negotiating vendor agreements and evaluating vendor privacy practices.	3.9	4	95% or .95
S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	3.13	3	40% or .40
A0024	Ability to develop clear directions and instructional materials.	3.7, 4.5.5	3	40% or .40
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	1.1 to 1.19	3	95% or .95
A0034	Ability to develop, update, and/or maintain standard operating procedures (SOPs).	4.15	3	95% or .95
A0104	Ability to select the appropriate implant to achieve operational goals.	3.1 to 3.14	4	95% or .95
A0105	Ability to tailor technical and planning information to a customer's level of understanding.	1.18, 2.1.8, 2.2.6, 3.13		95% or .95
A0110	Ability to monitor advancements in information privacy laws to ensure organizational adaptation and compliance.	4.4.9	3	95% or .95
A0111	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.	4.4.3	3	95% or .95
A0112	Ability to monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.	1.15, 1.16	3	95% or .95
A0113	Ability to determine whether a security incident violates a privacy principle or legal standard requiring specific legal action.	4.13.3	3	95% or .95
A0114	Ability to develop or procure curriculum that speaks to the topic at the appropriate level for the target.	3.6	3	95% or .95
A0115	Ability to work across departments and business units to implement organization's privacy principles and programs, and align privacy objectives with security objectives.	4.4.3	3	95% or .95
	Summary		**3**	**95% or .95**

NCWF JOB ROLE

Cyber Instructional Curriculum Developer

Job Role Description: A Cyber Instructional Curriculum Developer develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs..

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructional Curriculum Developer. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0230	Support the design and execution of exercise scenarios.	Analysis	6.1, 6.2	3	90% or .9
T0247	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	Write, Synthesis	5.2, 8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
T0345	Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.	Assess, Evaluation	NA		
T0352	Conduct learning needs assessments and identify requirements.	Conduct, Analysis	14.4	3	90% or .9
T0357	Create interactive learning exercises to create an effective learning environment.	Create, Synthesis	16.1, 16.2, 16.3	4	100% or 1
T0365	Develop or assist in the development of training policies and protocols for cyber training.	Develop, Analysis	17.6	3	90% or .9
T0367	Develop the goals and objectives for cyber curriculum.	Develop, Analysis	8.1	3	90% or .9
T0380	Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers.	Plan, Synthesis	6.1, 6.2, 13.1, 13.2, 13.3	4	100% or 1
T0437	Correlates training and learning to business or mission requirements.	Correlate, Evaluation	16.1, 16.2, 16.3	4	100% or 1
T0442	Create training courses tailored to the audience and physical environment.	Create, Synthesis	8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
T0450	Design training curriculum and course content based on requirements.	Design, Synthesis	8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
T0534	Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions).	Conduct	15.1, 15.2	3	90% or .9
T0536	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Serve	3.1, 3.2, 3.3	3	90% or .9

NCWF JOB ROLE

Cyber Instructional Curriculum Developer

Job Role Description: A Cyber Instructional Curriculum Developer develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs..

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructional Curriculum Developer. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0926	Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations	Develop, Synthesis	2.1, 2.2, 5.1, 6.1, 6.2, 8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
	Summary			**4**	**95% or .95**

NCWF JOB ROLE

Cyber Instructional Curriculum Developer

Job Role Description: A Cyber Instructional Curriculum Developer develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs..

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructional Curriculum Developer. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	NA		
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	NA		
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	18.2	2	50% or .5
K0004	* Knowledge of cybersecurity principles.	18.2	2	50% or .5
K0005	* Knowledge of cyber threats and vulnerabilities.	18.2	2	50% or .5
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	18.2	2	50% or .5
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	18.2	2	50% or .5
K0124	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain.	18.2, 18.4, 18.6	3	60% or .6
K0146	Knowledge of the organization's core business/mission processes.	1.1 to 1.9	3	100% or 1
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	18.2, 18.4, 18.6	3	60% or .6
K0239	Knowledge of media production, communication, and dissemination techniques and methods, including alternative ways to inform via written, oral, and visual media.	13.1, 13.2, 13.3	4	100% or 1
K0245	Knowledge of principles and processes for conducting training and education needs assessment.	2.1, 2.2, 3.1, 3.2, 3.3, 6.1, 6.2, 10.1, 10.2, 12.1, 13.1, 13.2, 13.3, 14.1, 16.1, 16.2, 16.3	4	100% or 1
K0246	Knowledge of relevant concepts, procedures, software, equipment, and technology applications.	17.1, 17.2, 17.3, 17.4, 17.5, 18.1, 18.2, 18.3, 18.4, 18.5, 18.6	4	100% or 1

NCWF JOB ROLE

Cyber Instructional Curriculum Developer

Job Role Description: A Cyber Instructional Curriculum Developer develops, plans, coordinates, and evaluates cyber training/education courses, methods, and techniques based on instructional needs..

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructional Curriculum Developer. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0252	Knowledge of training and education principles and methods for curriculum design, teaching and instruction for individuals and groups, and the measurement of training and education effects.	2.1, 2.2, 3.1, 3.2, 3.3, 6.1, 6.2, 10.1, 10.2, 12.1, 13.1, 13.2, 13.3, 14.1, 16.1, 16.2, 16.3	4	100% or 1
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	2.1, 2.2, 4.1, 4.2, 4.3, 5.1, 5.2, 5.3, 6.1, 6.2	4	100% or 1
S0064	Skill in developing and executing technical training programs and curricula.	8.1, 8.2, 8.3, 8.4, 8.5, 13.1, 13.2, 13.3	4	100% or 1
S0066	Skill in identifying gaps in technical capabilities.	6.1, 6.2, 7.1, 8.1, 8.2, 8.3, 8.4, 8.5, 10.1, 10.2, 11.1, 11.2	4	100% or 1
S0070	Skill in talking to others to convey information effectively.	12.1	3	90% or .9
S0102	Skill in applying technical delivery capabilities.	8.1, 8.2, 8.3, 8.4, 8.5, 13.,1, 13.2, 13.3	3	90% or .9
S0166	Skill in identifying gaps in technical delivery capabilities.	8.1, 8.2, 8.3, 8.4, 8.5, 13.,1, 13.2, 13.3	3	90% or .9
A0004	Ability to develop curriculum that speaks to the topic at the appropriate level for the target audience.	8.1, 8.2, 8.3, 8.4, 8.5	3	90% or .9
A0032	Ability to develop curriculum for use within a virtual environment.	8.1, 8.2, 8.3, 8.4, 8.5	3	90% or .9
A0054	Ability to apply the Instructional System Design (ISD) methodology.	8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
	Summary		**3**	**80% or .8**

NCWF JOB ROLE

Cyber Instructor

Job Role Description: A Cyber Instructor develops and conducts training or education of personnel within cyber domain.

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructor. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0030	Conduct interactive training exercises to create an effective learning environment.	Conduct, Synthesis	6.1, 14.1	4	100% or 1
T0073	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.	Develop, Synthesis	8.1, 8.2, 8.3, 8.4	4	100% or 1
T0101	Evaluate the effectiveness and comprehensiveness of existing training programs.	Evaluate	14.1, 15.1, 15.2	3	90% or .9
T0224	Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions).	Review	16.1, 16.2, 16.3	3	90% or .9
T0230	Support the design and execution of exercise scenarios.	Design	6.1, 6.2	3	90% or .9
T0247	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	Write, Synthesis	5.2, 8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
T0316	Develop or assist in the development of computer based training modules or classes.	Analysis, Synthesis	5.1, 5.2, 5.3	3	90% or .9
T0317	Develop or assist in the development of course assignments.	Analysis, Synthesis	14.1	3	90% or .9
T0318	Develop or assist in the development of course evaluations.	Analysis, Synthesis	14.1	3	90% or .9
T0319	Develop or assist in the development of grading and proficiency standards.	Analysis, Synthesis	16.1, 16.2, 16.3	3	90% or .9
T0320	Assist in the development of individual/collective development, training, and/or remediation plans.	Assist	3, 4, 2005	4	100% or 1
T0321	Develop or assist in the development of learning objectives and goals.	Analysis, Synthesis	8.1	3	90% or .9
T0322	Develop or assist in the development of on-the-job training materials or programs.	Analysis, Synthesis	8.1, 8.2, 8.3., 8.4, 8.5	4	100% or 1
T0323	Develop or assist in the development of written tests for measuring and assessing learner proficiency.	Analysis, Synthesis	10.1, 10.2, 12.1	4	100% or 1
T0443	Deliver training courses tailored to the audience and physical/virtual environments.	Deliver	13.1, 13.2, 13.3	3	90% or .9

NCWF JOB ROLE

Cyber Instructor

Job Role Description: A Cyber Instructor develops and conducts training or education of personnel within cyber domain.

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructor. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0444	Apply concepts, procedures, software, equipment, and/or technology applications to students.	Apply	1 - 16	3	90% or .9
T0450	Design training curriculum and course content based on requirements.	Design, Analysis, Synthesis	8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
T0467	Ensure training meets the goals and objectives for cybersecurity training, education, or awareness.	Analysis, Evaluation	14.1, 15.1, 15.2	4	100% or 1
T0519	Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for most effective learning environment.	Analysis, Evaluation	8.4, 8.5, 13.1, 13.2, 13.3	3	90% or .9
T0520	Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses).	Analysis	13.2, 13.3	3	90% or .9
T0535	Recommend revisions to curriculum end course content based on feedback from previous training sessions.	Analysis	11.1, 11.2	3	90% or .9
T0536	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Analysis	3.1, 3.2, 3.3	3	90% or .9
T0926	Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations	Develop, Analysis, Synthesis	2.1, 2.2, 5.1, 6.1, 6.2, 8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
	Summary			**4**	**95% or .95**

NCWF JOB ROLE

Cyber Instructor

Job Role Description: A Cyber Instructor develops and conducts training or education of personnel within cyber domain.

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructor. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	NA		
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	NA		
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	18.2	2	50% or .5
K0004	* Knowledge of cybersecurity principles.	18.2	2	50% or .5
K0005	* Knowledge of cyber threats and vulnerabilities.	18.2	2	50% or .5
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	18.2	2	50% or .5
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	18.2	2	50% or .5
K0115	Knowledge of emerging computer-based technology that has potential for exploitation by adversaries.	18.2	3	60% or .6
K0124	Knowledge of multiple cognitive domains and appropriate tools and methods for learning in each domain.	18.2, 18.4, 18.6	3	60% or .6
K0130	Knowledge of virtualization technologies and virtual machine development and maintenance.	All Labs	3	60% or .6
K0146	Knowledge of the organization's core business/mission processes.	1.1 to 1.9	3	100% or 1
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	18.2, 18.4, 18.6	3	60% or .6
K0204	Knowledge of assessment techniques (rubrics, evaluation plans, tests, quizzes).	14.1	3	60% or .6
K0208	Knowledge of computer based training and e-learning services.	3.1, 3.2, 3.3	3	70% or .7
K0213	Knowledge of instructional design and evaluation models (e.g., ADDIE, Smith/Ragan model, Gagne's Events of Instruction, Kirkpatrick's model of evaluation).	14.1, 15.1, 15.2	4	100% or 1
K0215	Knowledge of organizational training policies.	17.5	3	90% or .9
K0216	Knowledge of learning levels (i.e., Bloom's Taxonomy of learning).	10.1	3	90% or .9
K0217	Knowledge of Learning Management Systems and their use in managing learning.	10.1, 12.1, 16.1, 16.2, 16.3	4	100% or 1
K0218	Knowledge of learning styles (e.g., assimilator, auditory, kinesthetic).	3.2, 8.4, 16.1, 16.2, 16.3	3	85% or .85
K0220	Knowledge of modes of learning (e.g., rote learning, observation).	12.1	3	80% or .8

NCWF JOB ROLE

Cyber Instructor

Job Role Description: A Cyber Instructor develops and conducts training or education of personnel within cyber domain.

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructor. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0226	Knowledge of organizational training systems.	16.1, 16.2, 16.3	3	90% or .9
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	4.1, 4.2, 4.3	3	90% or .9
K0319	Knowledge of technical delivery capabilities and their limitations.	6.1, 6.2	4	100% or 1
S0064	Skill in developing and executing technical training programs and curricula.	8.1, 8.2, 8.3, 8.4, 8.5, 13.1, 13.2, 13.3	4	100% or 1
S0070	Skill in talking to others to convey information effectively.	12.1	3	90% or .9
S0100	Skill in utilizing or developing learning activities (e.g., scenarios, instructional games, interactive exercises).	6.1, 6.2, 8.1, 8.2, 8.3, 8.4, 8.5, 10.1, 10.2, 13.1, 13.2, 13.3, 14.1, 15.1, 15.2, 16.1, 16.2, 16.3	4	100% or 1
S0101	Skill in utilizing technologies (e.g., SmartBoards, websites, computers, projectors) for instructional purposes.	6.1, 6.2	3	90% or .9
A0006	Ability to prepare and deliver education and awareness briefings to ensure that systems, network, and data users are aware of and adhere to systems security policies and procedures.	Module 01	4	100% or 1
A0011	Ability to answer questions in a clear and concise manner.	10.1, 10.2	4	100% or 1
A0012	Ability to ask clarifying questions.	10.1, 10.2	4	100% or 1
A0013	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	3.1, 3.2, 3.3	4	100% or 1
A0014	Ability to communicate effectively when writing.	3.3	4	100% or 1
A0016	Ability to facilitate small group discussions.	9.3, 11.2	3	90% or .9
A0017	Ability to gauge learner understanding and knowledge level.	12.1	3	90% or .9
A0020	Ability to provide effective feedback to students for improving learning.	11.1	3	90% or .9
A0022	Ability to apply principles of adult learning.	10.1, 12.1, 13.1, 16.1, 16.2, 16.3	3	90% or .9

NCWF JOB ROLE

Cyber Instructor

Job Role Description: A Cyber Instructor develops and conducts training or education of personnel within cyber domain.

Maps To: Certified EC-Council Instructor (CEI)

Mapping Summary: Performance-based learning and evaluation in CEI imparts specific KSAs that should be demonstrated by a Cyber Instructor. CEI maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
A0023	Ability to design valid and reliable assessments.	14.1	4	100% or 1
A0024	Ability to develop clear directions and instructional materials.	8.1, 8.2, 8.3, 8.4, 8.5	3	90% or .9
A0057	Ability to tailor curriculum that speaks to the topic at the appropriate level for the target audience.	8.1, 8.2, 8.3, 8.4, 8.5	4	100% or 1
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0001	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	Synthesis, Evaluation	2.1.3, 3.4, 4.33, 4.4.2, 5.2.2,5.2.3	4	100% or 1
T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	Synthesis, Evaluation	5.2.2,5.2.3	4	100% or 1
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Synthesis, Evaluation	2.1.1, 4.4	4	100% or 1
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, and systems, and elements.	Synthesis, Evaluation	1.4, 3.3, 5.2.4, 5.2.8	4	100% or 1
T0005	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.	Synthesis, Evaluation	4.4.9	4	100% or 1
T0024	Collect and maintain data needed to meet system cybersecurity reporting.	Analysis, Evaluation	2.1.8	**3**	40% or .40
T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Analysis, Evaluation	1.13, 1.14, 3.13	3	90% or .9
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Synthesis, Evaluation	4.5.1,4.5.2	4	100% or 1
T0089	Ensure security improvement actions are evaluated, validated, and implemented as required.	Synthesis, Evaluation	3.14	4	100% or 1
T0091	Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.	Analysis, Evaluation	1.13	**3**	40% or .40
T0092	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).	Synthesis, Evaluation	4.5.9	4	100% or 1

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0093	Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture.	Synthesis, Evaluation	4.6.1	4	100% or 1
T0095	Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy.	Synthesis, Evaluation	5.1.1	4	100% or 1
T0097	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.	Analysis, Evaluation	3.1	3	60% or .60
T0099	Evaluate cost benefit, economic, and risk analysis in decision making process.	Analysis, Evaluation	3.11	3	60% or .60
T0106	Identify alternative information security strategies to address organizational security objective.	Analysis, Evaluation	5.14	3	40% or .40
T0115	Identify information technology (IT) security program implications of new technologies or technology upgrades.	Analysis, Evaluation	3.14	3	40% or .40
T0130	Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information.	Analysis, Evaluation	1.7, 1.13, 1.14, 4.4.5, 5.1.2	3	90% or .9
T0132	Interpret and/or approve security requirements relative to the capabilities of new information technologies.	Analysis, Evaluation	5.2.11	3	40% or .40
T0133	Interpret patterns of non-compliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	Synthesis, Evaluation	1.6, 1.12, 1.16, 1.17, 1.19, 4.4	4	100% or 1
T0134	Lead and align information technology (IT) security priorities with the security strategy.	Analysis, Evaluation	5.1.1	3	40% or .40
T0135	Lead and oversee information security budget, staffing, and contracting.	Synthesis, Evaluation	3.3	4	60% or .60
T0147	Manage the monitoring of information security data sources to maintain organizational situational awareness.	Synthesis, Evaluation	5.1.7	4	60% or .60

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0148	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.	Analysis, Evaluation	1.11, 3.7, 5.1.1	3	60% or .60
T0149	Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.	Analysis, Evaluation	4.4.8	3	60% or .60
T0151	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure they provide the intended level of protection.	Synthesis, Evaluation	3.12,5.1.5	4	100% or 1
T0157	Oversee the information security training and awareness program.	Analysis, Evaluation	3.6	3	60% or .60
T0158	Participate in an information security risk assessment during the Security Assessment and Authorization process.	Synthesis, Evaluation	4.4.3	4	60% or .60
T0159	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.	Synthesis, Evaluation	5.1.4	4	60% or .60
T0192	Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.	Application, Analysis	1.13	3	60% or .60
T0199	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Synthesis, Evaluation	4.5.5., 4.5.8	4	60% or .60
T0206	Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.	Synthesis, Evaluation	3.7	4	60% or .60
T0211	Provide system related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.	Synthesis, Evaluation	5.2.15	4	100% or 1
T0213	Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.	Synthesis, Evaluation	2.1.8	4	100% or 1

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0215	Recognize a possible security violation and take appropriate action to report the incident, as required.	Synthesis, Evaluation	4.13.1, 4.13.6	4	100% or 1
T0219	Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.	Synthesis, Evaluation	2.13	4	100% or 1
T0227	Recommend policy and coordinate review and approval.	Synthesis, Evaluation	1.13	4	100% or 1
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Synthesis, Evaluation	4.12.5,4.13.5	4	100% or 1
T0234	Track audit findings and recommendations to ensure appropriate mitigation actions are taken.	Synthesis, Evaluation	2.2.7	4	100% or 1
T0239	Use federal and organization-specific published documents to manage operations of their computing environment system(s).	Analysis	3.1	3	40% or .40
T0248	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Analysis	3.1	3	40% or .40
T0254	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.	Synthesis, Evaluation	1.1 to 1.18	4	40% or .40
T0255	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.	Synthesis, Evaluation	1.1	4	100% or 1
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Synthesis, Evaluation	5.2.8,5.2.14	4	100% or 1
T0263	Identify security requirements specific to an information technology (IT) system in all phases of the System Life Cycle.	Synthesis, Evaluation	4.9.1	4	100% or 1
T0264	Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Synthesis, Evaluation	4.4.9	4	60% or .60

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0265	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.	Synthesis, Evaluation	1.1 to 1.18	4	100% or 1
T0275	Support necessary compliance activities (e.g., ensure system security configuration guidelines are followed, compliance monitoring occurs).	Synthesis, Evaluation	1.1 to 1.18	4	100% or 1
T0276	Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.	Analysis, Evaluation	4.4.9	3	60% or .60
T0277	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Synthesis, Evaluation	5.2.11	4	60% or .60
T0280	Continuously validate the organization against policies/guidelines/procedures/ regulations/laws to ensure compliance.	Synthesis, Evaluation	1.1 to 1.18	4	60% or .60
T0281	Forecast ongoing service demands and ensure security assumptions are reviewed as necessary.	Synthesis, Evaluation	5.2.1	4	60% or .60
T0282	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Application, Analysis	1.1 to 1.18	3	60% or .60
	Summary			**4**	**90% or .9**

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0008	Knowledge of applicable business processes and operations of customer organizations.	5.11	3	40% or .40
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	4.11	3	60% or .6
K0021	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.	4.5.10	3	60% or .6
K0026	Knowledge of disaster recovery continuity of operations plans.	4.5.1 to 4.5.10	3	100% or 1
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	4.1, 4.6.3, 4.6.9	3	100% or 1
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	4.5.9	3	100% or 1
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	4.4.8, 4.6.7, 4.7.1, 4.9.4, 4.9.6, 4.10.1, 4.12	3	90% or .9
K0042	Knowledge of incident response and handling methodologies.	4.4.5, 4.4.6, 4.13	3	90% or .9
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	1.1 to 1.18	3	90% or .9
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	4.6	3	90% or .9

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4.9	4	100% or 1
K0053	Knowledge of measures or indicators of system performance and availability.	NA		
K0054	Knowledge of current industry methods for evaluating, implementing, and disseminating information technology (IT) security assessment, monitoring, detection, and remediation tools and procedures utilizing standards-based concepts and capabilities.	2.2.1 to 2.2.7	3	90% or .9
K0058	Knowledge of network traffic analysis methods.	NA		
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	2.1.3	4	90% or .9
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	NA		
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	4.2, 4.9,4.10,	3	60% or .60
K0072	Knowledge of resource management principles and techniques.	3.4	4	100% or 1
K0076	Knowledge of server administration and systems engineering theories, concepts, and methods.	NA		
K0077	Knowledge of server and client operating systems.	NA		
K0087	Knowledge of system software and organizational design standards, policies, and authorized approaches (e.g., International Organization for Standardization [ISO] guidelines) relating to system design.	1.1 to 1.10	4	100% or 1
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1 to 4.9.6	3	60% or .60
K0092	Knowledge of technology integration processes.	2.1.4	3	60% or .60
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	2.1.1	4	60% or .60
K0106	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	4.6	3	60% or .60

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0121	Knowledge of information security program management and project management principles and techniques.	3.1 to 3.14	4	100% or 1
K0126	Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management).	5.2.11	4	100% or 1
K0149	Knowledge of organization's risk tolerance and/or risk management approach.	2.1.1,4.4.1	4	100% or 1
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	4.4.5, 4.4.6, 4.13	3	90% or .9
K0151	Knowledge of current and emerging threats/threat vectors.	1.15	3	90% or .9
K0163	Knowledge of critical information technology (IT) procurement requirements.	5.2.15	3	90% or .9
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	4.10	3	90% or .9
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	1.1 to 1.19	**3**	95% or .95
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4.9	3	95% or .95
K0170	Knowledge of local specialized system requirements (e.g., critical infrastructure systems that may not use standard information technology [IT]) for safety, performance, and reliability.	2.1.3, 5.1.1	3	90% or .9
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	4.6.4	3	60% or .60
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	4.6	3	60% or .60
K0199	Knowledge of security architecture concepts and enterprise architecture reference models (e.g., Zachman, Federal Enterprise Architecture [FEA]).	5.1.1	3	60% or .60

NCWF JOB ROLE

Information Systems Security Manager

Job Role Description: A Information Systems Security Manager is responsible for the cybersecurity of a program, organization, system, or enclave.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Information Systems Security Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	1.1 to 1.19	**3**	95% or .95
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	1.1 to 1.19	**3**	95% or .95
K0262	Knowledge of Personal Health Information (PHI) data security standards.	1.1 to 1.19	**3**	95% or .95
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	1.1 to 1.19	**3**	95% or .95
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	4.1	2	40% or .4
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	4.6.4	2	40% or .4
K0342	Knowledge of penetration testing principles, tools, and techniques.	4.12	3	60% or .60
S0018	Skill in creating policies that reflect system security objectives.	1.1 to 1.19	**3**	95% or .95
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	4.1 - 4.13	3	90% or .9
S0086	Skill in evaluating the trustworthiness of the supplier and/or product.	5.2.10 - 5.2.14	3	90% or .9
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

COMSEC Manager

Job Role Description: A COMSEC Manager Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a COMSEC Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0003	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Synthesis, Evaluation	2.1.1, 4.4	4	100% or 1
T0004	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, and systems, and elements.	Synthesis, Evaluation	1.4, 3.3, 5.2.4, 5.2.8	4	100% or 1
T0025	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Synthesis, Evaluation	NA		
T0044	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Synthesis, Evaluation	4.5.1,4.5.2	4	100% or 1
T0089	Ensure security improvement actions are evaluated, validated, and implemented as required.	Synthesis, Evaluation	3.14	4	100% or 1
T0095	Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy.	Synthesis, Evaluation	5.1.1	4	100% or 1
T0099	Evaluate cost benefit, economic, and risk analysis in decision making process.	Synthesis, Evaluation	3.11	3	60% or .60
T0215	Recognize a possible security violation and take appropriate action to report the incident, as required.	Synthesis, Evaluation	4.13.1, 4.13.6	4	100% or 1
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Synthesis, Evaluation	4.12.5,4.13.5	4	100% or 1
	Summary			**4**	**100% or 1**

NCWF JOB ROLE

COMSEC Manager

Job Role Description: A COMSEC Manager Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a COMSEC Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	4.11	3	60% or .6
K0026	Knowledge of disaster recovery continuity of operations plans.	4.5.1 to 4.5.10	4	100% or 1
K0038	Knowledge of cybersecurity principles used to manage risks related to the use, processing, storage, and transmission of information or data.	4.5.9	4	100% or 1
K0042	Knowledge of incident response and handling methodologies.	4.4.5, 4.4.6, 4.13	3	60% or .6
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1 to 4.9.6	3	60% or .60
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	2.1.1	4	60% or .60
K0121	Knowledge of information security program management and project management principles and techniques.	3.1 to 3.14	4	100% or 1
K0126	Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management).	5.2.11	4	100% or 1
K0163	Knowledge of critical information technology (IT) procurement requirements.	5.2.15	3	60% or .60
K0267	Knowledge of relevant laws, policies, procedures, or governance related to critical infrastructure.	1.1 to 1.19	**3**	95% or .95

NCWF JOB ROLE

COMSEC Manager

Job Role Description: A COMSEC Manager Manages the Communications Security (COMSEC) resources of an organization (CNSSI 4009).

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a COMSEC Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	4.1	2	40% or .4
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	4.1 - 4.13	3	60% or .60
	Summary		**3**	**80% or .8**

NCWF JOB ROLE

Cyber Workforce Developer and Manager

Job Role Description: Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist (level 3) with a correlation coefficient of .5 on the framework tasks and .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0074	Develop policy, programs, and guidelines for implementation.	Synthesis, Evaluation	1.1	4	60% or .6
T0094	Establish and maintain communication channels with stakeholders.	Application, Analysis	3.13	**3**	80% or .8
T0116	Identify organizational policy stakeholders.	Analysis	1.14	3	60% or .6
T0222	Review existing and proposed policies with stakeholders.	Analysis	1.7	3	40% or .4
T0226	Serve on agency and interagency policy boards.	Analysis	1.1 to 1.20	3	40% or .4
T0341	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Analysis	3.8	**3**	40% or .4
T0355	Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.	Analysis	NA		
T0356	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	Analysis	2.1.3	3	40% or .4
T0362	Develop and implement standardized position descriptions based on established cyber work roles.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0363	Develop and review recruiting, hiring, and retention procedures in accordance with current Human Resource (HR) policies.	Application, Analysis	NA		
T0364	Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0368	Ensure cyber career fields are managed in accordance with organizational Human Resource (HR) policies and directives.	Analysis	NA		
T0369	Ensure cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/ employment practices.	Analysis	NA		

NCWF JOB ROLE

Cyber Workforce Developer and Manager

Job Role Description: Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist (level 3) with a correlation coefficient of .5 on the framework tasks and .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0372	Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0373	Establish and oversee waiver processes for cyber career field entry and training qualification requirements.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0374	Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0375	Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0376	Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements.	Application, Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0384	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Application, Analysis	1.1 to 1.20	3	40% or .4
T0387	Review and apply cyber career field qualification standards.	Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0388	Review and apply organizational policies related to or having an effect on the cyber workforce.	Analysis	1.1 to 1.20	3	40% or .4
T0390	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0391	Support integration of qualified cyber workforce personnel into information systems lifecycle development processes.	Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	3	40% or .4
T0408	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	Analysis	1.1 to 1.20	4	100% or 1
T0425	Analyze organizational cyber policy.	Synthesis, Evaluation	1.1 to 1.20	4	100% or 1

NCWF JOB ROLE

Cyber Workforce Developer and Manager

Job Role Description: Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist (level 3) with a correlation coefficient of .5 on the framework tasks and .5 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Analysis, Evaluation	1.1 to 1.20	3	100% or 1
T0441	Define and integrate current and future mission environments.	Application, Analysis	5.1.1 to 5.1.7	4	100% or 1
T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	Synthesis, Evaluation	5.1.1 to 5.1.7	4	100% or 1
T0472	Draft, staff, and publish cyber policy.	Analysis	1.1 to 1.20	3	40% or .4
T0481	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Analysis	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .4
T0505	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Analysis	1.1 to 1.20	3	40% or .4
T0506	Seek consensus on proposed policy changes from stakeholders.	Analysis	1.1 to 1.20	3	40% or .4
T0529	Provide policy guidance to cyber management, staff, and users.	Analysis	1.1 to 1.20	3	40% or .4
T0533	Review, conduct, or participate in audits of cyber programs and projects.	Analysis, Evaluation	2.2.1 to 2.2.7	3	40% or .4
T0537	Support the CIO in the formulation of cyber-related policies.	Analysis	1.1 to 1.20	3	40% or .4
T0552	Review and approve a supply chain security/risk management policy.	Analysis, Evaluation	1.1 to 1.20	3	40% or .4
	Summary			**3**	**50% or .5**

NCWF JOB ROLE

Cyber Workforce Developer and Manager

Job Role Description: Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist (level 3) with a correlation coefficient of .5 on the framework tasks and .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	4.2, 4.9,4.10,	3	60% or .60
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).	NA		
K0146	Knowledge of the organization's core business/mission processes.	3.1	3	40% or .40
K0166	Knowledge of the nature and function of the relevant information structure.	NA		
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	1.1 to 1.20	3	40% or .40
K0233	Knowledge of the National Cybersecurity Workforce Framework, work roles, and associated tasks, knowledge, skills, and abilities.	NA		
K0234	Knowledge of full spectrum cyber capabilities.	NA		
K0241	Knowledge of organizational human resource policies, processes, and procedures.	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .40

NCWF JOB ROLE

Cyber Workforce Developer and Manager

Job Role Description: Develops cyberspace workforce plans, strategies and guidance to support cyberspace workforce manpower, personnel, training and education requirements and to address changes to cyberspace policy, doctrine, materiel, force structure, and education and training requirements.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist (level 3) with a correlation coefficient of .5 on the framework tasks and .5 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0243	Knowledge of organizational training and education policies, processes, and procedures.	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .40
K0309	Knowledge of emerging technologies that have potential for exploitation by adversaries.	1.15	2	40% or .40
K0311	Knowledge of industry indicators useful for identifying technology trends.	1.15	2	40% or .40
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/ training and Research & Development).	NA		
K0335	Knowledge of current and emerging cyber technologies.	1.15	2	40% or .40
S0108	Skill in developing workforce and position qualification standards.	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .40
S0128	Skill in using manpower and personnel IT systems.	3.1 to 3.14	2	40% or .40
A0028	Ability to assess and forecast manpower requirements to meet organizational objectives.	5.1.4, 5.2.1	2	40% or .40
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	1.1 to 1.20	3	40% or .40
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	NA		
A0042	Ability to develop career path opportunities.	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .40
A0053	Ability to determine the validity of workforce trend data.	1.6, 3.5, 3.7, 4.4.4, 4.13.11	2	40% or .40
	Summary		**3**	**50% or .5**

NCWF JOB ROLE

Cyber Policy and Strategy Planner

Job Role Description: A Cyber Policy and Strategy Planner develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Policy and Strategy Planner. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .6 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0074	Develop policy, programs, and guidelines for implementation.	Synthesis, Evaluation	1.1	4	95% or .95
T0094	Establish and maintain communication channels with stakeholders.	Synthesis, Evaluation	**3.13**	**4**	95% or .95
T0222	Review existing and proposed policies with stakeholders.	Evaluation	1.7	4	95% or .95
T0226	Serve on agency and interagency policy boards.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
T0341	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Analysis	**3.8**	3	80% or .8
T0369	Ensure cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/ employment practices.	Analysis, Evaluation	NA		95% or .95
T0384	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Evaluation	1.1 to 1.20	4	95% or .95
T0390	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	Analysis, Evaluation	1.6, 3.5, 3.7, 4.4.4, 4.13.11	3	80% or .8
T0408	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	Evaluation	1.1 to 1.20	3	95% or .95
T0425	Analyze organizational cyber policy.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Evaluation	1.1 to 1.20	4	95% or .95
T0441	Define and integrate current and future mission environments.	Synthesis, Evaluation	**5.1.1 to 5.1.7**	**3**	95% or .95
T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	Synthesis, Evaluation	**5.1.1 to 5.1.7**	**3**	95% or .95
T0472	Draft, staff, and publish cyber policy.	Synthesis, Evaluation	1.1 to 1.20	4	95% or .95

NCWF JOB ROLE

Cyber Policy and Strategy Planner

Job Role Description: A Cyber Policy and Strategy Planner develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Policy and Strategy Planner. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .6 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0505	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
T0506	Seek consensus on proposed policy changes from stakeholders.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
T0529	Provide policy guidance to cyber management, staff, and users.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
T0533	Review, conduct, or participate in audits of cyber programs and projects.	Analysis, Evaluation	2.2.1 to 2.2.7	4	95% or .95
T0537	Support the CIO in the formulation of cyber-related policies.	Analysis, Evaluation	1.1 to 1.20	4	95% or .95
	Summary			**4**	**95% or .95**

NCWF JOB ROLE

Cyber Policy and Strategy Planner

Job Role Description: A Cyber Policy and Strategy Planner develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Policy and Strategy Planner. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .6 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	4.2, 4.9,4.10,	3	60% or .6
K0127	Knowledge of the nature and function of the relevant information structure (e.g., National Information Infrastructure).	NA		
K0146	Knowledge of the organization's core business/mission processes.	3.1	3	40% or .4
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	1.1 to 1.20	3	40% or .4
K0234	Knowledge of full spectrum cyber capabilities.	NA		
K0248	Knowledge of strategic theory and practice.	5.1	2	40% or .4
K0309	Knowledge of emerging technologies that have potential for exploitation by adversaries.	1.15	2	40% or .4
K0311	Knowledge of industry indicators useful for identifying technology trends.	1.15	2	40% or .4
K0313	Knowledge of external organizations and academic institutions with cyber focus (e.g., cyber curriculum/ training and Research & Development).	NA		
K0335	Knowledge of current and emerging cyber technologies.	1.15	2	40% or .4

NCWF JOB ROLE

Cyber Policy and Strategy Planner

Job Role Description: A Cyber Policy and Strategy Planner develops cyberspace plans, strategy and policy to support and align with organizational cyberspace missions and initiatives.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Policy and Strategy Planner. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and .6 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
A0003	Ability to determine the validity of technology trend data.	PM	2	40% or .4
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	1.1 to 1.20	3	40% or .4
A0037	Ability to leverage best practices and lessons learned of external organizations and academic institutions dealing with cyber issues.	NA		
	Summary		**3**	**60% or .6**

NCWF JOB ROLE

Executive Cyber Leadership

Job Role Description: A Executive Cyber Leadership executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0001	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	Evaluation	5.2.2	4	100% or 1
T0002	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	Evaluation	**5.2.3**	**4**	100% or 1
T0006	Advocate organization's official position in legal and legislative proceedings.	Evaluation	1.5	4	60% or .6
T0066	Develop and maintain strategic plans.	Synthesis, Evaluation	5.1	4	100% or 1
T0157	Oversee the information security training and awareness program.	Evaluation	**3.6**	**4**	90% or .9
T0229	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Evaluation	4.12.4	4	90% or .9
T0264	Ensure plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Analysis, Evaluation	2.2.7	3	90% or .9
T0282	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Synthesis, Evaluation	2.1.5	4	90% or .9
T0337	Supervise and assign work to programmers, designers, technologists and technicians and other engineering and scientific personnel.	Evaluation	3.6	3	60% or .6
T0356	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	Analysis	2.1.3	3	40% or .4
T0429	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Evaluation	1.5	3	60% or .6
T0445	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	Synthesis, Evaluation	5.1.4	4	90% or .9
T0509	Perform an information security risk assessment.	Evaluation	4.4.3	4	90% or .9

NCWF JOB ROLE

Executive Cyber Leadership

Job Role Description: A Executive Cyber Leadership executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0763	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Analysis, Evaluation	5.1.2	4	90% or .9
T0871	Collaborate on cyber privacy and security policies and procedures	Analysis, Evaluation	1.13	4	90% or .9
T0872	Collaborate with cyber security personnel on the security risk assessment process to address privacy compliance and risk mitigation	Analysis, Evaluation	1.12	4	90% or .9
T0927	Appoint and guide a team of IT security experts	Analysis, Evaluation	2.1.3,3.7	4	90% or .9
T0928	Collaborate with key stakeholders to establish a cybersecurity risk management program	Analysis, Evaluation	4.4.3	4	90% or .9
	Summary			**4**	**90% or .9**

NCWF JOB ROLE

Executive Cyber Leadership

Job Role Description: A Executive Cyber Leadership executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0009	Knowledge of application vulnerabilities.	4.9	3	60% or .6
K0085	Knowledge of system and application security threats and vulnerabilities.	4.9	3	60% or .6
K0106	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	4.2, 4.4.8, 4.4.9, 4.6.7, 4.7.1, 4.8, 4.9.6, 4.10.1, 4.12.2	4	90% or .9
K0314	Knowledge of industry technologies and how differences affect exploitation/vulnerabilities.	4.2, 4.4.8, 4.4.9, 4.6.7, 4.7.1, 4.8, 4.9.6, 4.10.1, 4.12.3	3	90% or .9
K0296	Knowledge of capabilities, applications, and potential vulnerabilities of network equipment including hubs, routers, switches, bridges, servers, transmission media, and related hardware.	4.2, 4.4.8, 4.4.9, 4.6.7, 4.7.1, 4.8, 4.9.6, 4.10.1, 4.12.4	4	90% or .9
K0147	Knowledge of emerging security issues, risks, and vulnerabilities.	4.2, 4.4.8, 4.4.9, 4.6.7, 4.7.1, 4.8, 4.9.6, 4.10.1, 4.12.5	4	90% or .9
S0356	Skill in communicating with all levels of management including Board members (e.g., interpersonal skills, approachability, effective listening skills, appropriate use of style and language for the audience).	3.7	3	95% or .95
S0357	Skill to anticipate new security threats.	1.15	3	95% or .95

NCWF JOB ROLE

Executive Cyber Leadership

Job Role Description: A Executive Cyber Leadership executes decision-making authorities and establishes vision and direction for an organization's cyber and cyber-related resources and/or operations.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
S0358	Skill to remain aware of evolving technical infrastructures.	1.15	3	95% or .95
S0359	Skill to use critical thinking to analyze organizational patterns and relationships.	5.1.2	3	95% or .95
A0033	Ability to develop policy, plans, and strategy in compliance with laws, regulations, policies, and standards in support of organizational cyber activities.	1.5	3	95% or .95
A0070	Ability to apply critical reading/thinking skills.	5.1	2	60% or .6
A0085	Ability to exercise judgment when policies are not well-defined.	1.16	2	60% or .6
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.	1.15	3	95% or .95
A0105	Ability to tailor technical and planning information to a customer's level of understanding.	5.13	2	60% or .6
A0106	Ability to think critically.	5.1	2	60% or .6
A0116	Ability to prioritize and allocate cybersecurity resources correctly and efficiently.	4.5.4	2	60% or .6
A0117	Ability to relate strategy, business, and technology in the context of organizational dynamics.	5.1	3	95% or .95
A0118	Ability to understand technology, management, and leadership issues related to organization processes and problem solving.	3.1 to 3.14	2	95% or .95
A0119	Ability to understand the basic concepts and issues related to cyber and its organizational impact.	4.13.3	2	60% or .6
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

Program Manager

Job Role Description: A Program Manager leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0066	Develop and maintain strategic plans.	Synthesis, Evaluation	5.1	4	95% or .95
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Synthesis, Evaluation	1.12	4	95% or .95
T0174	Perform needs analysis to determine opportunities for new and improved business process solutions.	Analysis, Evaluation	5.1.1,5.1.2	4	95% or .95
T0199	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Synthesis, Evaluation	4.4.2,4.4.3	4	95% or .95
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Analysis, Evaluation	1.5,1.7	3	90% or .9
T0223	Review or conduct audits of information technology (IT) programs and projects.	Evaluation	2.2	4	90% or .9
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Evaluation	5.2.4	3	90% or .9
T0273	Develop and document supply chain risks for critical system elements, as appropriate.	Application, Analysis	5.2.11	3	90% or .9
T0277	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Application, Analysis	5.2.11	3	90% or .9
T0302	Develop contract language to ensure supply chain, system, network, and operational security are met.	Application, Analysis	5.2.11	3	90% or .9
T0340	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Application, Analysis	3.1	3	90% or .9
T0354	Coordinate and manage the overall service provided to a customer end-to-end.	Application, Analysis	3.7	3	90% or .9
T0377	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Application, Analysis	3.11	3	80% or .8

NCWF JOB ROLE

Program Manager

Job Role Description: A Program Manager leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0379	Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).	Application, Analysis	NA		
T0407	Participate in the acquisition process as necessary.	Application, Analysis	5.2.11	3	90% or .9
T0412	Conduct import/export reviews for acquiring systems and software.	Analysis, Evaluation	3.4	4	90% or .9
T0414	Develop supply chain, system, network, performance, and cyber security requirements.	Application, Analysis	5.2.11	3	90% or .9
T0415	Ensure supply chain, system, network, performance, and cyber security requirements are included in contract language and delivered.	Application, Analysis	5.2.11	3	90% or .9
T0481	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Analysis	1.6, 3.5, 3.7, 3.3, 4.4.4, 4.13.11, 5.2.1	3	80% or .8
T0493	Lead and oversee budget, staffing, and contracting.	Analysis	1.6, 3.5, 3.7, 3.3, 4.4.4, 4.13.11, 5.2.2	3	80% or .8
T0551	Draft and publish supply chain security and risk management documents.	Application, Analysis	4.4	3	60% or .6
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

Program Manager

Job Role Description: A Program Manager leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0047	Knowledge of information technology (IT) architectural concepts and frameworks.	5.1.1	3	90% or .9
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	3	90% or .9
K0072	Knowledge of resource management principles and techniques.	3.4	3	90% or .9
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1	3	90% or .9
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	2.1.1	3	90% or .9
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	3.1 to 3.14	2	60% or .6
K0146	Knowledge of the organization's core business/mission processes.	2.1.1	3	95% or .95
K0148	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	NA		
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0164	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	NA		
K0165	Knowledge of risk threat assessment.	4.4		95% or .95

NCWF JOB ROLE

Program Manager

Job Role Description: A Program Manager leads, coordinates, communicates, integrates, and is accountable for the overall success of the program, ensuring alignment with critical agency priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Cyber Workforce Developer and Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	3	90% or .9
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.	5.1.1	3	90% or .9
K0196	Knowledge of Import/Export Regulations related to cryptography and other security technologies.	4.11	3	90% or .9
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	1.1,12	3	90% or .9
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	NA		
K0235	Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.	NA		
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.	5.2.11	3	90% or .9
K0270	Knowledge of the acquisition/procurement life cycle process.	5.2.7	3	90% or .9
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	5.5	4	90% or .9
A0009	Ability to apply supply chain risk management standards.	NA		
A0039	Ability to oversee the development and update of the lifecycle cost estimate.	5.2.11	3	90% or .9
A0045	Ability to evaluate/ensure the trustworthiness of the supplier and/or product.	5.2.11	3	90% or .9
A0056	Ability to ensure security practices are followed throughout the acquisition process.	4.13.13	3	90% or .9
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

IT Project Manager

Job Role Description: An IT Project Manager directly manages information technology projects to provide a unique service or product.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Project Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Synthesis, Evaluation	1.12	4	95% or .95
T0174	Perform needs analysis to determine opportunities for new and improved business process solutions.	Analysis	5.1.1,5.1.2	4	95% or .95
T0196	Provide advice on project costs, design concepts, or design changes.	Analysis	3.3	3	60% or .60
T0199	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Analysis	4.4.2,4.4.3	4	95% or .95
T0207	Provide ongoing optimization and problem solving support.	Analysis	2.1.8	4	95% or .95
T0208	Provide recommendations for possible improvements and upgrades.	Analysis	3.14	4	95% or .95
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Analysis	1.5,1.7	3	90% or .9
T0223	Review or conduct audits of information technology (IT) programs and projects.	Analysis	2.2	4	90% or .9
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Analysis	5.2.4	3	90% or .9
T0273	Develop and document supply chain risks for critical system elements, as appropriate.	Analysis	5.2.11	3	90% or .9
T0277	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Analysis	5.2.11	3	90% or .9
T0340	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Analysis	3.1	3	90% or .9
T0354	Coordinate and manage the overall service provided to a customer end-to-end.	Analysis	3.7	3	90% or .9
T0370	Ensure that appropriate Service Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.	Analysis	5.2.11	3	90% or .9

NCWF JOB ROLE

IT Project Manager

Job Role Description: An IT Project Manager directly manages information technology projects to provide a unique service or product.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Project Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0377	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Analysis	3.11	3	90% or .9
T0379	Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).	Analysis	NA		
T0389	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Analysis	5.1.5	3	90% or .9
T0394	Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.	Analysis	4.5.4	3	90% or .9
T0407	Participate in the acquisition process as necessary.	Analysis	5.2.11	3	90% or .9
T0412	Conduct import/export reviews for acquiring systems and software.	Analysis	3.4	3	90% or .9
T0414	Develop supply chain, system, network, performance, and cyber security requirements.	Analysis	5.2.11	3	90% or .9
T0415	Ensure supply chain, system, network, performance, and cyber security requirements are included in contract language and delivered.	Analysis	5.2.11	3	90% or .9
T0481	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Analysis	1.6, 3.5, 3.7, 3.3, 4.4.4, 4.13.11, 5.2.1	2	90% or .9
T0493	Lead and oversee budget, staffing, and contracting.	Analysis	4.4	3	90% or .9
T0551	Draft and publish supply chain security and risk management documents.	Application, Analysis	4.4	3	60% or .6
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

IT Project Manager

Job Role Description: An IT Project Manager directly manages information technology projects to provide a unique service or product.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Project Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0012	Knowledge of capabilities and requirements analysis.	3.11	3	90% or .9
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	1.7	3	90% or .9
K0047	Knowledge of information technology (IT) architectural concepts and frameworks.	5.1.1	3	90% or .9
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	3	90% or .9
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	2.1.3	3	90% or .9
K0072	Knowledge of resource management principles and techniques.	3.4	3	90% or .9
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1	3	90% or .9
K0101	Knowledge of the organization's enterprise information technology (IT) goals and objectives.	2.1.1	3	90% or .9
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	3.1 to 3.14	2	90% or .9
K0146	Knowledge of the organization's core business/mission processes.	2.1.1	3	95% or .95
K0148	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	NA		
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0164	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	NA		

NCWF JOB ROLE

IT Project Manager

Job Role Description: An IT Project Manager directly manages information technology projects to provide a unique service or product.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Project Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0165	Knowledge of risk threat assessment.	4.4	4	95% or .95
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	3	90% or .9
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.	5.1.1	3	90% or .9
K0196	Knowledge of Import/Export Regulations related to cryptography and other security technologies.	4.11	3	90% or .9
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	1.1,12	3	90% or .9
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	NA		
K0235	Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.	NA		90% or .9
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.	5.2.11	3	90% or .9
K0270	Knowledge of the acquisition/procurement life cycle process.	5.2.7	3	90% or .9
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	5.5	4	90% or .9
A0009	Ability to apply supply chain risk management standards.	NA		
A0039	Ability to oversee the development and update of the lifecycle cost estimate.	5.2.11	3	90% or .9
A0045	Ability to evaluate/ensure the trustworthiness of the supplier and/or product.	5.2.11	3	90% or .9
A0056	Ability to ensure security practices are followed throughout the acquisition process.	4.13.13	3	90% or .9
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

Product Support Manager

Job Role Description: A Product Support Manager Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Product Support Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Synthesis, Evaluation	1.12	4	95% or .95
T0174	Perform needs analysis to determine opportunities for new and improved business process solutions.	Analysis, Evaluation	5.1.1,5.1.2	4	95% or .95
T0196	Provide advice on project costs, design concepts, or design changes.	Analysis	3.3	3	90% or .9
T0204	Provide input to implementation plans and standard operating procedures.	Analysis	4.5.10	3	90% or .9
T0207	Provide ongoing optimization and problem solving support.	Analysis	2.1.8	4	95% or .95
T0208	Provide recommendations for possible improvements and upgrades.	Analysis, Evaluation	3.14	4	95% or .95
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Analysis	1.5,1.7	3	90% or .9
T0223	Review or conduct audits of information technology (IT) programs and projects.	Analysis, Evaluation	2.2	4	90% or .9
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Analysis, Evaluation	5.2.4	3	90% or .9
T0273	Develop and document supply chain risks for critical system elements, as appropriate.	Application, Analysis	5.2.11	3	90% or .9
T0277	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Analysis	5.2.11	3	90% or .9
T0302	Develop contract language to ensure supply chain, system, network, and operational security are met.	Application, Analysis	2.1.3	3	90% or .9
T0340	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Analysis	3.1	3	90% or .9
T0354	Coordinate and manage the overall service provided to a customer end-to-end.	Analysis	3.7	3	90% or .9

NCWF JOB ROLE

Product Support Manager

Job Role Description: A Product Support Manager Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Product Support Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0370	Ensure that appropriate Service Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.	Analysis	5.2.11	3	90% or .9
T0377	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Analysis	3.11	3	80% or .8
T0389	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Analysis	5.1.5	3	80% or .8
T0394	Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.	Analysis	4.5.4	3	80% or .8
T0412	Conduct import/export reviews for acquiring systems and software.	Application, Analysis	3.4	3	90% or .9
T0414	Develop supply chain, system, network, performance, and cyber security requirements.	Application, Analysis	5.2.11	3	90% or .9
T0493	Lead and oversee budget, staffing, and contracting.	Analysis	1.6, 3.5, 3.7, 3.3, 4.4.4, 4.13.11, 5.2.1	3	90% or .9
T0525	Provide enterprise cybersecurity and supply chain risk management guidance.	Analysis	5.1.1	3	90% or .9
T0551	Draft and publish supply chain security and risk management documents.	Analysis	4.4	3	90% or .9
T0553	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Analysis	4.1, 4.11	3	90% or .9
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

Product Support Manager

Job Role Description: A Product Support Manager Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Product Support Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	1.7	3	80% or .8
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	3	80% or .8
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	2.1.3	3	80% or .8
K0072	Knowledge of resource management principles and techniques.	3.4	3	80% or .8
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1	3	80% or .8
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	3.1 to 3.14	2	80% or .8
K0148	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	NA		
K0150	Knowledge of enterprise incident response program, roles, and responsibilities.	4.13	3	95% or .95
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0164	Knowledge of functionality, quality, and security requirements and how these will apply to specific items of supply (i.e., elements and processes).	NA		
K0165	Knowledge of risk threat assessment.	4.4	4	95% or .95

NCWF JOB ROLE

Product Support Manager

Job Role Description: A Product Support Manager Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Product Support Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	3	80% or .8
K0194	Knowledge of Cloud-based knowledge management technologies and concepts related to security, governance, procurement, and administration.	5.1.1	3	80% or .8
K0196	Knowledge of Import/Export Regulations related to cryptography and other security technologies.	4.11	3	80% or .8
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	1.1,1.2	3	80% or .8
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	NA		
K0235	Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.	NA		
K0249	Knowledge of sustainment technologies, processes and strategies.	5.1.1	3	80% or .8
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.	5.2.11	3	80% or .8
K0270	Knowledge of the acquisition/procurement life cycle process.	5.2.7	3	80% or .8
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	5.5	4	80% or .8
A0009	Ability to apply supply chain risk management standards.	NA		
A0031	Ability to conduct and implement market research to understand government and industry capabilities and appropriate pricing.	5.2.8	3	90% or .9
A0039	Ability to oversee the development and update of the lifecycle cost estimate.	5.2.11	3	90% or .9

NCWF JOB ROLE

Product Support Manager

Job Role Description: A Product Support Manager Manages the package of support functions required to field and maintain the readiness and operational capability of systems and components.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by a Product Support Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
A0045	Ability to evaluate/ensure the trustworthiness of the supplier and/or product.	5.2.11	3	90% or .9
A0056	Ability to ensure security practices are followed throughout the acquisition process.	4.13.13	3	90% or .9
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

IT Investment/Portfolio Manager

Job Role Description: An IT Investment/Portfolio Manager Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Investment/Portfolio Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Analysis, Evaluation	1.5,1.7	3	90% or .9
T0223	Review or conduct audits of information technology (IT) programs and projects.	Analysis, Evaluation	2.2	4	90% or .9
T0277	Ensure all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Analysis	5.2.11	4	90% or .9
T0302	Develop contract language to ensure supply chain, system, network, and operational security are met.	Analysis	2.1.3	3	90% or .9
T0377	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Analysis	3.11	3	60% or .6
T0415	Ensure supply chain, system, network, performance, and cyber security requirements are included in contract language and delivered.	Analysis	5.2.11	3	90% or .9
T0493	Lead and oversee budget, staffing, and contracting.	Analysis, Evaluation	1.6, 3.5, 3.7, 3.3, 4.4.4, 4.13.11, 5.2.1	3	90% or .9
T0551	Draft and publish supply chain security and risk management documents.	Application, Analysis	4.4	3	90% or .9
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

IT Investment/Portfolio Manager

Job Role Description: An IT Investment/Portfolio Manager Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Investment/Portfolio Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	3	60% or .60
K0072	Knowledge of resource management principles and techniques.	3.4	3	60% or .60
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	3.1 to 3.14	2	60% or .60
K0126	Knowledge of secure acquisitions (e.g., relevant Contracting Officer's Technical Representative [COTR] duties, secure procurement, supply chain risk management).	5.2.11	4	100% or 1
K0146	Knowledge of the organization's core business/mission processes.	2.1.1	3	95% or .95
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0165	Knowledge of risk threat assessment.	4.4	4	95% or .95
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	3	60% or .60
K0235	Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.	NA		
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.	5.2.11	3	60% or .60
K0270	Knowledge of the acquisition/procurement life cycle process.	5.2.7	3	60% or .60

NCWF JOB ROLE

IT Investment/Portfolio Manager

Job Role Description: An IT Investment/Portfolio Manager Manages a portfolio of IT capabilities that align with the overall needs of mission and business enterprise priorities.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Investment/Portfolio Manager. CCISO maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the Framework tasks and .8 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
A0039	Ability to oversee the development and update of the lifecycle cost estimate.	5.2.11	3	60% or .60
	Summary		**3**	**80% or .8**

NCWF JOB ROLE

IT Program Auditor

Job Role Description: An IT Program Auditor conducts evaluations of an IT program or its individual components, to determine compliance with published standards.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Program Auditor. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
T0072	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Synthesis, Evaluation	1.12	4	95% or .95
T0207	Provide ongoing optimization and problem solving support.	Analysis, Evaluation	2.1.8	4	95% or .95
T0208	Provide recommendations for possible improvements and upgrades.	Analysis, Evaluation	3.14	4	95% or .95
T0223	Review or conduct audits of information technology (IT) programs and projects.	Analysis, Evaluation	2.2	4	95% or .95
T0256	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Analysis, Evaluation	5.2.4	4	95% or .95
T0389	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Analysis, Evaluation	5.1.5	4	95% or .95
T0412	Conduct import/export reviews for acquiring systems and software.	Analysis, Evaluation	3.4	4	95% or .95
T0415	Ensure supply chain, system, network, performance, and cyber security requirements are included in contract language and delivered.	Analysis	5.2.11	4	95% or .95
	Summary			**4**	**95% or .95**

NCWF JOB ROLE

IT Program Auditor

Job Role Description: An IT Program Auditor conducts evaluations of an IT program or its individual components, to determine compliance with published standards.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Program Auditor. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	2.1, 4.6	3	60% or .6
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.12, 2.1.1, 4.4.1 - 4.4.9	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.5 - 1.10	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	4.1 - 4.4	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	4.2, 4.7 - 4.10	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.4, 2.1	4	95% or .95
K0043	Knowledge of industry-standard and organizationally accepted analysis principles and methods.	1.7	3	90% or .9
K0047	Knowledge of information technology (IT) architectural concepts and frameworks.	5.1.1	3	90% or .9
K0048	Knowledge of Risk Management Framework (RMF) requirements.	4.4	3	90% or .9
K0072	Knowledge of resource management principles and techniques.	3.4	3	90% or .9
K0090	Knowledge of system life cycle management principles, including software security and usability.	4.9.1	3	90% or .9
K0120	Knowledge of how information needs and collection requirements are translated, tracked, and prioritized across the extended enterprise.	3.1 to 3.14	2	90% or .9
K0148	Knowledge of import/export control regulations and responsible agencies for the purposes of reducing supply chain risk.	NA		
K0154	Knowledge of supply chain risk management standards, processes, and practices.	NA		
K0165	Knowledge of risk threat assessment.	4.4	4	95% or .95
K0169	Knowledge of information technology (IT) supply chain security and risk management policies, requirements, and procedures.	4.4	3	90% or .9
K0198	Knowledge of organizational process improvement concepts and process maturity models (e.g., Capability Maturity Model Integration (CMMI) for Development, CMMI for Services, and CMMI for Acquisitions).	1.1,1.2	3	90% or .9

NCWF JOB ROLE

IT Program Auditor

Job Role Description: An IT Program Auditor conducts evaluations of an IT program or its individual components, to determine compliance with published standards.

Maps To: Certified Chief Information Security Officer (CCISO)

Mapping Summary: Performance-based learning and evaluation in CCISO imparts specific KSAs that should be demonstrated by an IT Program Auditor. CCISO maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CCISO Exam Objectives	NICE Proficiency	Relational Coefficient
K0200	Knowledge of service management concepts for networks and related standards (e.g., Information Technology Infrastructure Library, current version [ITIL]).	NA		90% or .9
K0235	Knowledge of how to leverage government research and development centers, think tanks, academic research, and industry systems.	NA		90% or .9
K0257	Knowledge of information technology (IT) acquisition/procurement requirements.	5.2.11	3	90% or .9
K0270	Knowledge of the acquisition/procurement life cycle process.	5.2.7	3	90% or .9
S0038	Skill in identifying measures or indicators of system performance and the actions needed to improve or correct performance, relative to the goals of the system.	5.5	4	90% or .9
S0085	Skill in conducting audits or reviews of technical systems.	2.2	4	90% or .9
A0056	Ability to ensure security practices are followed throughout the acquisition process.	4.13.13	3	90% or .9
	Summary		**3**	**90% or .9**

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

PROTECT AND DEFEND (PR)

Specialty areas responsible for identification, analysis, and mitigation of threats to internal information technology (IT) systems or networks.

Cybersecurity Defense Analysis (DA)

Uses defensive measures and information collected from a variety of sources to identify, analyze, and report events that occur or might occur within the network in order to protect information, information systems, and networks from threats.

Cybersecurity Defense Infrastructure Support (INF)

Tests, implements, deploys, maintains, reviews and administers the infrastructure hardware and software that are required to effectively manage the computer network defense (CND) service provider network and resources. Monitors network to actively remediate unauthorized activities.

Incident Response (IR)

Responds to crisis or urgent situations within the pertinent domain to mitigate immediate and potential threats.
Uses mitigation, preparedness, and response and recovery approaches, as needed, to maximize survival of life, preservation of property, and information security. Investigates and analyzes all relevant response activities.

Vulnerability Assessment and Management (VA)

Conducts assessments of threats and vulnerabilities, determines deviations from acceptable configurations enterprise or local policy, assesses the level of risk, and develops and/or recommends appropriate mitigation countermeasures in operational and non-operational situations.

NCWF JOB ROLE

Cyber Defense Analyst

Job Role Description: A Cyber Defense Analyst uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Cyber Defense Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
T0020	Develop content for cyber defense tools.	Develop, Synthesize	6.7, 7.9, 8.6, 9.6, 11.7, 12.6, 13.7, 14.8, 15.7, 16.2, 17.5, 18.8	4	100% or 1
T0023	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Analyze	2.7, 3.7, 7.7, 14.4	4	90% or .9
T0043	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	Validate	16.1, 16.2	3	70% or .7
T0088	Ensure cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Test, Evaluate	1.6, 1.7, 1.8, 1.11, 6.7, 15.6, 16.1, 16.2, 17.5	4	100% or .1
T0155	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	Generate, Apply, Analyze	1.9	2	50% or .5
T0164	Perform cyber defense trend analysis and reporting.	Perform	1.1	4	100% or 1
T0166	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.	Perform	2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10, 2.11	4	100% or 1
T0178	Perform security reviews and identify security gaps in security architecture resulting in recommendations for the inclusion into the risk mitigation strategy.	Perform	1.6	2	70% or .7
T0187	Plan and recommend modifications or adjustments based on exercise results or system environment.		N/A		
T0198	Provide daily summary reports of network events and activity relevant to cyber defense practices.	Provide	7.1	2	50% or .5
T0214	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Analyze	16.2	3	90% or .9

NCWF JOB ROLE

Cyber Defense Analyst

Job Role Description: A Cyber Defense Analyst uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Cyber Defense Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
T0258	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.	Choose	16.2	3	90% or .9
T0259	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.	Analyze	6.6	3	90% or .9
T0260	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.	Analyze	1.10	3	90% or .9
T0290	Determine tactics, techniques, and procedures (TTPs) for intrusion sets.	Determine	16.1	4	100% or 1
T0291	Examine network topologies to understand data flows through the network.	Examine	3.8	3	90% or .9
T0292	Recommend computing environment vulnerability corrections.	Summarize	1.10	3	90% or .9
T0293	Identify and analyze anomalies in network traffic using metadata (e.g., CENTAUR).	Identify	7.7	3	90% or .9
T0294	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).	Conduct	Module 02	3	90% or .9
T0295	Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.	Validate	7.7, 16.2	4	100% or 1
T0296	Isolate and remove malware.	Analyze	6.5, 6.6	4	100% or 1
T0297	Identify applications and operating systems of a network device based on network traffic.	Identify	7.7	4	100% or 1
T0298	Reconstruct a malicious attack or activity based off network traffic.	Reconstruct	7.7	4	100% or 1
T0299	Identify network mapping and operating system (OS) fingerprinting activities.	Identify	3.6	4	100% or 1
T0310	Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the NE or enclave.	Design	18.5	3	90% or .9

NCWF JOB ROLE

Cyber Defense Analyst

Job Role Description: A Cyber Defense Analyst uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Cyber Defense Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
T0332	Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.	Point out	1.9	3	90% or .9
T0469	Analyze and report organizational security posture trends.	Analyze	1.1	3	90% or .9
T0470	Analyze and report system security posture trends.	Analyze	1.1	3	90% or .9
T0475	Assess adequate access controls based on principles of least privilege and need-to-know.	Assess	1.7, 1.8	3	70% or .7
T0503	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.	Determine	2.2, 2.4	3	90% or .9
T0504	Assess and monitor cybersecurity related to system implementation and testing practices.	Assess	1.10, 2.14, 3.11, 4.8, 5.8, 6.8, 7.10, 8.7, 9.7, 10.6, 11.8, 12.7, 14.9, 15.8, 16.8, 17.6	4	100% or 1
T0526	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Provide	2.13, 4.7, 6.7, 7.8, 8.6, 9.5, 9.6, 10.5, 11.5, 12.5, 13.6, 14.7, 16.7	4	100% or 1
T0545	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Experiment	1.9	3	90% or .9
T0548	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.		N/A		
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

Cyber Defense Analyst

Job Role Description: A Cyber Defense Analyst uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Cyber Defense Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 18	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0007	Knowledge of authentication, authorization, and access control methods.	NA		
K0013	Knowledge of cyber defense and vulnerability assessment tools, including open source tools, and their capabilities.	1.10, 3.7	4	100% or 1
K0015	Knowledge of computer algorithms.	N/A		
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	18.2	4	100% or 1
K0019	Knowledge of cryptography and cryptographic key management concepts.	18.1	4	100% or 1
K0024	Knowledge of database systems.	N/A		
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	16.1, 16.2, 16.5	3	90% or .9
K0040	Knowledge of known vulnerabilities from alerts, advisories, errata, and bulletins.	1.10, 3.7	4	100% or 1
K0042	Knowledge of incident response and handling methodologies.	1.9	3	90% or .9
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	1.2	3	90% or .9
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	16.1	4	100% or 1

NCWF JOB ROLE

Cyber Defense Analyst

Job Role Description: A Cyber Defense Analyst uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Cyber Defense Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0049	Knowledge of information technology (IT) security principles and methods (e.g., firewalls, demilitarized zones, encryption).	16.1, 18.1	4	100% or 1
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	18.4	4	100% or 1
K0058	Knowledge of network traffic analysis methods.	14.4, 16.5	4	100% or 1
K0059	Knowledge of new and emerging information technology (IT) and cybersecurity technologies.	1.1	4	100% or 1
K0060	Knowledge of operating systems.	N/A		
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	7.1	4	100% or 1
K0065	Knowledge of policy-based and risk adaptive access controls.	1.7	3	90% or .9
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	11.2, 12.2	3	90% or .9
K0074	Knowledge of key concepts in security management (e.g., Release Management, Patch Management).	11.6	3	90% or .9
K0075	Knowledge of security system design tools, methods, and techniques.	11.6, 11.7, 12.6, 14.8, 16.2	4	100% or 1
K0093	Knowledge of key telecommunications concepts (e.g., Routing Algorithms, Fiber Optics Systems Link Budgeting, Add/Drop Multiplexers).	N/A		
K0098	Knowledge of the cyber defense Service Provider reporting structure and processes within one's own organization.	N/A		
K0099	Knowledge of the common networking protocols (e.g., TCP/IP), services (e.g., web, mail, Domain Name Server), and how they interact to provide network communications.	2.5, 2.6, 2.8, 3.1	3	90% or .9
K0104	Knowledge of Virtual Private Network (VPN) security.	NA		
K0106	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	1.3	4	100% or 1

NCWF JOB ROLE

Cyber Defense Analyst

Job Role Description: A Cyber Defense Analyst uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Cyber Defense Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0110	Knowledge of common adversary tactics, techniques, and procedures in assigned area of responsibility (i.e., historical country-specific tactics, techniques, and procedures; emerging capabilities).	N/A		
K0111	Knowledge of common network tools (e.g., ping, traceroute, nslookup) and interpret the information results.	2.8, 2.10, 3.2, 3.3, 3.4	4	100% or 1
K0112	Knowledge of defense-in-depth principles and network security architecture.	1.6	4	100% or 1
K0113	Knowledge of different types of network communication (e.g., LAN, WAN, MAN, WLAN, WWAN).	N/A		
K0116	Knowledge of file extensions (e.g., .dll, .bat, .zip, .pcap, .gzip).	N/A		
K0139	Knowledge of interpreted and compiled computer languages.	N/A		
K0142	Knowledge of collection management processes, capabilities, and limitations.	2	4	100% or 1
K0143	Knowledge of front-end collection systems, including network traffic collection, filtering, and selection.	16.2	3	90% or .9
K0157	Knowledge of cyber defense policies, procedures, and regulations.	1.7	4	100% or 1
K0160	Knowledge of the common attack vectors on the network layer.	7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 9.2, 10.3	4	100% or 1
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	1.3	4	100% or 1
K0162	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non- nation state sponsored], and third generation [nation state sponsored]).	1.4	4	100% or 1
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	1 - 18	4	100% or 1
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	1.11	3	90% or .9
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1.6	3	90% or .9
K0180	Knowledge of network systems management principles, models, methods (e.g., end-to-end systems performance monitoring), and tools.	1.6	4	100% or 1

NCWF JOB ROLE

Cyber Defense Analyst

Job Role Description: A Cyber Defense Analyst uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Cyber Defense Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0190	Knowledge of encryption methodologies.	18.1, 18.2	4	100% or 1
K0191	Knowledge of signature implementation impact.	18.5	3	90% or .9
K0192	Knowledge of Windows/Unix ports and services.	4.1	3	90% or .9
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	N/A		
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	7.1, 10.1	2	70% or .7
K0222	Knowledge of relevant laws, legal authorities, restrictions, and regulations pertaining to cyber defense activities.	1.11	4	100% or 1
K0260	Knowledge of Personally Identifiable Information (PII) data security standards.	1.11	4	100% or 1
K0261	Knowledge of Payment Card Industry (PCI) data security standards.	1.11	4	100% or 1
K0262	Knowledge of Personal Health Information (PHI) data security standards.	1.11	4	100% or 1
K0273	Knowledge of general kill chain (e.g., footprinting and scanning, enumeration, gaining access, escalation of privileges, maintaining access, network exploitation, covering tracks).	1.4	4	100% or 1
K0290	Knowledge of systems security testing and evaluation methods.	1 - 18	4	100% or 1
K0297	Knowledge of countermeasure design for identified security risks.	2 - 18	4	100% or 1
K0300	Knowledge of network mapping and recreating network topologies.	3.8	4	100% or 1
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	7.7	4	100% or 1
K0303	Knowledge of the use of sub-netting tools.	N/A		
K0318	Knowledge of operating system command line/prompt.	1 - 18	4	100% or 1
K0322	Knowledge of embedded systems.	N/A		
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	16.2	4	100% or 1
K0331	Knowledge of network protocols (e.g., Transmission Critical Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP)), and directory services (e.g., Domain Name System (DNS)).	3.1, 7.7, 10.3, 15.5	4	100% or 1

NCWF JOB ROLE

Cyber Defense Analyst

Job Role Description: A Cyber Defense Analyst uses data collected from a variety of cyber defense tools (e.g., IDS alerts, firewalls, network traffic logs) to analyze events that occur within their environments for the purposes of mitigating threats.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Cyber Defense Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0339	Knowledge of how to use network analysis tools to identify vulnerabilities.	1.10, 3.7, 12.6, 14.8	4	100% or 1
K0342	Knowledge of penetration testing principles, tools, and techniques.	1.10, 2.14, 3.11, 4.8, 5.8, 6.8, 7.10, 8.7, 9.7, 10.6, 11.8, 12.7, 14.9, 15.8, 16.8, 17.6	4	100% or 1
S0020	Skill in developing and deploying signatures.	1.1	3	90% or .9
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	16.2	4	100% or 1
S0027	Skill in determining how a security system should work (including its resilience and dependability capabilities) and how changes in conditions, operations, or the environment will affect these outcomes.	1.6	3	90% or .9
S0036	Skill in evaluating the adequacy of security designs.	1.6	3	90% or .9
S0054	Skill in using incident handling methodologies.	1.9	3	90% or .9
S0057	Skill in using protocol analyzers.	7.1, 7.7	4	100% or 1
S0063	Skill in collecting data from a variety of cyber defense resources.	2.2 to 2.11, 8.2 to 8.5	4	100% or 1
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	1.10	4	100% or 1
S0096	Skill in reading and interpreting signatures (e.g., snort).	16.2	4	100% or 1
S0147	Skill in assessing security controls based on cybersecurity principles and tenets.	1.2, 1.6	4	100% or 1
S0167	Skill in recognizing vulnerabilities in security systems.	1.10	4	100% or 1
S0169	Skill in conducting trend analysis.	1.1	4	100% or 1
A0010	Ability to analyze malware.	6.5	4	100% or 1
A0015	Ability to conduct vulnerability scans and recognize vulnerabilities in security systems.	1.1	4	100% or 1
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	1.6 to 1.11	4	100% or 1
	Summary		**4**	**100% or 1**

NCWF JOB ROLE

Cyber Defense Infrastructure Support Specialist

Job Role Description: A Cyber Defense Infrastructure Support Specialist tests, implements, deploys, maintains, and administers the infrastructure hardware and software.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Cyber Defense Infrastructure Support Specialist. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .6 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CND Exam Objectives	NICE Proficiency	Relational Coefficient
T0042	Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, anti-virus, and content blacklists) for specialized cyber defense applications.	Coordinate	8.1 - 8.5	4	70% or .7
T0180	Perform system administration on specialized cyber defense applications and systems (e.g., anti-virus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup and restoration.	Perform	6.1 - 6.8, 9.1 - 9.10	4	70% or .7
T0261	Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.	Assist	1 - 14	2	30% or .3
T0335	Build, install, configure, and test dedicated cyber defense hardware.	Build	1 - 14	4	70% or .7
T0348	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.	Assist	1 - 14	4	70% or .7
T0420	Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).	Administer	1.4, 3.3, 8.5	4	70% or .7
T0438	Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).	Manage	3.3,7.8, 8.3	4	70% or .7
T0483	Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).	Identify	1 - 14	3	50% or .5
T0486	Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.	Implement	12.4	2	60% or .6
	Summary			**3**	**60% or .6**

NCWF JOB ROLE

Cyber Defense Infrastructure Support Specialist

Job Role Description: A Cyber Defense Infrastructure Support Specialist tests, implements, deploys, maintains, and administers the infrastructure hardware and software.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Cyber Defense Infrastructure Support Specialist. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .6 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.1 - 1.4	4	100% or 1
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	12.2 - 12.4	4	100% or 1
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	4.6	3	95% or .95
K0004	* Knowledge of cybersecurity principles.	3.1	4	100% or 1
K0005	* Knowledge of cyber threats and vulnerabilities.	2.1 - 2.4	4	100% or 1
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.1	3	95% or .95
K0021	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.	13.7, 13.10	4	100% or 1
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	3.3,6.3	4	100% or 1
K0042	Knowledge of incident response and handling methodologies.	14.1 - 14.3	4	100% or 1
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	3.1	4	100% or 1
K0062	Knowledge of packet-level analysis.	11.1 - 11.9	4	100% or 1
K0104	Knowledge of Virtual Private Network (VPN) security.	9.1 - 9.11	4	100% or 1
K0106	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	2.1 - 2.7	4	100% or 1
K0135	Knowledge of web filtering technologies.	3.7	4	100% or 1
K0157	Knowledge of cyber defense policies, procedures, and regulations.	4.1 - 4.6	4	100% or 1
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1 - 14	4	100% or 1
K0205	Knowledge of basic system, network, and OS hardening techniques.	6.2	4	100% or 1
K0258	Knowledge of test procedures, principles, and methodologies (e.g., Capabilities and Maturity Model Integration (CMMI)).	NA		

NCWF JOB ROLE

Cyber Defense Infrastructure Support Specialist

Job Role Description: A Cyber Defense Infrastructure Support Specialist tests, implements, deploys, maintains, and administers the infrastructure hardware and software.

Maps To: Certified Network Defender (CND)

Mapping Summary: Performance-based learning and evaluation in CND imparts specific KSAs that should be demonstrated by a Cyber Defense Infrastructure Support Specialist. CND maps to this job role at a Specialist level (level 3) with a correlation coefficient of .6 on the framework Tasks and a correlation coefficient of 1 on the KSA proficiency descriptions.

KSA

ID	Statement	CND Exam Objectives	NICE Proficiency	Relational Coefficient
K0274	Knowledge of transmission records (e.g., Bluetooth, Radio Frequency Identification (RFID), Infrared Networking (IR), Wireless Fidelity (Wi-Fi). paging, cellular, satellite dishes, Voice over Internet Protocol (VoIP)), and jamming techniques that enable transmission of undesirable information, or prevent installed systems from operating correctly.	10.1 - 10.15	3	40% or .4
K0324	Knowledge of Intrusion Detection System (IDS)/Intrusion Prevention System (IPS) tools and applications.	8.1 - 8.10	4	100% or 1
K0331	Knowledge of network protocols (e.g., Transmission Critical Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP)), and directory services (e.g., Domain Name System (DNS)).	1.3	4	100% or 1
K0334	Knowledge of network traffic analysis (tools, methodologies, processes).	11.1 - 11.8	4	100% or 1
K0340	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol (TCP), Internet Protocol (IP), Open System Interconnection Model (OSI)).	1.2,1.3	4	100% or 1
S0007	Skill in applying host/network access controls (e.g., access control list).	3.3,6.3	4	100% or 1
S0053	Skill in tuning sensors.	8.5	4	100% or 1
S0054	Skill in using incident handling methodologies.	14.1 - 14.3	4	100% or 1
S0059	Skill in using Virtual Private Network (VPN) devices and encryption.	9.1 - 9.11	4	100% or 1
S0077	Skill in securing network communications.	3.8	4	100% or 1
S0079	Skill in protecting a network against malware.	6.3	4	100% or 1
S0121	Skill in system, network, and OS hardening techniques.	6.2 - 6.10	4	100% or 1
S0124	Skill in troubleshooting and diagnosing cyber defense infrastructure anomalies and work through resolution.	1 - 14	4	100% or 1
	Summary		**4**	**100% or 1**

NCWF JOB ROLE

Cyber Defense Incident Responder

Job Role Description: A Cyber Defense Incident Responder investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

Maps To: EC-Council Certified Incident Handler (ECIH)

Mapping Summary: Performance-based learning and evaluation in ECIH imparts specific KSAs that should be demonstrated by a Cyber Defense Incident Responder. ECIH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .8 on the framework Tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECIH Exam Objectives	NICE Proficiency	Relational Coefficient
T0041	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.	Evaluation	7.6, 9.3, 9.7, 11.9	3	75% or .75
T0047	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.	Evaluation	1.5, 2.2	3	90% or .9
T0161	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.	Evaluation	7.6, 9.5	4	95% or .95
T0163	Perform cyber defense incident triage, to include determining scope, urgency, and potential impact; identifying the specific vulnerability; and making recommendations that enable expeditious remediation.	Comprehension, Synthesis	2.4, 2.5, 2.7, 2.8, 10.7,	1	30% or .3
T0170	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.	Comprehension, Synthesis	8.4, 8.5, 8.6, 8.7,	4	95% or .95
T0175	Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).	Comprehension, Synthesis	3.2, 3.3, 3.4, 3.5, 4.2, 5.2, 6.2, 7.5, 8.2, 8.3,	3	75% or .75
T0214	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Synthesis	5.2, 5.4, 5.5, 5.6, 5.7, 7.3,	3	75% or .75
T0233	Track and document cyber defense incidents from initial detection through final resolution.	Construct	2.4, 3.4, 11.6, 1.9, 4.11, 9.1, 9.2, 9.3, 9.4, 9.6, 9.7,	3	90% or .9
T0246	Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.	Construct, Create	9.1, 9.2, 9.3, 9.4, 9.6, 9.7, 11.6,	2	75% or .75
T0262	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).	Synthesis	11.7,	2	30% or .3
T0278	Collect intrusion artifacts (e.g., source code, malware, trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Evaluation	2.4, 2.5, 2.8, 3.5, 4.10, 4.11,	3	75% or .75

NCWF JOB ROLE

Cyber Defense Incident Responder

Job Role Description: A Cyber Defense Incident Responder investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

Maps To: EC-Council Certified Incident Handler (ECIH)

Mapping Summary: Performance-based learning and evaluation in ECIH imparts specific KSAs that should be demonstrated by a Cyber Defense Incident Responder. ECIH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .8 on the framework Tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECIH Exam Objectives	NICE Proficiency	Relational Coefficient
T0279	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.	Evaluation	4.2, 4.3, 4.5, 4.4, 9.5, 9.6, 10.4, 11.4, 11.5, 11.6, 11.7	3	90% or .9
T0312	Coordinate with intelligence analysts to correlate threat assessment data.	Analyze		2	90% or .9
T0333	Perform cyber defense trend analysis and reporting.	Construct, Create	1.5, 1.6, 1.7, 9.2, 9.3, 9.4,	3	90% or .9
T0395	Write and publish after action reviews.	Construct, Create	9.2, 9.3, 9.4,	3	90% or .9
T0503	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.	Evaluation	1.3, 1.4, 1.5, 1.6, 2.2, 2.3, 10.6,	3	90% or .9
T0510	Coordinate incident response functions.	Evaluation	4.1, 4.2, 4.3, 4.4, 4.5, 5.2, 6.2, 7.5, 8.2, 8.3,	3	90% or .9
	Summary			**3**	**80% or .8**

NCWF JOB ROLE

Cyber Defense Incident Responder

Job Role Description: A Cyber Defense Incident Responder investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

Maps To: EC-Council Certified Incident Handler (ECIH)

Mapping Summary: Performance-based learning and evaluation in ECIH imparts specific KSAs that should be demonstrated by a Cyber Defense Incident Responder. ECIH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .8 on the framework Tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	ECIH Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1.3, 1.4, 5.1, 5.9,	2	50% or .5
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	2.1, 2.2, 2.3, 2.4, 2.5, 2.6, 2.7, 2.8, 2.9, 2.10	3	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	11.1, 11.2, 11.3, 11.4, 11.5, 11.6, 11.7, 11.8, 11.9, 11.10, 11.11, 11.12, 11.13	3	50% or .5
K0004	* Knowledge of cybersecurity principles.	1.4, 1.6, 3.9, 3.10,	3	95% or .95
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3, 1.4, 5.1, 5.9,	4	95% or .95
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	2.3, 2.4, 2.5, 2.6,	3	90% or .9
K0021	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.	7.6	3	90% or .9
K0026	Knowledge of disaster recovery continuity of operations plans.	10.1, 10.2, 10.3, 10.4, 10.5, 10.6, 10.7, 10.8,	2	50% or .5
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	7.2, 7.3, 11.7	2	50% or .5
K0034	Knowledge of how network services and protocols interact to provide network communications.	1.3, 1.4, 5.1,	2	50% or .5
K0041	Knowledge of incident categories, incident responses, and timelines for responses.	1.3, 1.4, 5.1, 5.6, 6.5, 7.4, 7.5,	2	90% or .9
K0042	Knowledge of incident response and handling methodologies.	5.6, 6.5, 7.4, 7.5,	2	90% or .9
K0046	Knowledge of intrusion detection methodologies and techniques for detecting host and network-based intrusions via intrusion detection technologies.	1.5, 1.6, 1.7, 3.3, 3.4, 5.4, 5.5, 5.6, 6.4, 6.5, 7.4, 7.5,	2	50% or .5
K0058	Knowledge of network traffic analysis methods.	5.4, 5.5, 5.6, 5.7, 5.8,	4	90% or .9
K0062	Knowledge of packet-level analysis.	5.6, 5.7, 5.8,	4	90% or .9

NCWF JOB ROLE

Cyber Defense Incident Responder

Job Role Description: A Cyber Defense Incident Responder investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

Maps To: EC-Council Certified Incident Handler (ECIH)

Mapping Summary: Performance-based learning and evaluation in ECIH imparts specific KSAs that should be demonstrated by a Cyber Defense Incident Responder. ECIH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .8 on the framework Tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	ECIH Exam Objectives	NICE Proficiency	Relational Coefficient
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	1.3, 1.4, 5.1, 5.9,	3	90% or .9
K0106	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	1.3, 1.4, 5.4, 5.5,	3	90% or .9
K0157	Knowledge of cyber defense policies, procedures, and regulations.	11.2, 11.3, 11.4, 11.5,	2	90% or .9
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	1.3, 1.4, 5.3, 6.1, 7.1	3	75% or .75
K0162	Knowledge of different operational threat environments (e.g., first generation [script kiddies], second generation [non- nation state sponsored], and third generation [nation state sponsored]).	1.5, 5.1, 6.1, 7.1,	3	75% or .75
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	3.3, 3.6, 3.7, 3.8,	3	75% or .75
K0177	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	3.5	3	75% or .75
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1.5, 1.6, 5.4, 5.5,	3	75% or .75
K0221	Knowledge of OSI model and underlying network protocols (e.g., TCP/IP).	NA		
K0225	Knowledge of the common networking protocol and services deployed at CC/S/A.	NA		
K0230	Knowledge of cloud service models and possible limitations for an incident response.	6.1, 6.2, 6.3, 6.4, 6.5,	2	90% or .9
K0259	Knowledge of malware analysis concepts and methodologies.	6.1, 6.2, 6.3, 6.4, 6.5,	3	60% or .60
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	4.2, 4.3, 4.4, 4.5, 4.6, 4 .7,	3	90% or .9
K0332	Knowledge of network protocols such as TCP/IP, Dynamic Host Configuration, Domain Name System (DNS), and directory services.	NA		
S0003	Skill of identifying, capturing, containing, and reporting malware.	6.1, 6.2, 6.3, 6.4, 6.5,	3	90% or .9
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	3.4, 3.5, 6.4,	4	95% or .95

NCWF JOB ROLE

Cyber Defense Incident Responder

Job Role Description: A Cyber Defense Incident Responder investigates, analyzes, and responds to cyber incidents within the network environment or enclave.

Maps To: EC-Council Certified Incident Handler (ECIH)

Mapping Summary: Performance-based learning and evaluation in ECIH imparts specific KSAs that should be demonstrated by a Cyber Defense Incident Responder. ECIH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .8 on the framework Tasks and a correlation coefficient of .8 on the KSA proficiency descriptions.

KSA

ID	Statement	ECIH Exam Objectives	NICE Proficiency	Relational Coefficient
S0077	Skill in securing network communications.	5.1, 5.2, 5.3, 5.4, 5.5, 5.6,	3	60% or .60
S0078	Skill in recognizing and categorizing types of vulnerabilities and associated attacks.	1.3, 1.4, 1.5, 1.6, 5.3, 5.4, 6.1, 6.2, 7.2,	3	95% or .95
S0079	Skill in protecting a network against malware.	6.3, 6.4, 6.5,	3	95% or .95
S0080	Skill in performing damage assessments.	2.2, 2.3, 2.4, 5.4, 6.4	3	95% or .95
S0173	Skill in using security event correlation tools.	5.5, 5.6, 5.8,	3	90% or .9
	Summary		**3**	**80% or .8**

NCWF JOB ROLE

Vulnerability Assessment Analyst

Job Role Description: Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Vulnerability Assessment Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
T0010	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.	Analyze	1.7	3	90% or .9
T0028	Conduct and/or support authorized penetration testing on enterprise network assets.	Conduct	1 - 18	3	90% or .9
T0138	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.	Maintain	6.7, 7.9, 8.6, 9.6, 11.7, 12.6, 13.7, 14.8, 15.7, 16.2, 17.5, 18.8	4	90% or .9
T0142	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.	Maintain	1.7, 1.8, 1.11	4	90% or .9
T0188	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.	Prepare	1 - 18	3	90% or .9
T0252	Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).	Conduct	1 - 18	3	90% or .9
T0549	Perform technical (evaluation of technology) and non-technical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).	Perform	1.10	3	90% or .9
T0550	Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).	Assess	1.10	3	90% or .9
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

Vulnerability Assessment Analyst

Job Role Description: Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Vulnerability Assessment Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 18	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0009	Knowledge of application vulnerabilities.	1.10	3	90% or .9
K0019	Knowledge of cryptography and cryptographic key management concepts.	18.1	4	90% or .9
K0021	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.	NA		
K0033	Knowledge of host/network access control mechanisms (e.g., access control list).	16.1, 16.2, 16.5	3	90% or .9
K0044	Knowledge of cybersecurity principles and organizational requirements (relevant to confidentiality, integrity, availability, authentication, non-repudiation).	1.2	4	100% or 1
K0056	Knowledge of network access, identity, and access management (e.g., public key infrastructure [PKI]).	18.4	4	100% or 1
K0061	Knowledge of how traffic flows across the network (e.g., Transmission Control Protocol [TCP] and Internet Protocol [IP], Open System Interconnection Model [OSI], Information Technology Infrastructure Library, current version [ITIL]).	7.1	3	90% or .9
K0068	Knowledge of programming language structures and logic.	N/A		
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	11.2, 12.2	4	100% or 1
K0085	Knowledge of system and application security threats and vulnerabilities.	1.3, 1.10	4	100% or 1
K0089	Knowledge of systems diagnostic tools and fault identification techniques.	ECSA	4	90% or .9
K0106	Knowledge of what constitutes a network attack and the relationship to both threats and vulnerabilities.	1.3	4	100% or 1

NCWF JOB ROLE

Vulnerability Assessment Analyst

Job Role Description: Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Vulnerability Assessment Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0139	Knowledge of interpreted and compiled computer languages.	N/A		
K0161	Knowledge of different classes of attacks (e.g., passive, active, insider, close-in, distribution).	1.3	4	100% or 1
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	CND	4	100% or 1
K0177	Knowledge of general attack stages (e.g., foot printing and scanning, enumeration, gaining access, escalation or privileges, maintaining access, network exploitation, covering tracks).	1.4	4	100% or 1
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	1.6	3	90% or .9
K0203	Knowledge of security models (e.g., Bell-LaPadula model, Biba integrity model, Clark-Wilson integrity model).	N/A		
K0206	Knowledge of ethical hacking principles and techniques.	1.4, 1.5	4	100% or 1
K0210	Knowledge of data backup and restoration concepts.	NA		
K0224	Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems.	NA		
K0265	Knowledge of infrastructure supporting information technology (IT) for safety, performance, and reliability.	1.6	3	90% or .9
K0287	Knowledge of an organization's information classification program and procedures for information compromise.	1.6	3	90% or .9
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	7.7	4	100% or 1
K0308	Knowledge of cryptology.	18.1	4	100% or 1
K0331	Knowledge of network protocols (e.g., Transmission Critical Protocol (TCP), Internet Protocol (IP), Dynamic Host Configuration Protocol (DHCP)), and directory services (e.g., Domain Name System (DNS)).	3.1, 7.7, 10.3, 15.5	4	90% or .9
K0342	Knowledge of penetration testing principles, tools, and techniques.	"1.10, 2.14, 3.11, 4.8, 5.8, 6.8, 7.10,		
K0342	Knowledge of penetration testing principles, tools, and techniques.	1.10, 2.14, 3.11, 4.8, 5.8, 6.8, 7.10, 8.7, 9.7, 10.6, 11.8, 12.7, 14.9, 15.8, 16.8, 17.6	4	100% or 1

NCWF JOB ROLE

Vulnerability Assessment Analyst

Job Role Description: Performs assessments of systems and networks within the network environment or enclave and identifies where those systems/networks deviate from acceptable configurations, enclave policy, or local policy. Measures effectiveness of defense-in-depth architecture against known vulnerabilities.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Vulnerability Assessment Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0344	Knowledge of threat environments.	1.6	4	90% or .9
K0345	Knowledge of cyber attackers (e.g., script kiddies, insider threat, non-nation state sponsored, and nation sponsored).	1.4	3	90% or .9
S0001	Skill in conducting vulnerability scans and recognizing vulnerabilities in security systems.	1.10, 3.7	4	100% or 1
S0009	Skill in assessing the robustness of security systems and designs.	1.6	3	90% or .9
S0025	Skill in detecting host and network based intrusions via intrusion detection technologies (e.g., Snort).	16.2	4	100% or 1
S0044	Skill in mimicking threat behaviors.	1.6, 6.1, 6.2, 6.3, 6.4	4	100% or 1
S0051	Skill in the use of penetration testing tools and techniques.	1.10, 2.14, 3.11, 4.8, 5.8, 6.8, 7.10, 8.7, 9.7, 10.6, 11.8, 12.7, 14.9, 15.8, 16.8, 17.6	4	100% or 1
S0052	Skill in the use of social engineering techniques.	8.2, 8.3, 8.4	4	100% or 1
S0081	Skill in using network analysis tools to identify vulnerabilities.	1.10, 3.7, 12.6, 14.8	4	100% or 1
S0120	Skill in reviewing logs to identify evidence of past intrusions.	NA		
S0137	Skill in conducting application vulnerability assessments.	1.10	4	100% or 1
S0171	Skill in performing impact/risk assessments.	1.10	4	90% or .9
A0001	Ability to identify systemic security issues based on the analysis of vulnerability and configuration data.	1.10, 3.7	3	100% or 1
A0044	Ability to apply programming language structures (e.g., source code review) and logic.	N/A		
	Summary		**4**	**90% or .9**

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

ANALYZE (AN)

Specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness for intelligence.

Threat Analysis (TA)

Identifies and assesses the capabilities and activities of cyber criminals or foreign intelligence entities; produces findings to help initialize or support law enforcement and counterintelligence investigations or activities.

Targets (TD)

Applies current knowledge of one or more regions, countries, non-state entities, and/or technologies.

Exploitation Analysis (XA)

Analyzes collected information to identify vulnerabilities and potential for exploitation.

Language Analysis (LA)

Applies language, cultural, and technical expertise to support information collection, analysis, and other cybersecurity activities.

All-Source Analysis (AN)

Analyzes threat information from multiple sources, disciplines, and agencies across the Intelligence Community. Synthesizes and places intelligence information in context; draws insights about the possible implications.

NCWF JOB ROLE

Warning Analyst

Job Role Description: A Warning Analyst develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Warning Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
T0569	Answer requests for information.	Answer, Analyze	2.1 - 2.14	3	80% or .8
T0583	Provide subject matter expertise to the development of a common operational picture.	Classify, Analyze	1.6	3	80% or .8
T0584	Maintain a common intelligence picture.	Maintain	2.7	3	90% or .9
T0585	Provide subject matter expertise to the development of cyber operations specific indicators.	Provide, Analyze	1.1 - 1.11	3	100% or 1
T0586	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Assist	2.1 - 2.14	3	100% or 1
T0589	Assist in the identification of intelligence collection shortfalls.	Assist	2.7	4	100% or 1
T0593	Brief threat and/or target current situations.	Explain, Evaluate	1.10, 3.7	4	90% or .9
T0597	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Collaborate	2.1 - 2.14	3	100% or 1
T0615	Conduct in-depth research and analysis.	Conduct	2.1 - 2.14	3	100% or 1
T0617	Conduct nodal analysis.		N/A		
T0660	Develop information requirements necessary for answering priority information requests.	Develop, Synthesisze	2.1 - 2.14	4	100% or 1
T0685	Evaluate threat decision-making processes.	Evaluate	1.6	3	90% or .9
T0687	Identify threats to Blue Force vulnerabilities.	Identify	1.6	3	90% or .9
T0707	Generate requests for information.	Generate	2.1 - 2.14	3	100% or 1
T0708	Identify threat tactics, and methodologies.	Identify	1.6	3	100% or 1
T0718	Identify intelligence gaps and shortfalls.	Identify	1.1	3	100% or 1
T0748	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Document	1.6	3	100% or 1

NCWF JOB ROLE

Warning Analyst

Job Role Description: A Warning Analyst develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Warning Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
T0749	Monitor and report on validated threat activities.	Document	1.6	3	90% or .9
T0751	Monitor open source websites for hostile content directed towards organizational or partner interests.	Review	2.5	3	90% or .9
T0752	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	Review	2.1 - 2.14	4	100% or 1
T0758	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	Document	1.6	4	100% or 1
T0761	Provide SME and support to planning/developmental forums and working groups as appropriate.		N/A		
T0783	Provide current intelligence support to critical internal/external stakeholders as appropriate.	Provide	2.7	3	90% or .9
T0785	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	Provide	2.1 - 2.14	4	100% or 1
T0786	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Provide	1.1	2	50% or .5
T0792	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.	Provide	2.1 - 2.14	3	100% or 1
T0800	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.	Provide	1- 18	3	100% or 1
T0805	Report intelligence-derived significant network events and intrusions.	Report	16.1 - 16.8	3	100% or 1
T0834	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	Coordinate	2.1 - 2.14	3	100% or 1
	Summary			**3**	**95% or .95**

NCWF JOB ROLE

Warning Analyst

Job Role Description: A Warning Analyst develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Warning Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 18	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0036	Knowledge of human-computer interaction principles.	N/A		
K0058	Knowledge of network traffic analysis methods.	14.4, 16.5	4	100% or 1
K0173	Withdrawn – Integrated into K0499	N/A		
K0348	Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).	14.1	4	100% or 1
K0349	Knowledge of a wide range of concepts associated with websites (e.g., website types, administration, functions, software systems, etc.).	2.2, 2.5, 2.7	4	100% or 1
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	5.2, 7.2, 7.3, 7.4, 7.5, 7.6, 8.2, 9.2, 10.2, 10.3, 11.2, 12.2, 13.2, 14.3, 14.6, 15.2, 15.4, 15.5, 16.3, 16.4, 17.2, 17.3, 18.7	4	100% or 1
K0369	Knowledge of basic malicious activity concepts (e.g., foot printing, scanning and enumeration).	2.1 - 2.14, 3.1 - 3.11, 4.1 - 4.8	4	100% or 1
K0370	Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	NA		
K0377	Knowledge of classification and control markings standards, policies and procedures.	1.7	4	100% or 1

NCWF JOB ROLE

Warning Analyst

Job Role Description: A Warning Analyst develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Warning Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).	6.1, 6.2, 6.3, 6.4	4	100% or 1
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)			
K0405	Knowledge of current computer-based intrusion sets.	16.1	4	100% or 1
K0409	Knowledge of cyber intelligence/information collection capabilities and repositories.	2.1 - 2.14	4	100% or 1
K0415	Knowledge of cyber operations terminology/lexicon.	1.4	4	100% or 1
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).			
K0427	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).	18.2, 18.5	4	100% or 1
K0431	Knowledge of evolving/emerging communications technologies.	1- 18	4	100% or 1
K0436	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber attack, cyber defense), principles, capabilities, limitations, and effects.	1.1 - 1.11	4	100% or 1
K0437	Knowledge of general SCADA system components.	N/A		
K0440	Knowledge of host-based security products and how they affect exploitation and vulnerability.	16.2	4	100% or 1
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	2.6, 4.6	3	70% or .7
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.	N/A		
K0446	Knowledge of how modern wireless communications systems impact cyber operations.	14.3	4	100% or 1
K0449	Knowledge of how to extract, analyze, and use metadata.	2.1 - 2.14	4	100% or 1
K0458	Knowledge of intelligence disciplines.	2.1 - 2.14	4	100% or 1
K0460	Knowledge of intelligence preparation of the environment and similar processes.	2.1 - 2.14	3	70% or .7
K0464	Knowledge of intelligence support to planning, execution, and assessment.	2.1 - 2.14	3	70% or .7
K0469	Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions.	1- 18	4	100% or 1

NCWF JOB ROLE

Warning Analyst

Job Role Description: A Warning Analyst develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Warning Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
K0471	Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).	3.1 - 3.11	4	100% or 1
K0480	Knowledge of malware.	6.1, 6.2, 6.3, 6.4	4	100% or 1
K0511	Knowledge of organizational hierarchy and cyber decision making processes.	1.6	4	100% or 1
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	16.1	4	100% or 1
K0556	Knowledge of telecommunications fundamentals.			
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.			
K0561	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	16.1 - 16.8, 18.1 - 18.8	4	100% or 1
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	2.5, 2.6, 2.9, 3.1, 7.1	4	100% or 1
K0603	Knowledge of the ways in which targets or threats use the Internet.	1- 18	4	100% or 1
K0604	Knowledge of threat and/or target systems.	1- 18	4	100% or 1
K0610	Knowledge of virtualization products (VMware, Virtual PC).	N/A		
K0612	Knowledge of what constitutes a "threat" to a network.	1.3	3	80% or .8
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.	14.1	3	80% or .8
S0194	Skill in conducting non-attributable research.	1.1	3	80% or .8
S0196	Skill in conducting research using deep web.	1.1	3	80% or .8
S0203	Skill in defining and characterizing all pertinent aspects of the operational environment.	1.6	3	90% or .9
S0211	Skill in developing or recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.	1- 18	4	100% or 1

NCWF JOB ROLE

Warning Analyst

Job Role Description: A Warning Analyst develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Warning Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
S0218	Skill in evaluating information for reliability, validity, and relevance.	1.1 - 1.11	4	100% or 1
S0227	Skill in identifying alternative analytical interpretations in order to minimize unanticipated outcomes.	1- 18	4	100% or 1
S0228	Skill in identifying critical target elements, to include critical target elements for the cyber domain.	1- 18	4	100% or 1
S0229	Skill in identifying cyber threats which may jeopardize organization and/or partner interests.	1.6, 1.10	4	100% or 1
S0249	Skill in preparing and presenting briefings.	1- 18	4	100% or 1
S0256	Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.	1.6, 1.10	4	100% or 1
S0278	Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).	1.6, 1.10	4	100% or 1
S0285	Skill in using Boolean operators to construct simple and complex queries.	N/A		
S0288	Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).	N/A		
S0289	Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.	2.1 - 2.14	4	100% or 1
S0296	Skill in utilizing feedback in order to improve processes, products, and services.	N/A		
S0297	Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).	N/A		
S0303	Skill in writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.	6.7, 7.9, 8.6, 9.6, 11.7, 12.6, 13.7, 14.8, 15.7, 16.2, 17.5, 18.8	4	100% or 1
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	1- 18	4	100% or 1
A0072	Ability to clearly articulate intelligence requirements into well-formulated research questions and data tracking variables for inquiry tracking purposes.	2.1 - 2.14	4	100% or 1
A0075	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	1- 18	4	100% or 1

NCWF JOB ROLE

Warning Analyst

Job Role Description: A Warning Analyst develops unique cyber indicators to maintain constant awareness of the status of the highly dynamic operating environment. Collects, processes, analyzes, and disseminates cyber warning assessments.

Maps To: Certified Ethical Hacker (CEH)

Mapping Summary: Performance-based learning and evaluation in CEH imparts specific KSAs that should be demonstrated by a Warning Analyst. CEH maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

KSA

ID	Statement	CEH Exam Objectives	NICE Proficiency	Relational Coefficient
A0080	Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.	1.1 - 1.11	4	100% or 1
A0082	Ability to effectively collaborate via virtual teams.	1.9	3	80% or .8
A0083	Ability to evaluate information for reliability, validity, and relevance.	1.6, 1.7	3	80% or .8
A0084	Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.	6.7, 7.9, 8.6, 9.6, 11.7, 12.6, 13.7, 14.8, 15.7, 16.2, 17.5, 18.8	4	100% or 1
A0087	Ability to focus research efforts to meet the customer's decision-making needs.	1.6, 1.7	4	100% or 1
A0088	Ability to function effectively in a dynamic, fast-paced environment.	1- 18	4	100% or 1
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.	1- 18	4	100% or 1
A0091	Ability to identify intelligence gaps.	1- 18	4	100% or 1
A0101	Ability to recognize and mitigate cognitive biases which may affect analysis.	1- 18	4	100% or 1
A0102	Ability to recognize and mitigate deception in reporting and analysis.	1- 18	4	100% or 1
A0106	Ability to think critically.	1- 18	4	100% or 1
A0107	Ability to think like threat actors.	1- 18	4	100% or 1
A0109	Ability to utilize multiple intelligence sources across all intelligence disciplines.	2.1 - 2.14	4	100% or 1
	Summary		**4**	**95% or .95**

NCWF JOB ROLE

Exploitation Analyst

Job Role Description: An Exploitation Analyst collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an Exploitation Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0570	Apply and utilize authorized cyber capabilities to enable access to targeted networks.	Apply	1.1 - 1.15, 3.1 - 3.10	3	100% or 1
T0572	Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements.	Apply	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
T0574	Apply and obey applicable statutes, laws, regulations and policies.	Apply	1.5, 1.6, 1.7	4	100% or 1
T0591	Perform analysis for target infrastructure exploitation activities.	Perform	4 - 15	3	100% or 1
T0600	Collaborate with other internal and external partner organizations on target access and operational issues.	Collaborate	3.1 - 3.10	3	90% or .9
T0603	Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers.	Communicate	3.1 - 3.10	4	90% or .9
T0608	Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.	Conduct, Analysis	1 - 16	3	90% or .9
T0614	Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access.	Conduct, Analysis	4.1 - 4.13	4	100% or 1
T0641	Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities.	Create	5.1 - 5.6	4	100% or 1
T0695	Examine intercept-related metadata and content with an understanding of targeting significance.	Examine, Evaluate	4.1 - 4.13	4	100% or 1
T0701	Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development.	Collaborate	3.8, 3.10	4	100% or 1
T0720	Identify gaps in our understanding of target technology and developing innovative collection approaches.	Identify, Analysis	3 - 15	4	90% or .9
T0727	Identify, locate, and track targets via geospatial analysis techniques.	Identify, Analysis	4.2	3	90% or .9

NCWF JOB ROLE

Exploitation Analyst

Job Role Description: An Exploitation Analyst collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an Exploitation Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0736	Lead or enable exploitation operations in support of organization objectives and target requirements.	Employ	1 - 16	4	100% or 1
T0738	Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications.	Maintain, Analyze	1.1, 1.2	3	90% or .9
T0754	Monitor target networks to provide indications and warning of target communications changes or processing failures.	Monitor, Evaluate	1 - 16	4	100% or 1
T0775	Produce network reconstructions.	Produce, Synthesize	1 - 16	4	100% or 1
T0777	Profile network or system administrators and their activities.	Profile	3.1 - 3.10	4	90% or .9
	Summary			**4**	**95% or .95**

NCWF JOB ROLE

Exploitation Analyst

Job Role Description: An Exploitation Analyst collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an Exploitation Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0131	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.	4.2, 4.9	4	100% or 1
K0142	Knowledge of collection management processes, capabilities, and limitations.	4.1 - 4.13	4	100% or 1
K0348	Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).	N/A		
K0349	Knowledge of a wide range of concepts associated with websites (e.g., website types, administration, functions, software systems, etc.).	4.2, 4.8, 10.3, 11.5	4	100% or 1
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	1.10, 6.6, 7.6, 8.12, 9.4, 10.4, 10.5, 10.6, 10.7, 10.8, 10.10, 10.11, 10.12, 11.5, 12.3, 12.5, 13.5, 13.6, 13.8, 13.9, 14.3	4	100% or 1
K0369	Knowledge of basic malicious activity concepts (e.g., foot printing, scanning and enumeration).	4.1 - 4.13, 06	4	100% or 1
K0370	Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	N/A		
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).	N/A		
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	4.2, 4.9, 4.11, 6.5, 6.6, 7.11	4	100% or 1

NCWF JOB ROLE

Exploitation Analyst

Job Role Description: An Exploitation Analyst collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an Exploitation Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0471	Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).	2.1 - 2.6	3	90% or .9
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.	2.5	3	90% or .9
K0351	Knowledge of all applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.	1.5, 1.6, 1.7	4	100% or 1
K0354	Knowledge of all relevant reporting and dissemination procedures.	1 - 16	4	100% or 1
K0368	Knowledge of basic implants.	1 - 16	4	100% or 1
K0371	Knowledge of basic principles of the collection development processes (e.g., Dialed Number Recognition, Social Network Analysis).	1 - 16	4	100% or 1
K0376	Knowledge of both internal and external customers and partner organizations, including information needs, objectives, structure, capabilities, etc.	3.1 - 3.10	4	100% or 1
K0379	Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.	3.1	3	70% or .7
K0388	Knowledge of collection searching/analyzing techniques and tools for chat/buddy list, emerging technologies, VOIP, Media Over IP, VPN, VSAT/wireless, web mail and cookies.	1 - 16	4	100% or 1
K0393	Knowledge of common networking devices and their configurations.	2 - 15	2	50% or .5
K0394	Knowledge of common reporting databases and tools.	16.1 - 16.6	4	100% or 1
K0397	Knowledge of concepts for operating systems (e.g., Linux, Unix.)	1 - 16	3	90% or .9
K0418	Knowledge of data flow process for terminal or environment collection.	2.5	4	100% or 1
K0430	Knowledge of evasion strategies and techniques.	9.5, 9.8	4	100% or 1
K0434	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.	8.1, 8.2, 8.3, 8.4, 9.1, 9.2	4	100% or 1
K0443	Knowledge of how hubs, switches, routers work together in the design of a network.	2 - 15	3	90% or .9
K0447	Knowledge of how to collect, view, and identify essential information on targets of interest from metadata (e.g., email, http).	4.1 - 4.13	4	100% or 1
K0451	Knowledge of identification and reporting processes.	1 - 16	4	100% or 1

NCWF JOB ROLE

Exploitation Analyst

Job Role Description: An Exploitation Analyst collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an Exploitation Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0470	Knowledge of Internet and routing protocols.	2.4	3	70% or .7
K0473	Knowledge of intrusion sets.	9.1, 9.2	4	100% or 1
K0484	Knowledge of midpoint collection (process, objectives, organization, targets, etc.).	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
K0487	Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	8.1, 9.1, 10.7	4	100% or 1
K0489	Knowledge of network topology.	2 - 15	3	90% or .9
K0509	Knowledge of organizational and partner authorities, responsibilities, and contributions to achieving objectives.	3.1 - 3.10	3	90% or .9
K0510	Knowledge of organizational and partner policies, tools, capabilities, and procedures.	1.5	4	100% or 1
K0523	Knowledge of products and nomenclature of major vendors (e.g., security suites - Trend Micro, Symantec, McAfee, Outpost, Panda, Kaspersky) and how differences affect exploitation/vulnerabilities.	5.4, 5.5	3	90% or .9
K0529	Knowledge of scripting	N/A		
K0535	Knowledge of strategies and tools for target research.	4.1 - 4.13	4	100% or 1
K0537	Knowledge of system administration concepts for the Unix/Linux and Windows operating systems (e.g., process management, directory structure, installed applications, Access Controls).	2 - 15	3	90% or .9
K0544	Knowledge of target intelligence gathering and operational preparation techniques and life cycles.	4.1 - 4.13	4	100% or 1
K0557	Knowledge of terminal or environmental collection (process, objectives, organization, targets, etc.).	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
K0559	Knowledge of the basic structure, architecture, and design of converged applications.	10.1	3	90% or .9
K0608	Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).	2 - 15	3	90% or .9
S0066	Skill in identifying gaps in technical capabilities.	1.1	3	90% or .9
S0184	Skill in analyzing traffic to identify network devices.	8.1 - 8.14, 9.1 - 9.8	4	100% or 1
S0199	Skill in creating and extracting important information from packet captures.	2.1 - 2.6	4	100% or 1
S0200	Skill in creating collection requirements in support of data acquisition activities.	3.1, 3.7	3	90% or .9

NCWF JOB ROLE

Exploitation Analyst

Job Role Description: An Exploitation Analyst collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an Exploitation Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0201	Skill in creating plans in support of remote operations.	3.1 - 3.10	3	90% or .9
S0204	Skill in depicting source or collateral data on a network map.	7.2	4	100% or 1
S0207	Skill in determining the effect of various router and firewall configurations on traffic patterns and network performance in both LAN and WAN environments.	8.5 - 8.12	3	80% or .8
S0214	Skill in evaluating accesses for intelligence value.	4.3	2	50% or .5
S0223	Skill in generating operation plans in support of mission and target requirements.	3.1 - 3.10	4	100% or 1
S0236	Skill in identifying the devices that work at each level of protocol models.	2.1 - 2.6, 3.1 - 3.10	3	80% or .8
S0237	Skill in identifying, locating, and tracking targets via geospatial analysis techniques	4.2	3	80% or .8
S0239	Skill in interpreting compiled and interpretive programming languages.	6.6	2	50% or .5
S0240	Skill in interpreting metadata and content as applied by collection systems.	4.1 - 4.13	3	90% or .9
S0245	Skill in navigating network visualization software.	2 - 15	3	90% or .9
S0247	Skill in performing data fusion from existing intelligence for enabling new and continued collection.	4.1 - 4.13	4	100% or 1
S0258	Skill in recognizing and interpreting malicious network activity in traffic.	6.2, 6.6, 7.11, 7.12, 9.3, 9.4, 9.8, 12.1, 13.4, 13.5, 14.2	4	100% or 1
S0260	Skill in recognizing midpoint opportunities and essential information.	1.1	3	70% or .7
S0264	Skill in recognizing technical information that may be used for leads to enable remote operations (data includes users, passwords, email addresses, IP ranges of the target, frequency in DNI behavior, mail servers, domain servers, SMTP header information).	4.1 - 4.13	4	100% or 1
S0269	Skill in researching vulnerabilities and exploits utilized in traffic.	5.1 - 5.6	4	100% or 1
S0279	Skill in target development in direct support of collection operations.	4.1 - 4.13	4	100% or 1
S0286	Skill in using databases to identify target-relevant information.	4.5, 4.10, 11.2, 11.4, 12.1 - 12.9	4	100% or 1

NCWF JOB ROLE

Exploitation Analyst

Job Role Description: An Exploitation Analyst collaborates to identify access and collection gaps that can be satisfied through cyber collection and/or preparation activities. Leverages all authorized resources and analytic techniques to penetrate targeted networks.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an Exploitation Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0290	Skill in using non-attributable networks.	N/A		
S0294	Skill in using trace route tools and interpreting the results as they apply to network analysis and reconstruction.	4.7	3	70% or .7
S0300	Skill in writing (and submitting) requirements to meet gaps in technical capabilities.	3.1 - 3.10	4	100% or 1
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	4.1 - 4.13	3	70% or .7
A0075	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0080	Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0084	Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0074	Ability to collaborate effectively with others.	3.1 - 3.10	4	100% or 1
A0086	Ability to expand network access by conducting target analysis and collection in order to identify targets of interest.	4.1 - 4.13	4	100% or 1
A0092	Ability to identify/describe target vulnerability.	1 - 16	4	100% or 1
A0093	Ability to identify/describe techniques/methods for conducting technical exploitation of the target.	1 - 16	4	100% or 1
A0104	Ability to select the appropriate implant to achieve operational goals.	3.1 - 3.10	4	100% or 1
	Summary		**4**	**90% or .9**

NCWF JOB ROLE

All-Source Analyst

Job Role Description: An All-Source Analyst analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All-Source Analyst. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0569	Answer requests for information.	Answer, Analyze	4.1 - 4.13	3	80% or .8
T0582	Provide expertise to course of action development.	Provide	3.8	3	70% or .7
T0583	Provide subject matter expertise to the development of a common operational picture.	Provide	3.8	3	70% or .7
T0584	Maintain a common intelligence picture.	Maintain	4.3	3	90% or .9
T0585	Provide subject matter expertise to the development of cyber operations specific indicators.	Provide	3.8	3	70% or .7
T0586	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Assist	3.1 - 3.10	3	90% or .9
T0589	Assist in the identification of intelligence collection shortfalls.	Assist	4.1 - 4.13	3	90% or .9
T0593	Brief threat and/or target current situations.	Brief	5.1 - 5.6	3	90% or .9
T0597	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Collaborate	4.1 - 4.13	3	90% or .9
T0615	Conduct in-depth research and analysis.	Conduct	4.1 - 4.13, 5.1 - 5.6	3	90% or .9
T0617	Conduct nodal analysis.		N/A		
T0642	Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.	Maintain	4.1 - 4.13	3	90% or .9
T0660	Develop information requirements necessary for answering priority information requests.	Develop	3.1 - 3.10	3	90% or .9
T0678	Engage customers to understand customers' intelligence needs and wants.	Engage	3.1 - 3.10	4	100% or 1
T0685	Evaluate threat decision-making processes.	Evaluate	3.1 - 3.10	3	90% or .9
T0686	Identify threat vulnerabilities.	Identify	5.1 - 5.6	4	100% or 1
T0687	Identify threats to Blue Force vulnerabilities.	Identify	5.1 - 5.6	4	100% or 1

NCWF JOB ROLE

All-Source Analyst

Job Role Description: An All-Source Analyst analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All-Source Analyst. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0707	Generate requests for information.	Generate	3.1 - 3.10	4	100% or 1
T0708	Identify threat tactics, and methodologies.	Identify	1.11	4	100% or 1
T0710	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Identify	5.1 - 5.6	3	90% or .9
T0713	Identify and submit intelligence requirements for the purposes of designating priority information requirements.	Identify	3.1 - 3.10	4	100% or 1
T0718	Identify intelligence gaps and shortfalls.	Identify	1.1	3	90% or .9
T0748	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Monitor	1 - 16	4	100% or 1
T0749	Monitor and report on validated threat activities.	Monitor	5.1 - 5.6	4	100% or 1
T0751	Monitor open source websites for hostile content directed towards organizational or partner interests.	Monitor	4.1 - 4.13	4	100% or 1
T0752	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	Monitor	4.1 - 4.13	4	100% or 1
T0758	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	Produce	1.1 - 1.15, 5.1 - 5.6	4	100% or 1
T0761	Provide SME and support to planning/developmental forums and working groups as appropriate.	Provide	3.1 - 3.10	3	90% or .9
T0771	Provide subject matter expertise to website characterizations.	Provide	10.1 - 10.12	4	100% or 1
T0782	Provide analyses and support for effectiveness assessment.	Provide	5.1 - 5.6	3	90% or .9
T0783	Provide current intelligence support to critical internal/external stakeholders as appropriate.	Provide	3.1 - 3.10	4	100% or 1
T0785	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	Provide	1 - 16	4	100% or 1

NCWF JOB ROLE

All-Source Analyst

Job Role Description: An All-Source Analyst analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All-Source Analyst. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0786	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Provide	3.1 - 3.10	3	90% or .9
T0788	Provide input and assist in post-action effectiveness assessments.	Provide	5.2	3	90% or .9
T0789	Provide input and assist in the development of plans and guidance.	Provide	1.10	3	90% or .9
T0792	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.	Provide	1 - 16	4	100% or 1
T0797	Provide target recommendations which meet leadership objectives.	Provide	3.1 - 3.10	3	90% or .9
T0800	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.	Provide	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
T0805	Report intelligence-derived significant network events and intrusions.	Report	9.1 - 9.8	3	90% or .9
T0834	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	Examine	1.1 - 1.15, 3.1 - 3.10	3	90% or .9
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

All-Source Analyst

Job Role Description: An All-Source Analyst analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All-Source Analyst. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0036	Knowledge of human-computer interaction principles.	N/A		
K0058	Knowledge of network traffic analysis methods.	6.2, 6.6, 7.11, 7.12, 9.3, 13.4, 14.2	4	100% or 1
K0348	Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).	N/A		
K0349	Knowledge of a wide range of concepts associated with websites (e.g., website types, administration, functions, software systems, etc.).	4.2, 4.8, 10.3, 11.5	4	100% or 1
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	1.10, 6.6, 7.6, 8.12, 9.4, 10.4, 10.5, 10.6, 10.7, 10.8, 10.10, 10.11, 10.12, 11.5, 12.3, 12.5, 13.5, 13.6, 13.8, 13.9, 14.3	4	100% or 1
K0369	Knowledge of basic malicious activity concepts (e.g., foot printing, scanning and enumeration).	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
K0370	Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	N/A		
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	4.2, 4.9, 4.11, 6.5, 6.6, 7.11	4	100% or 1

NCWF JOB ROLE

All-Source Analyst

Job Role Description: An All-Source Analyst analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All-Source Analyst. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0471	Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).	2.1 - 2.6	3	90% or .9
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.	2.5	4	100% or 1
K0377	Knowledge of classification and control markings standards, policies and procedures.	1.5, 1.6	4	100% or 1
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).	7.7	3	50% or .5
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)	N/A		
K0405	Knowledge of current computer-based intrusion sets.	9.2	4	100% or 1
K0409	Knowledge of cyber intelligence/information collection capabilities and repositories.	2.1 - 2.6	4	100% or 1
K0427	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).	N/A		
K0431	Knowledge of evolving/emerging communications technologies.	1.1	3	90% or .9
K0436	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber attack, cyber defense), principles, capabilities, limitations, and effects.	1.1 - 1.15	4	100% or 1
K0437	Knowledge of general SCADA system components.	N/A	3	90% or .9
K0440	Knowledge of host-based security products and how they affect exploitation and vulnerability.	5.5, 7.13, 9.8	3	90% or .9
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.	N/A		
K0446	Knowledge of how modern wireless communications systems impact cyber operations.	13.1	3	90% or .9
K0449	Knowledge of how to extract, analyze, and use metadata.	4.1 - 4.13	4	100% or 1
K0458	Knowledge of intelligence disciplines.	4.3	4	100% or 1
K0460	Knowledge of intelligence preparation of the environment and similar processes.	4.3	3	70% or .7
K0464	Knowledge of intelligence support to planning, execution, and assessment.	4.1 - 4.13	3	70% or .7
K0469	Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions.	1.2	3	90% or .9

NCWF JOB ROLE

All-Source Analyst

Job Role Description: An All-Source Analyst analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All-Source Analyst. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0480	Knowledge of malware.	7.7	3	50% or .5
K0511	Knowledge of organizational hierarchy and cyber decision making processes.	4.1 - 4.13	1	50% or .5
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	N/A		
K0556	Knowledge of telecommunications fundamentals.	N/A		
K0561	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	8.1 to 8.4	4	100% or 1
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	2.1 - 2.6	4	100% or 1
K0603	Knowledge of the ways in which targets or threats use the Internet.	1 - 16	4	100% or 1
K0604	Knowledge of threat and/or target systems.	1 - 16	4	100% or 1
K0610	Knowledge of virtualization products (VMware, Virtual PC).	N/A		
K0612	Knowledge of what constitutes a "threat" to a network.	1.2	4	100% or 1
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.	N/A		
K0357	Knowledge of analytical constructs and their use in assessing the operational environment.	N/A		
K0410	Knowledge of cyber laws and their effect on Cyber planning.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
K0457	Knowledge of intelligence confidence levels.	4.1 - 4.13	4	100% or 1
K0465	Knowledge of internal and external partner cyber operations capabilities and tools.	1 - 16	4	100% or 1
K0507	Knowledge of organization or partner exploitation of digital networks.	1 - 16	4	100% or 1
K0515	Knowledge of OSI model and underlying networking protocols (e.g., TCP/IP).	2.1 - 2.6	4	100% or 1
K0533	Knowledge of specific target identifiers, and their usage.	1 - 16	4	100% or 1
K0542	Knowledge of target development (i.e., concepts, roles, responsibilities, products, etc.).	1 - 16	4	100% or 1

NCWF JOB ROLE

All-Source Analyst

Job Role Description: An All-Source Analyst analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All-Source Analyst. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0549	Knowledge of target or threat cyber actors and procedures.	1.1	4	100% or 1
K0551	Knowledge of targeting cycles.	1 - 16	4	100% or 1
K0577	Knowledge of the intelligence frameworks, processes, and related systems.	4.1 - 4.13	3	50% or .5
K0598	Knowledge of the structure and intent of organization specific plans, guidance and authorizations.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
S0194	Skill in conducting non-attributable research.	1.1	3	90% or .9
S0203	Skill in defining and characterizing all pertinent aspects of the operational environment.	3.1 - 3.10	4	100% or 1
S0211	Skill in developing or recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.	1 - 16	4	100% or 1
S0218	Skill in evaluating information for reliability, validity, and relevance.	1.1 - 1.15	4	100% or 1
S0227	Skill in identifying alternative analytical interpretations in order to minimize unanticipated outcomes.	1 - 16	4	100% or 1
S0229	Skill in identifying cyber threats which may jeopardize organization and/or partner interests.	5.1 - 5.6	3	90% or .9
S0249	Skill in preparing and presenting briefings.	1 - 16	4	100% or 1
S0256	Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.	5.1 - 5.6	3	90% or .9
S0278	Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).	5.1 - 5.6	3	90% or .9
S0285	Skill in using Boolean operators to construct simple and complex queries.	N/A		
S0288	Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).	N/A		
S0289	Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.	4.1 - 4.13	3	90% or .9
S0296	Skill in utilizing feedback in order to improve processes, products, and services.	N/A		
S0297	Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).	N/A		
S0303	Skill in writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.	1 - 16	4	100% or 1

NCWF JOB ROLE

All-Source Analyst

Job Role Description: An All-Source Analyst analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All-Source Analyst. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0189	Skill in assessing and/or estimating effects generated during and after cyber operations.	1 - 16	4	100% or 1
S0254	Skill in providing analysis to aid writing phased after action reports.	3.1 - 3.10, 16.1 - 16.6	4	100% or 1
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	4.1 - 4.13	3	90% or .9
A0075	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0080	Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0084	Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0072	Ability to clearly articulate intelligence requirements into well-formulated research questions and data tracking variables for inquiry tracking purposes.	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
A0082	Ability to effectively collaborate via virtual teams.	3.1 - 3.10	3	90% or .9
A0083	Ability to evaluate information for reliability, validity, and relevance.	1.1 - 1.15	3	90% or .9
A0085	Ability to exercise judgment when policies are not well-defined.	1.1 - 1.15	3	90% or .9
A0087	Ability to focus research efforts to meet the customer's decision-making needs.	3.1 - 3.10	3	90% or .9
A0088	Ability to function effectively in a dynamic, fast-paced environment.	3.1 - 3.10	3	90% or .9
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.	3.1 - 3.10	3	90% or .9
A0091	Ability to identify intelligence gaps.	1.1	3	90% or .9
A0101	Ability to recognize and mitigate cognitive biases which may affect analysis.	1.1 - 1.15	3	90% or .9
A0102	Ability to recognize and mitigate deception in reporting and analysis.	16.1 - 16.6	3	90% or .9
A0106	Ability to think critically.	1.1 - 1.15	3	90% or .9

NCWF JOB ROLE

All-Source Analyst

Job Role Description: An All-Source Analyst analyzes data/information from one or multiple sources to conduct preparation of the environment, respond to requests for information, and submit intelligence collection and production requirements in support of planning and operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All-Source Analyst. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
A0107	Ability to think like threat actors.	1.1 - 1.15	3	90% or .9
A0108	Ability to understand objectives and effects.	3.1 - 3.10	3	90% or .9
A0109	Ability to utilize multiple intelligence sources across all intelligence disciplines.	3.1 - 3.10	3	90% or .9
	Summary		**4**	**90% or .9**

NCWF JOB ROLE

Mission Assessment Specialist

Job Role Description: Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Mission Assessment Specialist. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0582	Provide expertise to course of action development.	Provide	3.8	3	70% or .7
T0583	Provide subject matter expertise to the development of a common operational picture.	Provide	3.8	3	70% or .7
T0585	Provide subject matter expertise to the development of cyber operations specific indicators.	Provide	3.8	3	70% or .7
T0586	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Assist	3.1 - 3.10	3	90% or .9
T0588	Provide expertise to the development of measures of effectiveness and measures of performance.		N/A		
T0589	Assist in the identification of intelligence collection shortfalls.	Assist	4.1 - 4.13	3	90% or .9
T0593	Brief threat and/or target current situations.	Brief	5.1 - 5.6	3	90% or .9
T0597	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Collaborate	4.1 - 4.13	3	90% or .9
T0611	Conduct end-of-operations assessments.	Conduct	3.1 - 3.10	3	90% or .9
T0615	Conduct in-depth research and analysis.	Conduct	4.1 - 4.13, 5.1 - 5.6	3	90% or .9
T0617	Conduct nodal analysis.		N/A		
T0624	Conduct target research and analysis.	Conduct	4.1 - 4.13, 5.1 - 5.6	4	100% or 1
T0660	Develop information requirements necessary for answering priority information requests.	Develop	3.1 - 3.10	3	90% or .9
T0661	Develop measures of effectiveness and measures of performance.	Develop	3.1 - 3.10	3	90% or .9
T0663	Develop munitions effectiveness assessment or operational assessment materials.	Develop	5.1 - 5.6	3	90% or .9
T0678	Engage customers to understand customers' intelligence needs and wants.	Engage	3.1 - 3.10	4	100% or 1
T0684	Estimate operational effects generated through cyber activities.	Estimate	3.1 - 3.10, 5.1 - 5.6	3	90% or .9

NCWF JOB ROLE

Mission Assessment Specialist

Job Role Description: Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Mission Assessment Specialist. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0685	Evaluate threat decision-making processes.	Evaluate	3.1 - 3.10	3	90% or .9
T0686	Identify threat vulnerabilities.	Identify	5.1 - 5.6	4	100% or 1
T0707	Generate requests for information.	Generate	3.1 - 3.10	4	100% or 1
T0718	Identify intelligence gaps and shortfalls.	Identify	1.1	3	90% or .9
T0748	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Monitor	1 - 16	4	100% or 1
T0749	Monitor and report on validated threat activities.	Monitor	5.1 - 5.6	4	100% or 1
T0752	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	Monitor	4.1 - 4.13	4	100% or 1
T0758	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	Produce	1.1 - 1.15, 5.1 - 5.6	4	100% or 1
T0761	Provide SME and support to planning/developmental forums and working groups as appropriate.	Provide	3.1 - 3.10	3	90% or .9
T0782	Provide analyses and support for effectiveness assessment.	Provide	5.1 - 5.6	3	90% or .9
T0783	Provide current intelligence support to critical internal/external stakeholders as appropriate.	Provide	3.1 - 3.10	4	100% or 1
T0785	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	Provide	1 - 16	4	100% or 1
T0786	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Provide	3.1 - 3.10	3	90% or .9
T0788	Provide input and assist in post-action effectiveness assessments.	Provide	5.2	3	90% or .9
T0789	Provide input and assist in the development of plans and guidance.	Provide	1.1	3	90% or .9

NCWF JOB ROLE

Mission Assessment Specialist

Job Role Description: Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Mission Assessment Specialist. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0793	Provide effectiveness support to designated exercises, and/or time sensitive operations.		N/A		
T0797	Provide target recommendations which meet leadership objectives.	Provide	3.1 - 3.10	3	90% or .9
T0834	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	Examine	1.1 - 1.15, 3.1 - 3.10	3	90% or .9
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

Mission Assessment Specialist

Job Role Description: Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Mission Assessment Specialist. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0036	Knowledge of human-computer interaction principles.	N/A		
K0058	Knowledge of network traffic analysis methods.	6.2, 6.6, 7.11, 7.12, 9.3, 13.4, 14.2	4	100% or 1
K0348	Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).	N/A		
K0349	Knowledge of a wide range of concepts associated with websites (e.g., website types, administration, functions, software systems, etc.).	4.2, 4.8, 10.3, 11.5	4	100% or 1
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	1.10, 6.6, 7.6, 8.12, 9.4, 10.4, 10.5, 10.6, 10.7, 10.8, 10.10, 10.11, 10.12, 11.5, 12.3, 12.5, 13.5, 13.6, 13.8, 13.9, 14.3	4	100% or 1
K0369	Knowledge of basic malicious activity concepts (e.g., foot printing, scanning and enumeration).	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
K0370	Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	N/A		
K0377	Knowledge of classification and control markings standards, policies and procedures.	1.5, 1.6	4	100% or 1
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).	7.7	3	90% or .9

NCWF JOB ROLE

Mission Assessment Specialist

Job Role Description: Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Mission Assessment Specialist. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)	N/A		
K0405	Knowledge of current computer-based intrusion sets.	9.2	4	100% or 1
K0409	Knowledge of cyber intelligence/information collection capabilities and repositories.	2.1 - 2.6	4	100% or 1
K0410	Knowledge of cyber laws and their effect on Cyber planning.	1.7	4	100% or 1
K0414	Knowledge of cyber operations support or enabling processes.	1.1 - 1.15	3	90% or .9
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).	N/A		
K0427	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).	N/A		
K0431	Knowledge of evolving/emerging communications technologies.	1.1	3	90% or .9
K0436	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber attack, cyber defense), principles, capabilities, limitations, and effects.	1.1 - 1.15	4	100% or 1
K0437	Knowledge of general SCADA system components.	N/A	3	90% or .9
K0440	Knowledge of host-based security products and how they affect exploitation and vulnerability.	5.5, 7.13, 9.8	3	90% or .9
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	4.1 - 4.13	3	90% or .9
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.	N/A		
K0446	Knowledge of how modern wireless communications systems impact cyber operations.	13.1	3	90% or .9
K0449	Knowledge of how to extract, analyze, and use metadata.	4.1 - 4.13	4	100% or 1
K0457	Knowledge of intelligence confidence levels.	4.1 - 4.13	4	100% or 1
K0460	Knowledge of intelligence preparation of the environment and similar processes.	4.3	3	70% or .7
K0464	Knowledge of intelligence support to planning, execution, and assessment.	4.1 - 4.13	3	70% or .7
K0465	Knowledge of internal and external partner cyber operations capabilities and tools.	3.1 - 3.10	3	90% or .9

NCWF JOB ROLE

Mission Assessment Specialist

Job Role Description: Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Mission Assessment Specialist. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0469	Knowledge of internal tactics to anticipate and/or emulate threat capabilities and actions.	1.2	3	90% or .9
K0471	Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).	N/A		
K0480	Knowledge of malware.	7.7	3	90% or .9
K0507	Knowledge of organization or partner exploitation of digital networks.	1 - 16	3	90% or .9
K0511	Knowledge of organizational hierarchy and cyber decision making processes.	4.1 - 4.13	1	50% or .5
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	2 - 15	4	100% or 1
K0549	Knowledge of target or threat cyber actors and procedures.	5.1 - 5.6	4	100% or 1
K0551	Knowledge of targeting cycles.	1.1	4	100% or 1
K0556	Knowledge of telecommunications fundamentals.	N/A		
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.	2 - 15	4	100% or 1
K0561	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	8.1 - 8.4	4	100% or 1
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	2.1 - 2.6	4	100% or 1
K0598	Knowledge of the structure and intent of organization specific plans, guidance and authorizations.			
K0603	Knowledge of the ways in which targets or threats use the Internet.	1 - 16	4	100% or 1
K0604	Knowledge of threat and/or target systems.	1 - 16	4	100% or 1
K0610	Knowledge of virtualization products (VMware, Virtual PC).	N/A		
K0612	Knowledge of what constitutes a "threat" to a network.	1.2	4	100% or 1
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.	13.1 - 13.9	4	90% or .9

NCWF JOB ROLE

Mission Assessment Specialist

Job Role Description: Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Mission Assessment Specialist. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0189	Skill in assessing and/or estimating effects generated during and after cyber operations.	3.1 - 3.10	4	100% or 1
S0194	Skill in conducting non-attributable research.	1.1	3	90% or .9
S0203	Skill in defining and characterizing all pertinent aspects of the operational environment.	3.1 - 3.10	4	100% or 1
S0211	Skill in developing or recommending analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.	1 - 16	4	100% or 1
S0216	Skill in evaluating available capabilities against desired effects in order to provide effective courses of action.	1 - 16	4	100% or 1
S0218	Skill in evaluating information for reliability, validity, and relevance.	1.1 - 1.15	4	100% or 1
S0227	Skill in identifying alternative analytical interpretations in order to minimize unanticipated outcomes.	1 - 16	4	100% or 1
S0228	Skill in identifying critical target elements, to include critical target elements for the cyber domain.	5.1 - 5.6	3	
S0229	Skill in identifying cyber threats which may jeopardize organization and/or partner interests.	5.1 - 5.6	3	90% or .9
S0249	Skill in preparing and presenting briefings.	1 - 16	4	100% or 1
S0254	Skill in providing analysis to aid writing phased after action reports.	6.1 - 6.9	3	90% or .9
S0256	Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.	5.1 - 5.6	3	90% or .9
S0271	Skill in reviewing and editing assessment products.	N/A		
S0278	Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).	5.1 - 5.6	3	90% or .9
S0285	Skill in using Boolean operators to construct simple and complex queries.	N/A		
S0288	Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).	N/A		
S0289	Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.	4.1 - 4.13	3	90% or .9
S0292	Skill in using targeting databases and software packages.	12.1 - 12.9	4	100% or 1
S0296	Skill in utilizing feedback in order to improve processes, products, and services.	N/A		

NCWF JOB ROLE

Mission Assessment Specialist

Job Role Description: Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Mission Assessment Specialist. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0297	Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).	N/A		
S0303	Skill in writing, reviewing and editing cyber-related Intelligence/assessment products from multiple sources.	1 - 16	4	100% or 1
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	4.1 - 4.13	3	90% or .9
A0075	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0080	Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0084	Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0072	Ability to clearly articulate intelligence requirements into well-formulated research questions and data tracking variables for inquiry tracking purposes.	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
A0082	Ability to effectively collaborate via virtual teams.	3.1 - 3.10	3	90% or .9
A0083	Ability to evaluate information for reliability, validity, and relevance.	1.1 - 1.15	3	90% or .9
A0087	Ability to focus research efforts to meet the customer's decision-making needs.	3.1 - 3.10	3	90% or .9
A0088	Ability to function effectively in a dynamic, fast-paced environment.	3.1 - 3.10	3	90% or .9
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.	3.1 - 3.10	3	90% or .9
A0091	Ability to identify intelligence gaps.	1.1	3	90% or .9
A0101	Ability to recognize and mitigate cognitive biases which may affect analysis.	1.1 - 1.15	3	90% or .9
A0102	Ability to recognize and mitigate deception in reporting and analysis.	16.1 - 16.6	3	90% or .9
A0106	Ability to think critically.	1.1 - 1.15	3	90% or .9
A0107	Ability to think like threat actors.	1.1 - 1.15	3	90% or .9

NCWF JOB ROLE

Mission Assessment Specialist

Job Role Description: Develops assessment plans and measures of performance/effectiveness. Conducts strategic and operational effectiveness assessments as required for cyber events. Determines whether systems performed as expected and provides input to the determination of operational effectiveness.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Mission Assessment Specialist. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
A0109	Ability to utilize multiple intelligence sources across all intelligence disciplines.	3.1 - 3.10	3	90% or .9
A0085	Ability to exercise judgment when policies are not well-defined.	1.1 - 1.15	3	90% or .9
A0108	Ability to understand objectives and effects.	3.1 - 3.10	3	90% or .9
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

Target Developer

Job Role Description: Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Developer. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0597	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Collaborate	4.1 - 4.13	3	90% or .9
T0617	Conduct nodal analysis.		N/A		
T0707	Generate requests for information.	Generate	3.1 - 3.10	4	100% or 1
T0582	Provide expertise to course of action development.	Provide	3.8	3	70% or .7
T0782	Provide analyses and support for effectiveness assessment.	Provide	5.1 - 5.6	3	90% or .9
T0797	Provide target recommendations which meet leadership objectives.	Provide	3.1 - 3.10	3	90% or .9
T0588	Provide expertise to the development of measures of effectiveness and measures of performance.		N/A		
T0624	Conduct target research and analysis.	Conduct	4.1 - 4.13, 5.1 - 5.6	4	100% or 1
T0661	Develop measures of effectiveness and measures of performance.	Develop	3.1 - 3.10	3	90% or .9
T0663	Develop munitions effectiveness assessment or operational assessment materials.	Develop	5.1 - 5.6	3	90% or .9
T0684	Estimate operational effects generated through cyber activities.	Estimate	3.1 - 3.10, 5.1 - 5.6	3	90% or .9
T0642	Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.	Maintain	4.1 - 4.13	3	90% or .9
T0710	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Identify	5.2	3	90% or .9
T0561	Accurately characterize targets.	Characterize	4.1 - 4.13	4	100% or 1
T0594	Build and maintain electronic target folders.	Build	4.1 - 4.13	4	100% or 1
T0599	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.	Collaborate	4.2, 4.3, 4.11	4	100% or 1
T0633	Coordinate target vetting with appropriate partners.	Coordinate	4.4	4	100% or 1
T0650	Determine what technologies are used by a given target.	Coordinate	4.2, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7	4	100% or 1

NCWF JOB ROLE

Target Developer

Job Role Description: Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Developer. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0652	Develop all-source intelligence targeting materials.	Develop	4.12, 6.8	4	100% or 1
T0688	Evaluate available capabilities against desired effects in order to recommend efficient solutions.	Evaluate	6.9	4	100% or 1
T0717	Identify critical target elements.	Identify	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
T0731	Initiate requests to guide tasking and assist with collection management.	Assist	5.1 - 5.6, 5.1 - 5.6, 6.1 - 6.9	4	100% or 1
T0744	Maintain target lists (i.e., RTL, JTL, CTL, etc.).	Maintain	4.2	4	100% or 1
T0769	Perform targeting automation activities.	Perform	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
T0770	Develop website characterizations.	Develop	4.2	4	100% or 1
T0776	Produce target system analysis products.	Produce	6.1 - 6.9	4	100% or 1
T0781	Provide aim point and re-engagement recommendations.	Provide	16.5	4	100% or 1
T0790	Provide input for targeting effectiveness assessments for leadership acceptance.	Provide	16.4	4	100% or 1
T0794	Provide operations and re-engagement recommendations.	Provide	16.4, 16.5	4	100% or 1
T0798	Provide targeting products and targeting support as designated.	Provide	16.4, 16.5	4	100% or 1
T0799	Provide time sensitive targeting support.	Provide	16.4, 16.5	4	100% or 1
T0802	Review appropriate information sources to determine validity and relevance of information gathered.	Review	16.4, 16.5	4	100% or 1
T0815	Sanitize and minimize information to protect sources and methods.	Sanitize	16.3	4	100% or 1
T0824	Support identification and documentation of collateral effects.	Support	16.4, 16.5	4	100% or 1
T0835	Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date.	Identify	16.4, 16.5	4	100% or 1
	Summary			**4**	**95% or .95**

NCWF JOB ROLE

Target Developer

Job Role Description: Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Developer. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0036	Knowledge of human-computer interaction principles.	N/A		
K0058	Knowledge of network traffic analysis methods.	6.2, 6.6, 7.11, 7.12, 9.3, 13.4, 14.2	4	100% or 1
K0142	Knowledge of collection management processes, capabilities, and limitations.	4.1 - 4.13	4	100% or 1
K0173	Withdrawn – Integrated into K0499	N/A		
K0348	Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).	N/A		
K0349	Knowledge of a wide range of concepts associated with websites (e.g., website types, administration, functions, software systems, etc.).	4.2, 4.8, 10.3, 11.5	4	100% or 1
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	1.10, 6.6, 7.6, 8.12, 9.4, 10.4, 10.5, 10.6, 10.7, 10.8, 10.10, 10.11, 10.12, 11.5, 12.3, 12.5, 13.5, 13.6, 13.8, 13.9, 14.3	4	100% or 1
K0369	Knowledge of basic malicious activity concepts (e.g., foot printing, scanning and enumeration).	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
K0370	Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	N/A	3	90% or .9
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	4.9, 6.5, 7.11	3	90% or .9

NCWF JOB ROLE

Target Developer

Job Role Description: Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Developer. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0471	Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).	4.1 - 4.13	3	90% or .9
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.	N/A	4	100% or 1
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).	7.7	3	90% or .9
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)	N/A	4	100% or 1
K0409	Knowledge of cyber intelligence/information collection capabilities and repositories.	2.1 - 2.6	4	100% or 1
K0427	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).	N/A		
K0431	Knowledge of evolving/emerging communications technologies.	1.1	3	90% or .9
K0436	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber attack, cyber defense), principles, capabilities, limitations, and effects.	1.1 - 1.15	4	100% or 1
K0437	Knowledge of general SCADA system components.	N/A	3	90% or .9
K0440	Knowledge of host-based security products and how they affect exploitation and vulnerability.	5.5, 7.13, 9.8	3	90% or .9
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.	N/A		
K0446	Knowledge of how modern wireless communications systems impact cyber operations.	13.1	3	90% or .9
K0449	Knowledge of how to extract, analyze, and use metadata.	4.1 - 4.13	4	100% or 1
K0460	Knowledge of intelligence preparation of the environment and similar processes.	4.3	3	70% or .7
K0464	Knowledge of intelligence support to planning, execution, and assessment.	4.1 - 4.13	3	70% or .7
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	N/A	4	100% or 1
K0556	Knowledge of telecommunications fundamentals.	N/A	4	100% or 1

NCWF JOB ROLE

Target Developer

Job Role Description: Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Developer. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0561	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	8.1 - 8.4	4	100% or 1
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	2.1 - 2.6	4	100% or 1
K0603	Knowledge of the ways in which targets or threats use the Internet.	1 - 16	4	100% or 1
K0604	Knowledge of threat and/or target systems.	1 - 16	4	100% or 1
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.	CEH	4	100% or 1
K0457	Knowledge of intelligence confidence levels.	4.1 - 4.13	4	100% or 1
K0465	Knowledge of internal and external partner cyber operations capabilities and tools.	3.1 - 3.10	3	90% or .9
K0507	Knowledge of organization or partner exploitation of digital networks.	1 - 16	3	90% or .9
K0549	Knowledge of target or threat cyber actors and procedures.	5.1 - 5.6	4	100% or 1
K0551	Knowledge of targeting cycles.	1.1	4	100% or 1
K0598	Knowledge of the structure and intent of organization specific plans, guidance and authorizations.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).	N/A	4	100% or 1
K0458	Knowledge of intelligence disciplines.	4.3	4	100% or 1
K0357	Knowledge of analytical constructs and their use in assessing the operational environment.	N/A		
K0533	Knowledge of specific target identifiers, and their usage.	4.1 - 4.13	4	100% or 1
K0542	Knowledge of target development (i.e., concepts, roles, responsibilities, products, etc.).	4.1 - 4.13, 5.1 - 5.6, 6.1 - 6.9	4	100% or 1
K0351	Knowledge of all applicable statutes, laws, regulations and policies governing cyber targeting and exploitation.	1.5, 1.6, 1.7	4	100% or 1
K0379	Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.	4.1 - 4.13	4	100% or 1

NCWF JOB ROLE

Target Developer

Job Role Description: Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Developer. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0473	Knowledge of intrusion sets.	9.2	4	100% or 1
K0381	Knowledge of collateral damage and estimating impact(s).	N/A		
K0402	Knowledge of criticality and vulnerability factors (e.g., value, recuperation, cushion, countermeasures) for target selection and applicability to the cyber domain.	5.2	3	90% or .9
K0413	Knowledge of cyber operation objectives, policies, and legalities.	1.3, 1.5, 1.6, 1.7	4	100% or 1
K0426	Knowledge of dynamic and deliberate targeting.	4.1 - 4.13, 5.1 - 5.6, 6.1 - 6.9	4	100% or 1
K0439	Knowledge of governing authorities for targeting.	1.5, 1.6, 1.7	4	100% or 1
K0461	Knowledge of intelligence production processes.	4.3	4	100% or 1
K0466	Knowledge of internal and external partner intelligence processes and the development of information requirements and essential information.	4.3	4	100% or 1
K0478	Knowledge of legal considerations in targeting.	1.7	4	100% or 1
K0479	Knowledge of malware analysis and characteristics.	7.7	3	90% or .9
K0497	Knowledge of operational effectiveness assessment.	4.1 - 4.13	4	100% or 1
K0543	Knowledge of target estimated repair and recuperation times.	N/A		
K0546	Knowledge of target list development (i.e. RTL, JTL, CTL, etc.).	4.2	4	100% or 1
K0547	Knowledge of target methods and procedures.	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
K0555	Knowledge of TCP/IP networking protocols.	2.1 - 2.6	4	100% or 1
S0194	Skill in conducting non-attributable research.	4.1 - 4.13	4	100% or 1
S0203	Skill in defining and characterizing all pertinent aspects of the operational environment.	4.1 - 4.13	4	100% or 1
S0218	Skill in evaluating information for reliability, validity, and relevance.	4.1 - 4.13	4	100% or 1
S0227	Skill in identifying alternative analytical interpretations in order to minimize unanticipated outcomes.	4.1 - 4.13	4	100% or 1

NCWF JOB ROLE

Target Developer

Job Role Description: Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Developer. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0229	Skill in identifying cyber threats which may jeopardize organization and/or partner interests.	5.1 - 5.6	3	90% or .9
S0249	Skill in preparing and presenting briefings.	1 - 16	4	100% or 1
S0256	Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.	5.1 - 5.6	3	90% or .9
S0278	Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).	5.1 - 5.6	3	90% or .9
S0285	Skill in using Boolean operators to construct simple and complex queries.	N/A		
S0288	Skill in using multiple analytic tools, databases, and techniques (e.g., Analyst's Notebook, A-Space, Anchory, M3, divergent/convergent thinking, link charts, matrices, etc.).	N/A		
S0289	Skill in using multiple search engines (e.g., Google, Yahoo, LexisNexis, DataStar) and tools in conducting open-source searches.	4.1 - 4.13	3	90% or .9
S0296	Skill in utilizing feedback in order to improve processes, products, and services.	N/A		
S0297	Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).	N/A		
S0189	Skill in assessing and/or estimating effects generated during and after cyber operations.	3.1 - 3.10	4	100% or 1
S0228	Skill in identifying critical target elements, to include critical target elements for the cyber domain.	4.1 - 4.13, 5.1 - 5.6, 6.1 - 6.9	4	100% or 1
S0216	Skill in evaluating available capabilities against desired effects in order to provide effective courses of action.	5.1 - 5.6	4	100% or 1
S0292	Skill in using targeting databases and software packages.	11.1 - 11.7, 12.1 - 12.9	4	100% or 1
S0196	Skill in conducting research using deep web.	4.1 - 4.13	4	100% or 1
S0187	Skill in applying various analytical methods, tools, and techniques (e.g., competing hypotheses; chain of reasoning; scenario methods; denial and deception detection; high impact-low probability; network/ association or link analysis; Bayesian, Delphi, and Pattern analyses).	4.1 - 4.13 to 15	4	100% or 1
S0205	Skill in determining appropriate targeting options through the evaluation of available capabilities against desired effects.	4.1 - 4.13, 5.1 - 5.6,, 6.1 - 6.9	4	100% or 1

NCWF JOB ROLE

Target Developer

Job Role Description: Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Developer. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0208	Skill in determining the physical location of network devices.	6.2	4	100% or 1
S0222	Skill in fusion analysis	4 - 15	4	100% or 1
S0248	Skill in performing target system analysis.	5 - 15	4	100% or 1
S0274	Skill in reviewing and editing target materials.	5 - 15	4	100% or 1
S0287	Skill in using geospatial data and applying geospatial resources.	4.2	3	90% or .9
S0302	Skill in writing effectiveness reports.	16.1 - 16.6	4	100% or 1
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	4.1 - 4.13	3	90% or .9
A0075	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0080	Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0084	Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0087	Ability to focus research efforts to meet the customer's decision-making needs.	3.1 - 3.10	3	90% or .9
A0088	Ability to function effectively in a dynamic, fast-paced environment.	3.1 - 3.10	3	90% or .9
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.	3.1 - 3.10	3	90% or .9
A0091	Ability to identify intelligence gaps.	1.1	3	90% or .9
A0101	Ability to recognize and mitigate cognitive biases which may affect analysis.	1.1 - 1.15	3	90% or .9
A0102	Ability to recognize and mitigate deception in reporting and analysis.	16.1 - 16.6	3	90% or .9
A0106	Ability to think critically.	1.1 - 1.15	3	90% or .9
A0109	Ability to utilize multiple intelligence sources across all intelligence disciplines.	3.1 - 3.10	3	90% or .9

NCWF JOB ROLE

Target Developer

Job Role Description: Performs target system analysis, builds and/or maintains electronic target folders to include inputs from environment preparation, and/or internal or external intelligence sources. Coordinates with partner target activities and intelligence organizations, and presents candidate targets for vetting and validation.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Developer. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
A0085	Ability to exercise judgment when policies are not well-defined.	1.1 - 1.15	3	90% or .9
A0073	Ability to clearly articulate intelligence requirements into well-formulated research questions and requests for information.	4.3	4	100% or 1
	Summary		**4**	**95% or .95**

NCWF JOB ROLE

Target Network Analyst

Job Role Description: Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Network Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0617	Conduct nodal analysis.		N/A		
T0707	Generate requests for information.	Generate	3.1 - 3.10	4	100% or 1
T0582	Provide expertise to course of action development.	Provide	3.8	3	70% or .7
T0797	Provide target recommendations which meet leadership objectives.	Provide	3.1 - 3.10	3	90% or .9
T0624	Conduct target research and analysis.	Conduct	4.1 - 4.13, 5.1 - 5.6	4	100% or 1
T0710	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Identify	5.2	3	90% or .9
T0599	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.	Collaborate	4.2, 4.3, 4.11	4	100% or 1
T0650	Determine what technologies are used by a given target.	Coordinate	4.2, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7	4	100% or 1
T0802	Review appropriate information sources to determine validity and relevance of information gathered.	Review	16.4, 16.5	4	100% or 1
T0595	Classify documents in accordance with classification guidelines.	Classify	3.1 - 3.10	4	100% or 1
T0606	Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.	Compile	4.1 - 4.13, 5.1 - 5.6	4	100% or 1
T0607	Identify and conduct analysis of target communications to identify information essential to support operations.	Identify	6.1 - 6.9	4	100% or 1
T0621	Conduct quality control in order to determine validity and relevance of information gathered about networks.	Conduct	6.3 - 6.7	4	100% or 1
T0653	Apply analytic techniques to gain more target information.	Apply	4.1 - 4.13	4	100% or 1
T0692	Generate and evaluate the effectiveness of network analysis strategies.	Generate	6.1 - 6.9	4	100% or 1
T0706	Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)	Gather	4.1 - 4.13, 6.1 - 6.9	4	100% or 1

NCWF JOB ROLE

Target Network Analyst

Job Role Description: Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Network Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0715	Identify collection gaps and potential collection strategies against targets.	Identify	4.1 - 4.13	4	100% or 1
T0722	Identify network components and their functionality to enable analysis and target development.	Identify	6.2 - 6.7	4	100% or 1
T0745	Make recommendations to guide collection in support of customer requirements.	Recommendation	16.5	4	100% or 1
T0765	Provide subject matter expertise to development of exercises.	Provide	3.1 - 3.10	4	100% or 1
T0767	Perform content and/or metadata analysis to meet organization objectives.	Perform	4.1 - 4.13	4	100% or 1
T0778	Profile targets and their activities.	Profile	4.2, 4.3, 4.4	4	100% or 1
T0803	Reconstruct networks in diagram or report format.	Reconstruct	6.2	4	100% or 1
T0807	Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.	Research	1.1	3	90% or .9
	Summary			**4**	**100% or 1**

NCWF JOB ROLE

Target Network Analyst

Job Role Description: Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Network Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0348	Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).	N/A		
K0349	Knowledge of a wide range of concepts associated with websites (e.g., website types, administration, functions, software systems, etc.).	4.2, 4.8, 10.3, 11.5	4	100% or 1
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	1.10, 6.6, 7.6, 8.12, 9.4, 10.4, 10.5, 10.6, 10.7, 10.8, 10.10, 10.11, 10.12, 11.5, 12.3, 12.5, 13.5, 13.6, 13.8, 13.9, 14.3	4	100% or 1
K0369	Knowledge of basic malicious activity concepts (e.g., foot printing, scanning and enumeration).	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
K0370	Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	N/A		
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	4.9, 6.5, 7.11	3	90% or .9
K0471	Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).	4.1 - 4.13	3	90% or .9
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).	7.7	3	90% or .9

NCWF JOB ROLE

Target Network Analyst

Job Role Description: Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Network Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)	N/A		
K0431	Knowledge of evolving/emerging communications technologies.	1.1	3	90% or .9
K0436	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber attack, cyber defense), principles, capabilities, limitations, and effects.	1.1 - 1.15	4	100% or 1
K0440	Knowledge of host-based security products and how they affect exploitation and vulnerability.	5.5, 7.13, 9.8	3	90% or .9
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.	N/A		
K0449	Knowledge of how to extract, analyze, and use metadata.	4.1 - 4.13	4	100% or 1
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	N/A		
K0379	Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.	4.1 - 4.13	4	100% or 1
K0473	Knowledge of intrusion sets.	9.2	4	100% or 1
K0413	Knowledge of cyber operation objectives, policies, and legalities.	1.3, 1.5, 1.6, 1.7	4	100% or 1
K0439	Knowledge of governing authorities for targeting.	1.5, 1.6, 1.7	4	100% or 1
K0479	Knowledge of malware analysis and characteristics.	4.1 - 4.13	4	100% or 1
K0547	Knowledge of target methods and procedures.	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
K0487	Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	8.1, 9.1, 10.7	4	100% or 1
K0544	Knowledge of target intelligence gathering and operational preparation techniques and life cycles.	4.1 - 4.13	4	100% or 1
K0559	Knowledge of the basic structure, architecture, and design of converged applications.	10.1	3	90% or .9
K0389	Knowledge of collection sources including conventional and non-conventional sources.	4.1 - 4.13	4	100% or 1
K0403	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.	N/A		
K0424	Knowledge of denial and deception techniques.	9.4, 10.5, 13.5	3	90% or .9

NCWF JOB ROLE

Target Network Analyst

Job Role Description: Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Network Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0442	Knowledge of how converged technologies impact cyber operations (e.g., digital, telephony, wireless).	13.1	3	70% or .7
K0462	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions.	16.1, 16.2, 16.3	4	100% or 1
K0472	Knowledge of intrusion detection systems and signature development.	9.2	4	100% or 1
K0483	Knowledge of methods to integrate and summarize information from any potential sources.	4.1 - 4.13	4	100% or 1
K0500	Knowledge of organization and/or partner collection systems, capabilities, and processes (e.g., collection and protocol processors).	4.3, 4.4	4	100% or 1
K0520	Knowledge of principles and practices related to target development such as target knowledge, associations, communication systems, and infrastructure.	4.2, 4.3, 4.4	4	100% or 1
K0550	Knowledge of target, including related current events, communication profile, actors, and history (language, culture) and/or frame of reference.	4.2, 4.3, 4.4	4	100% or 1
K0567	Knowledge of the data flow from collection origin to repositories and tools.	4.5, 4.6, 4.7	4	100% or 1
K0592	Knowledge of the purpose and contribution of target templates.	4.4	3	90% or .9
K0599	Knowledge of the structure, architecture, and design of modern digital and telephony networks.	4.2, 4.8, 4.9	3	90% or .9
K0600	Knowledge of the structure, architecture, and design of modern wireless communications systems.	13.3	4	100% or 1
S0194	Skill in conducting non-attributable research.	4.1 - 4.13	4	100% or 1
S0203	Skill in defining and characterizing all pertinent aspects of the operational environment.	4.1 - 4.13	4	100% or 1
S0229	Skill in identifying cyber threats which may jeopardize organization and/or partner interests.	5.1 - 5.6	3	90% or .9
S0256	Skill in providing understanding of target or threat systems through the identification and link analysis of physical, functional, or behavioral relationships.	5.1 - 5.6	3	90% or .9
S0228	Skill in identifying critical target elements, to include critical target elements for the cyber domain.	4.1 - 4.13, 5.1 - 5.6,, 6.1 - 6.9	4	100% or 1

NCWF JOB ROLE

Target Network Analyst

Job Role Description: Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Network Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0196	Skill in conducting research using deep web.	4.1 - 4.13	4	100% or 1
S0187	Skill in applying various analytical methods, tools, and techniques (e.g., competing hypotheses; chain of reasoning; scenario methods; denial and deception detection; high impact-low probability; network/ association or link analysis; Bayesian, Delphi, and Pattern analyses).	4.1 - 4.13 - 15	4	100% or 1
S0205	Skill in determining appropriate targeting options through the evaluation of available capabilities against desired effects.	4.1 - 4.13, 5.1 - 5.6,, 6.1 - 6.9	4	100% or 1
S0208	Skill in determining the physical location of network devices.	6.2	4	100% or 1
S0222	Skill in fusion analysis	4.1 - 4.13 - 15	4	100% or 1
S0248	Skill in performing target system analysis.	5.1 - 5.6 - 15	4	100% or 1
S0274	Skill in reviewing and editing target materials.	5.1 - 5.6 - 15	4	100% or 1
S0287	Skill in using geospatial data and applying geospatial resources.	4.2	3	90% or .9
S0177	Skill in analyzing a target's communication networks.	6.1 - 6.9	4	100% or 1
S0178	Skill in analyzing essential network data (e.g., router configuration files, routing protocols).	6.1 - 6.9	3	90% or .9
S0181	Skill in analyzing midpoint collection data.	6.1 - 6.9	3	90% or .9
S0183	Skill in analyzing terminal or environment collection data.	6.1 - 6.9	3	90% or .9
S0191	Skill in assessing the applicability of available analytical tools to various situations.	4.1 - 4.13 - 15	4	100% or 1
S0197	Skill in conducting social network analysis, buddy list analysis, and/or cookie analysis.	4.2, 4.4	4	100% or 1
S0217	Skill in evaluating data sources for relevance, reliability, and objectivity.	4.1 - 4.13	4	100% or 1
S0219	Skill in evaluating information to recognize relevance, priority, etc.	4.1 - 4.13	4	100% or 1
S0220	Skill in exploiting/querying organizational and/or partner collection databases.	4.3	3	90% or .9
S0225	Skill in identifying a target's communications networks.	6.1 - 6.9	4	100% or 1
S0231	Skill in identifying how a target communicates.	6.1 - 6.9	4	100% or 1

NCWF JOB ROLE

Target Network Analyst

Job Role Description: Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Network Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0234	Skill in identifying leads for target development.	6.1 - 6.9	4	100% or 1
S0244	Skill in managing client relationships, including determining client needs/requirements, managing client expectations, and demonstrating commitment to delivering quality results.	3.1 - 3.10	4	100% or 1
S0246	Skill in number normalization.	N/A		
S0259	Skill in recognizing denial and deception techniques of the target.	9.4, 10.5, 13.5	3	90% or .9
S0261	Skill in recognizing relevance of information.	6.3 - 6.7	4	100% or 1
S0262	Skill in recognizing significant changes in a target's communication patterns.	6.1 - 6.9	4	100% or 1
S0263	Skill in recognizing technical information that may be used for leads for metadata analysis.	6.1 - 6.9	4	100% or 1
S0268	Skill in researching essential information.	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
S0277	Skill in synthesizing, analyzing, and prioritizing meaning across data sets.	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
S0280	Skill in target network anomaly identification (e.g., intrusions, dataflow or processing, target implementation of new technologies).	9.3, 9.4, 9.5, 9.6	4	100% or 1
S0291	Skill in using research methods including multiple, different sources to reconstruct a target network.	6.1 - 6.9	4	100% or 1
S0301	Skill in writing about facts and ideas in a clear, convincing, and organized manner.	16.1 - 16.6	4	100% or 1
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	4.1 - 4.13	3	90% or .9
A0075	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0080	Ability to develop or recommend analytic approaches or solutions to problems and situations for which information is incomplete or for which no precedent exists.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0084	Ability to evaluate, analyze, and synthesize large quantities of data (which may be fragmented and contradictory) into high quality, fused targeting/intelligence products.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0087	Ability to focus research efforts to meet the customer's decision-making needs.	3.1 - 3.10	3	90% or .9
A0088	Ability to function effectively in a dynamic, fast-paced environment.	3.1 - 3.10	3	90% or .9

NCWF JOB ROLE

Target Network Analyst

Job Role Description: Conducts advanced analysis of collection and open-source data to ensure target continuity; to profile targets and their activities; and develop techniques to gain more target information. Determines how targets communicate, move, operate and live based on knowledge of target technologies, digital networks and the applications on them.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Target Network Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of 1 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.	3.1 - 3.10	3	90% or .9
A0091	Ability to identify intelligence gaps.	1.1	3	90% or .9
A0101	Ability to recognize and mitigate cognitive biases which may affect analysis.	1.1 - 1.15	3	90% or .9
A0102	Ability to recognize and mitigate deception in reporting and analysis.	16.1 - 16.6	3	90% or .9
A0106	Ability to think critically.	1.1 - 1.15	3	90% or .9
A0109	Ability to utilize multiple intelligence sources across all intelligence disciplines.	3.1 - 3.10	3	90% or .9
A0085	Ability to exercise judgment when policies are not well-defined.	1.1 - 1.15	3	90% or .9
A0073	Ability to clearly articulate intelligence requirements into well-formulated research questions and requests for information.	4.3	4	100% or 1
	Summary		**4**	**95% or .95**

NCWF JOB ROLE

Multi-Disciplined Language Analyst

Job Role Description: Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Multi-Disciplined Language Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0650	Determine what technologies are used by a given target.	Coordinate	4.2, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7	4	100% or 1
T0606	Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.	Compile	4.1 - 4.13, 5.1 - 5.6	4	100% or 1
T0715	Identify collection gaps and potential collection strategies against targets.	Identify	4.1 - 4.13	4	100% or 1
T0745	Make recommendations to guide collection in support of customer requirements.	Recommendation	16.5	4	100% or 1
T0761	Provide SME and support to planning/developmental forums and working groups as appropriate.	Provide	3.1 - 3.10	3	90% or .9
T0837	Advise managers and operators on language and cultural issues that impact organization objectives.		N/A		
T0838	Analyze and process information using language and/or cultural expertise.		N/A		
T0839	Assess, document, and apply a target's motivation and/or frame of reference to facilitate analysis, targeting and collection opportunities.	Apply	3.1 - 3.10	3	90% or .9
T0840	Collaborate across internal and/or external organizational lines to enhance collection, analysis and dissemination.	Collaborate	6.1 - 6.9, 7.1 - 7.14	4	100% or 1
T0841	Conduct all-source target research to include the use of open source materials in the target language.	Conduct	4.1 - 4.13	4	100% or 1
T0842	Conduct analysis of target communications to identify essential information in support of organization objectives.	Conduct	6.1 - 6.9	4	100% or 1
T0843	Perform quality review and provide feedback on transcribed or translated materials.	Perform	16.2	3	90% or .9
T0844	Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing.	Evaluate	4.4	4	100% or 1
T0845	Identify cyber threat tactics and methodologies.	Identify	6 - 15	4	100% or 1
T0846	Identify target communications within the global network.	Identify	6.1 - 6.9, 7.1 - 7.14	4	100% or 1

NCWF JOB ROLE

Multi-Disciplined Language Analyst

Job Role Description: Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Multi-Disciplined Language Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0847	Maintain awareness of target communication tools, techniques, and the characteristics of target communication networks (e.g., capacity, functionality, paths, critical nodes) and their potential implications for targeting, collection, and analysis.	Maintain	6.1 - 6.9, 7.1 - 7.14	4	100% or 1
T0848	Provide feedback to collection managers to enhance future collection and analysis.	Provide	16.4, 16.5	4	100% or 1
T0849	Perform foreign language and dialect identification in initial source data.	Perform	4.1 - 4.13	3	90% or .9
T0850	Perform or support technical network analysis and mapping.	Perform	6.1 - 6.9	4	100% or 1
T0851	Provide requirements and feedback to optimize the development of language processing tools.		N/A		
T0852	Perform social network analysis and document as appropriate.	Perform	4.2	4	100% or 1
T0853	Scan, identify and prioritize target graphic (including machine-to-machine communications) and/or voice language material.	Identify	6.2	4	100% or 1
T0854	Tip critical or time-sensitive information to appropriate customers.	Maintain	16.1 - 16.6	3	90% or .9
T0855	Transcribe target voice materials in the target language.		N/A		
T0856	Translate (e.g., verbatim, gists, and/or summaries) target graphic material.		N/A		
T0857	Translate (e.g., verbatim, gists, and/or summaries) target voice material.		N/A		
T0858	Identify foreign language terminology within computer programs (e.g., comments, variable names).		N/A		
T0859	Provide near-real time language analysis support (e.g., live operations).		N/A		
T0860	Identify cyber/technology-related terminology in the target language.		N/A		
	Summary			**4**	**90% or .9**

NCWF JOB ROLE

Multi-Disciplined Language Analyst

Job Role Description: Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Multi-Disciplined Language Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0173	Withdrawn – Integrated into K0499	N/A		
K0348	Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).	N/A		
K0431	Knowledge of evolving/emerging communications technologies.	1.1	3	90% or .9
K0449	Knowledge of how to extract, analyze, and use metadata.	4.1 - 4.13	4	100% or 1
K0413	Knowledge of cyber operation objectives, policies, and legalities.	1.3, 1.5, 1.6, 1.7	4	100% or 1
K0487	Knowledge of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	8.1, 9.1, 10.7	4	100% or 1
K0462	Knowledge of intelligence reporting principles, policies, procedures, and vehicles, including report formats, reportability criteria (requirements and priorities), dissemination practices, and legal authorities and restrictions.	16.1, 16.2, 16.3	4	100% or 1
K0520	Knowledge of principles and practices related to target development such as target knowledge, associations, communication systems, and infrastructure.	4.2, 4.3, 4.4	4	100% or 1
K0550	Knowledge of target, including related current events, communication profile, actors, and history (language, culture) and/or frame of reference.	4.2, 4.3, 4.4	4	100% or 1
K0567	Knowledge of the data flow from collection origin to repositories and tools.	4.5, 4.6, 4.7	4	100% or 1
K0599	Knowledge of the structure, architecture, and design of modern digital and telephony networks.	4.2, 4.8, 4.9	3	90% or .9
K0600	Knowledge of the structure, architecture, and design of modern wireless communications systems.	13.3	4	100% or 1

NCWF JOB ROLE

Multi-Disciplined Language Analyst

Job Role Description: Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Multi-Disciplined Language Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).	N/A		
K0377	Knowledge of classification and control markings standards, policies and procedures.	1.5, 1.6	4	100% or 1
K0434	Knowledge of front-end collection systems, including traffic collection, filtering, and selection.	7.1 - 7.14	4	100% or 1
K0356	Knowledge of analytic tools and techniques.	6.1 - 6.9 to 15	4	100% or 1
K0359	Knowledge of approved intelligence dissemination processes.	4.3	3	80% or .8
K0367	Knowledge of basic cyber operations activity concepts (e.g., foot printing, scanning and enumeration, penetration testing, white/black listing).	1.1 - 1.15, 4.1 - 4.13, 6.1 - 6.9,, 7.1 - 7.14	4	100% or 1
K0391	Knowledge of collection systems, capabilities, and processes.	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
K0396	Knowledge of computer programming concepts, including computer languages, programming, testing, debugging, and file types.	N/A		
K0398	Knowledge of concepts related to websites (e.g., web servers/pages, hosting, DNS, registration, web languages such as HTML).	4.4, 4.5, 4.6, 4.8, 10.1	4	100% or 1
K0407	Knowledge of customer information needs.	3.1	4	100% or 1
K0416	Knowledge of cyber operations.	6.1 - 6.9 to 15	4	100% or 1
K0476	Knowledge of language processing tools and techniques.	6.1 - 6.9 to 15	4	100% or 1
K0488	Knowledge of network security implementations (e.g., host-based IDS, IPS, access control lists), including their function and placement in a network.	9.2	4	100% or 1
K0491	Knowledge of networking and internet communications fundamentals (i.e. devices, device configuration, hardware, software, applications, ports/protocols, addressing, network architecture and infrastructure, routing, operating systems, etc.).	2.1 - 2.6	2	50% or .5
K0493	Knowledge of obfuscation techniques (e.g., TOR/Onion/anonymizers, VPN/VPS, encryption).	8.12, 9.5	2	50% or .5
K0524	Knowledge of relevant laws, regulations, policies.	1.5, 1.6, 1.7	4	100% or 1

NCWF JOB ROLE

Multi-Disciplined Language Analyst

Job Role Description: Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Multi-Disciplined Language Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0532	Knowledge of specialized target language (e.g., acronyms, jargon, technical terminology, codewords).	N/A		
K0539	Knowledge of target communication profiles and their key elements (e.g., target associations, activities, communication infrastructure).	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
K0540	Knowledge of target communication tools and techniques.	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
K0541	Knowledge of target cultural references, dialects, expressions, idioms, and abbreviations.	4.4	3	90% or .9
K0545	Knowledge of target language(s).	N/A		
K0548	Knowledge of target vetting and validation procedures.	4.4	3	90% or .9
K0564	Knowledge of the characteristics of targeted communication networks (e.g., capacity, functionality, paths, critical nodes).	6.1 - 6.9	3	90% or .9
K0571	Knowledge of the feedback cycle in collection processes.	16.5	3	90% or .9
K0574	Knowledge of the impact of language analysis on on-net operator functions.	N/A		
K0579	Knowledge of the organization, roles and responsibilities of higher, lower and adjacent sub-elements.	N/A		
K0596	Knowledge of the request for information process.	3.9	3	90% or .9
K0606	Knowledge of transcript development processes and techniques (e.g., verbatim, gists, summaries).	N/A		
K0607	Knowledge of translation processes and techniques.	N/A		
S0187	Skill in applying various analytical methods, tools, and techniques (e.g., competing hypotheses; chain of reasoning; scenario methods; denial and deception detection; high impact-low probability; network/ association or link analysis; Bayesian, Delphi, and Pattern analyses).	4.1 - 4.13 to 15	4	100% or 1
S0217	Skill in evaluating data sources for relevance, reliability, and objectivity.	4.1 - 4.13	4	100% or 1
S0244	Skill in managing client relationships, including determining client needs/requirements, managing client expectations, and demonstrating commitment to delivering quality results.	3.1 - 3.10	4	100% or 1
S0259	Skill in recognizing denial and deception techniques of the target.	9.4, 10.5, 13.5	3	90% or .9
S0262	Skill in recognizing significant changes in a target's communication patterns.	6.1 - 6.9	4	100% or 1

NCWF JOB ROLE

Multi-Disciplined Language Analyst

Job Role Description: Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Multi-Disciplined Language Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0277	Skill in synthesizing, analyzing, and prioritizing meaning across data sets.	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
S0218	Skill in evaluating information for reliability, validity, and relevance.	1.1 - 1.15	4	100% or 1
S0184	Skill in analyzing traffic to identify network devices.	6.1 - 6.9, 7.1 - 7.14	4	100% or 1
S0290	Skill in using non-attributable networks.	6.1 - 6.9, 7.1 - 7.14	4	100% or 1
S0179	Skill in analyzing language processing tools to provide feedback to enhance tool development.	N/A		
S0188	Skill in assessing a target's frame of reference (e.g., motivation, technical capability, organizational structure, sensitivities).	N/A		
S0193	Skill in complying with the legal restrictions for targeted information.	1.7	4	100% or 1
S0195	Skill in conducting research using all available sources.	4.1 - 4.13	4	100% or 1
S0198	Skill in conducting social network analysis.	4.2	4	100% or 1
S0210	Skill in developing intelligence reports.	4.3	4	100% or 1
S0212	Skill in disseminating items of highest intelligence value in a timely manner.	4.3	4	100% or 1
S0215	Skill in evaluating and interpreting metadata.	4.1 - 4.13	4	100% or 1
S0224	Skill in gisting target communications.	6.1 - 6.9	4	100% or 1
S0226	Skill in identifying a target's network characteristics.	6.1 - 6.9	4	100% or 1
S0232	Skill in identifying intelligence gaps and limitations.	4.3	4	100% or 1
S0233	Skill in identifying language issues that may have an impact on organization objectives.	4.4	3	90% or .9
S0235	Skill in identifying non-target regional languages and dialects	4.4	3	90% or .9
S0241	Skill in interpreting traceroute results, as they apply to network analysis and reconstruction.	4.7	4	100% or 1
S0251	Skill in prioritizing target language material.	4.4	4	100% or 1
S0253	Skill in providing analysis on target-related matters (e.g., language, cultural, communications).	4.4	4	100% or 1

NCWF JOB ROLE

Multi-Disciplined Language Analyst

Job Role Description: Applies language and culture expertise with target/threat and technical knowledge to process, analyze, and/or disseminate intelligence information derived from language, voice and/or graphic material. Creates, and maintains language specific databases and working aids to support cyber action execution and ensure critical knowledge sharing. Provides subject matter expertise in foreign language-intensive or interdisciplinary projects.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Multi-Disciplined Language Analyst. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0265	Skill in recognizing technical information that may be used for target development including intelligence development.	4.1 - 4.13, 6.1 - 6.9	3	90% or .9
S0283	Skill in transcribing target language communications.	6.1 - 6.9	4	100% or 1
S0284	Skill in translating target graphic and/or voice language materials.	6.1 - 6.9	4	100% or 1
A0075	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.	3.1 - 3.10	3	90% or .9
A0071	Ability to apply language and cultural expertise to analysis.	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
A0103	Ability to review processed target language materials for accuracy and completeness.	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
	Summary		**4**	**95% or .95**

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

COLLECT AND OPERATE (CO)

Specialty areas responsible for specialized denial and deception operations and Collection of cybersecurity information that may be used to develop intelligence.

Collection Operations (CL)

Executes collection using appropriate strategies and within the priorities established through the collection management process.

Cyber Operations (OP)

Performs activities to gather evidence on criminal or foreign intelligence entities in order to mitigate possible or real-time threats, protect against espionage or insider threats, foreign sabotage, international terrorist activities, or to support other intelligence activities.

Cyber Operational Planning (PL)

Performs in-depth joint targeting and cyber planning process. Gathers information and develops detailed Operational Plans and Orders supporting requirements. Conducts strategic and operational-level planning across the full range of operations for integrated information and cyberspace operations.

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0562	Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements.	Synchronize	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
T0564	Analyze feedback to determine extent to which collection products and services are meeting requirements.	Analyze	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
T0568	Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirement s (e.g., duration, scope, communication requirements, interagency/international agreements).	Analyze	3.1 - 3.10	3	90% or .9
T0573	Assess and apply operational environment factors and risks to collection management process.	Assess	1.4	3	90% or .9
T0578	Assess performance of collection assets against prescribed specifications.	Assess	4.1 - 4.13	3	90% or .9
T0604	Compare allocated and available assets to collection demand as expressed through requirements.	Compare	3.1	3	90% or .9
T0605	Compile lessons learned from collection management activity's execution of organization collection objectives.	Compile	4.1 - 4.13	3	90% or .9
T0625	Consider efficiency and effectiveness of collection assets and resources if/when applied against priority information requirements.	Consider	4.1 - 4.13	3	90% or .9
T0626	Construct collection plans and matrixes using established guidance and procedures.	Construct	3.8	4	100% or 1
T0631	Coordinate resource allocation of collection assets against prioritized collection requirements with collection discipline leads.	Coordinate	3.8	3	90% or .9
T0632	Coordinate inclusion of collection plan in appropriate documentation.	Coordinate	3.8, 16.4	3	90% or .9
T0634	Re-task or re-direct collection assets and resources.	Retask	16.5	3	90% or .9
T0645	Determine course of action for addressing changes to objectives, guidance, and operational environment.	Determine	16.5	4	100% or 1

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0646	Determine existing collection management webpage databases, libraries and storehouses.	Determine	3.9	4	100% or 1
T0647	Determine how identified factors affect the tasking, collection, processing, exploitation and dissemination architecture's form and function.	Determine	16.5	4	100% or 1
T0649	Determine organizations and/or echelons with collection authority over all accessible collection assets.	Determine	16.5	4	100% or 1
T0651	Develop a method for comparing collection reports to outstanding requirements to identify information gaps.	Develop	16.5	4	100% or 1
T0657	Develop coordinating instructions by collection discipline for each phase of an operation.	Develop	3.8	3	90% or .9
T0662	Allocate collection assets based on leadership's guidance, priorities, and/or operational emphasis.	Allocate	3.6	4	100% or 1
T0674	Disseminate tasking messages and collection plans.	Disseminate	3.6, 3.7	3	90% or .9
T0681	Establish alternative processing, exploitation and dissemination pathways to address identified issues or problems.	Establish	16.4, 16.5	4	100% or 1
T0683	Establish processing, exploitation and dissemination management activity using approved guidance and/or procedures.	Establish	16.5	4	100% or 1
T0698	Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers.	Facilitate	16.5	3	90% or .9
T0702	Formulate collection strategies based on knowledge of available intelligence discipline capabilities and gathering methods that align multi-discipline collection capabilities and accesses with targets and their observables.	Formulate	3.8	3	90% or .9
T0714	Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.	Identify	3.6	2	70% or .7

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0716	Identify coordination requirements and procedures with designated collection authorities.	Identify	3.7	4	100% or 1
T0721	Identify issues or problems that can disrupt and/or degrade processing, exploitation and dissemination architecture effectiveness.	Identify	3.8	3	90% or .9
T0723	Identify potential collection disciplines for application against priority information requirements.	Identify	3.8	3	90% or .9
T0725	Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.	Identify	3.8, 3.9	3	90% or .9
T0734	Issue requests for information.	Check	3.8, 3.9	3	90% or .9
T0737	Link priority collection requirements to optimal assets and resources.	Compare	3.8, 3.9	3	90% or .9
T0750	Monitor completion of reallocated collection efforts.	Monitor	3.8, 3.9	3	90% or .9
T0753	Monitor operational status and effectiveness of the processing, exploitation and dissemination architecture.	Monitor	3.8	3	90% or .9
T0755	Monitor the operational environment for potential factors and risks to the collection operation management process.	Monitor	1.4, 3.8	2	70% or .7
T0757	Optimize mix of collection assets and resources to increase effectiveness and efficiency against essential information associated with priority intelligence requirements.	Optimize	3.8	2	70% or .7
T0773	Prioritize collection requirements for collection platforms based on platform capabilities.	Prioritize	3.8	2	70% or .7
T0779	Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations.	Provide	3.8	2	70% or .7

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0806	Request discipline-specific processing, exploitation, and dissemination information collected using discipline's collection assets and resources in accordance with approved guidance and/or procedures.	Collect	3.10	3	90% or .9
T0809	Review capabilities of allocated collection assets.	Review	3.10	3	90% or .9
T0810	Review intelligence collection guidance for accuracy/applicability.	Review	3.8	3	90% or .9
T0811	Review list of prioritized collection requirements and essential information.	Review	3.7	3	90% or .9
T0812	Review and update overarching collection plan, as required.	Review	3.8	3	90% or .9
T0814	Revise collection matrix based on availability of optimal assets and resources.	Revise	3.10	3	90% or .9
T0820	Specify changes to collection plan and/or operational environment that necessitate re-tasking or re-directing of collection assets and resources.	Specify	3.8, 3.10	4	100% or 1
T0821	Specify discipline-specific collections and/or taskings that must be executed in the near term.	Specify	3.10	4	100% or 1
T0827	Synchronize the integrated employment of all available organic and partner intelligence collection assets using available collaboration capabilities and techniques.	Synchronize	3.8, 3.9, 3.10	4	100% or 1
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0036	Knowledge of human-computer interaction principles.	N/A		
K0058	Knowledge of network traffic analysis methods.	6.2, 6.6, 7.11, 7.12, 9.3, 13.4, 14.2	4	100% or 1
K0431	Knowledge of evolving/emerging communications technologies.	1.1	3	80% or .8
K0449	Knowledge of how to extract, analyze, and use metadata.	4.1 - 4.13	4	100% or 1
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).	2.1 - 2.6	3	80% or .8
K0579	Knowledge of the organization, roles and responsibilities of higher, lower and adjacent sub-elements.	3.5	3	80% or .8
K0596	Knowledge of the request for information process.	3.9	4	100% or 1
K0369	Knowledge of basic malicious activity concepts (e.g., foot printing, scanning and enumeration).	4.1 - 4.13, 06	4	100% or 1
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	4.2, 4.9, 4.11, 6.5, 6.6, 7.11	2	50% or .5
K0471	Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).	2.1 - 2.6	2	50% or .5
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).	7.7	3	90% or .9

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)	N/A		
K0440	Knowledge of host-based security products and how they affect exploitation and vulnerability.	5.5, 7.13, 9.8	4	100% or 1
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.	N/A		
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	2 - 15	3	90% or .9
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.	2 - 15	3	90% or .9
K0427	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).	N/A		
K0446	Knowledge of how modern wireless communications systems impact cyber operations.	13.1	3	90% or .9
K0561	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	8.1 to 8.4	3	90% or .9
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	2.1 - 2.6	4	100% or 1
K0405	Knowledge of current computer-based intrusion sets.	9.2	4	100% or 1
K0480	Knowledge of malware.	7.7	3	90% or .9
K0610	Knowledge of virtualization products (VMware, Virtual PC).	N/A		
K0612	Knowledge of what constitutes a "threat" to a network.	1.2	3	90% or .9
K0353	Knowledge of all possible circumstances that would result in changing collection management authorities.	3.7, 3.10	3	90% or .9
K0361	Knowledge of asset availability, capabilities and limitations.	3.1	4	100% or 1
K0364	Knowledge of available databases and tools necessary to assess appropriate collection tasking.	3.7	4	100% or 1
K0366	Knowledge of basic computer components and architectures, including the functions of various peripherals.	N/A		
K0380	Knowledge of collaborative tools and environments.	1 - 16	4	100% or 1
K0382	Knowledge of collection capabilities and limitations.	3.7, 3.8	3	90% or .9

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0383	Knowledge of collection capabilities, accesses, performance specifications, and constraints utilized to satisfy collection plan.	3.7, 3.8	3	90% or .9
K0386	Knowledge of collection management tools.	3.7	4	100% or 1
K0387	Knowledge of collection planning process and collection plan.	3.8	4	100% or 1
K0390	Knowledge of collection strategies.	3.8	4	100% or 1
K0401	Knowledge of criteria for evaluating collection products.	3.7, 3.8	4	100% or 1
K0404	Knowledge of current collection requirements.	3.7	4	100% or 1
K0412	Knowledge of cyber lexicon/terminology	1.1 - 1.15	3	90% or .9
K0419	Knowledge of database administration and maintenance.	N/A		
K0425	Knowledge of different organization objectives at all levels, including subordinate, lateral and higher.	3.1 - 3.10	4	100% or 1
K0435	Knowledge of fundamental cyber concepts, principles, limitations, and effects.	1.3	2	70% or .7
K0448	Knowledge of how to establish priorities for resources.	3.8, 3.10	4	100% or 1
K0453	Knowledge of indications and warning.	1 - 16	4	100% or 1
K0454	Knowledge of information needs.	3.1	4	100% or 1
K0467	Knowledge of internal and external partner organization capabilities and limitations (those with tasking, collection, processing, exploitation and dissemination responsibilities).	3.7	4	100% or 1
K0474	Knowledge of key cyber threat actors and their equities.	1.1, 1.2	3	90% or .9
K0475	Knowledge of key factors of the operational environment and threat.	1.1, 1.2	3	90% or .9
K0477	Knowledge of leadership's Intent and objectives.	3.8, 3.10	3	90% or .9
K0482	Knowledge of methods for ascertaining collection asset posture and availability.	3.8, 3.10	3	90% or .9
K0492	Knowledge of non-traditional collection methodologies.	4.1 - 4.13	4	100% or 1
K0495	Knowledge of ongoing and future operations.	3.8	4	100% or 1

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0496	Knowledge of operational asset constraints.	3.10	4	100% or 1
K0498	Knowledge of operational planning processes.	3.8	3	90% or .9
K0503	Knowledge of organization formats of resource and asset readiness reporting, its operational relevance and intelligence collection impact.	3.7, 3.10	4	100% or 1
K0505	Knowledge of organization objectives and associated demand on collection management.	3.1	4	100% or 1
K0513	Knowledge of organizational priorities, legal authorities and requirements submission processes.	3.2, 3.7	4	100% or 1
K0521	Knowledge of priority information, how it is derived, where it is published, how to access, etc.	3.2	4	100% or 1
K0522	Knowledge of production exploitation and dissemination needs and architectures.	3.7, 3.10	4	100% or 1
K0526	Knowledge of research strategies and knowledge management.	3.10	3	90% or .9
K0527	Knowledge of risk management and mitigation strategies.	1.4	3	90% or .9
K0552	Knowledge of tasking mechanisms.	3.8, 3.10	4	100% or 1
K0553	Knowledge of tasking processes for organic and subordinate collection assets.	3.8, 3.10	4	100% or 1
K0554	Knowledge of tasking, collection, processing, exploitation and dissemination.	3.8, 3.10	4	100% or 1
K0558	Knowledge of the available tools and applications associated with collection requirements and collection management.	3.7	4	100% or 1
K0562	Knowledge of the capabilities and limitations of new and emerging collection capabilities, accesses and/or processes.	3.8	3	90% or .9
K0563	Knowledge of the capabilities, limitations and tasking methodologies of internal and external collections as they apply to planned cyber activities.	3.8	3	90% or .9
K0569	Knowledge of the existent tasking, collection, processing, exploitation and dissemination architecture.	3.7	3	90% or .9
K0570	Knowledge of the factors of threat that could impact collection operations.	1.2	3	90% or .9
K0580	Knowledge of the organization's established format for collection plan.	3.7	4	100% or 1
K0581	Knowledge of the organization's planning, operations and targeting cycles.	3.1, 3.7	4	100% or 1

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0583	Knowledge of the organizational plans/directives/guidance that describe objectives.	3.1, 3.7	4	100% or 1
K0584	Knowledge of the organizational policies/procedures for temporary transfer of collection authority.	3.1, 3.2, 3.4	4	100% or 1
K0587	Knowledge of the POC's, databases, tools and applications necessary to establish environment preparation and surveillance products.	3.7	4	100% or 1
K0588	Knowledge of the priority information requirements from subordinate, lateral and higher levels of the organization.	3.7, 3.9	4	100% or 1
K0601	Knowledge of the systems/architecture/communications used for coordination.	3.7	3	90% or .9
K0605	Knowledge of tipping, cueing, mixing, and redundancy.	N/A		
K0613	Knowledge of who the organization's operational planners are, how and where they can be contacted, and what are their expectations.	3.7	3	90% or .9
S0238	Skill in information prioritization as it relates to operations.	3.1 - 3.10	4	100% or 1
S0304	Skill to access information on current assets available, usage.	3.7, 3.8	4	100% or 1
S0305	Skill to access the databases where plans/directives/guidance are maintained.	3.7	4	100% or 1
S0311	Skill to apply the capabilities, limitations and tasking methodologies of available platforms, sensors, architectures and apparatus as they apply to organization objectives.	3.1 - 3.10	4	100% or 1
S0313	Skill to articulate a needs statement/requirement and integrate new and emerging collection capabilities, accesses and/or processes into collection operations.	3.7, 3.8	4	100% or 1
S0316	Skill to associate Intelligence gaps to priority information requirements and observables.	3.7, 3.8	4	100% or 1
S0317	Skill to compare and contrast indicators/observables with requirements.	3.2	3	90% or .9
S0324	Skill to determine feasibility of collection.	3.8	3	90% or .9
S0325	Skill to develop a collection plan that clearly shows the discipline that can be used to collect the information needed.	3.8	3	90% or .9
S0327	Skill to ensure that the collection strategy leverages all available resources.	3.8, 3.10	3	90% or .9

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0328	Skill to evaluate factors of the operational environment to objectives, and information requirements.	3.7, 3.8	3	90% or .9
S0330	Skill to evaluate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.	3.7, 3.8	4	100% or 1
S0332	Skill to extract information from available tools and applications associated with collection requirements and collection operations management.	4 - 15	4	100% or 1
S0334	Skill to identify and apply tasking, collection, processing, exploitation and dissemination to associated collection disciplines.	4 - 15	4	100% or 1
S0335	Skill to identify Intelligence gaps.	3.7, 3.8	3	90% or .9
S0336	Skill to identify when priority information requirements are satisfied.	3.7, 3.8	3	90% or .9
S0339	Skill to interpret readiness reporting, its operational relevance and intelligence collection impact.	16.4, 16.5	3	90% or .9
S0342	Skill to optimize collection system performance through repeated adjustment, testing, and re-adjustment.	3.7, 3.8	3	90% or .9
S0344	Skill to prepare and deliver reports, presentations and briefings, to include using visual aids or presentation technology.	16.1 - 16.6	4	100% or 1
S0347	Skill to review performance specifications and historical information about collection assets.	16.4, 16.5	3	90% or .9
S0351	Skill to translate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.	3.7, 3.8	4	100% or 1
S0352	Skill to use collaborative tools and environments.	4 - 15	4	100% or 1
A0069	Ability to apply collaborative skills and strategies.	3.1 - 3.10	4	100% or 1
A0070	Ability to apply critical reading/thinking skills.	4 - 15	4	100% or 1
A0076	Ability to coordinate and collaborate with analysts regarding surveillance requirements and essential information development.	3.1 - 3.10	4	100% or 1
A0078	Ability to coordinate, collaborate and disseminate information to subordinate, lateral and higher-level organizations.	3.1 - 3.10	4	100% or 1

NCWF JOB ROLE

All Source-Collection Manager

Job Role Description: Identifies collection authorities and environment; incorporates priority information requirements into collection management; develops concepts to meet leadership's intent. Determines capabilities of available collection assets, identifies new collection capabilities; and constructs and disseminates collection plans. Monitors execution of tasked collection to ensure effective execution of the collection plan.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
A0079	Ability to correctly employ each organization or element into the collection plan and matrix.	3.1 - 3.10	4	100% or 1
	Summary		**4**	**95% or .95**

NCWF JOB ROLE

All Source-Collection Requirements Manager

Job Role Description: Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Requirements Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0564	Analyze feedback to determine extent to which collection products and services are meeting requirements.	Analyze	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
T0568	Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirement s (e.g., duration, scope, communication requirements, interagency/international agreements).	Analyze	3.1 - 3.10	3	90% or .9
T0578	Assess performance of collection assets against prescribed specifications.	Assess	4.1 - 4.13	3	90% or .9
T0605	Compile lessons learned from collection management activity's execution of organization collection objectives.	Compile	4.1 - 4.13	3	90% or .9
T0651	Develop a method for comparing collection reports to outstanding requirements to identify information gaps.	Develop	16.5	4	100% or 1
T0714	Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.	Identify	3.6	2	70% or .7
T0725	Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.	Identify	3.8, 3.9	3	90% or .9
T0734	Issue requests for information.	Check	3.8, 3.9	3	90% or .9
T0809	Review capabilities of allocated collection assets.	Review	3.1	3	90% or .9
T0810	Review intelligence collection guidance for accuracy/applicability.	Review	3.8	3	90% or .9
T0811	Review list of prioritized collection requirements and essential information.	Review	3.7	3	90% or .9
T0565	Analyze incoming collection requests.	Analyze	3.1, 3.2	4	100% or 1
T0577	Assess efficiency of existing information exchange and management systems.	Assess	3.8	3	90% or .9
T0580	Assess the effectiveness of collections in satisfying priority information gaps, using available capabilities and methods, and then adjust collection strategies and collection requirements accordingly.	Assess	3.7, 3.8	3	90% or .9
T0596	Close requests for information once satisfied.	Check	3.8	3	90% or .9

NCWF JOB ROLE

All Source-Collection Requirements Manager

Job Role Description: Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Requirements Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0602	Collaborates with customer to define information requirements.	Collaborate	3.1 - 3.7	4	100% or 1
T0613	Conduct formal and informal coordination of collection requirements in accordance with established guidelines and procedures.	Conduct	3.7, 3.8, 3.9	4	100% or 1
T0668	Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centers.	Develop	3.7	3	90% or .9
T0673	Disseminate reports to inform decision makers on collection issues.	Desseminate	3.7	3	90% or .9
T0675	Conduct and document an assessment of the collection results using established procedures.	Conduct	16.1 - 16.6	4	100% or 1
T0682	Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership.	Validate	16.4, 16.5	4	100% or 1
T0689	Evaluate extent to which collected information and/or produced intelligence satisfy information requests.	Evaluate	16.4, 16.5	4	100% or 1
T0693	Evaluate extent to which collection operations are synchronized with operational requirements.	Evaluate	16.4, 16.5	4	100% or 1
T0694	Evaluate the effectiveness of collection operations against the collection plan.	Evaluate	16.4, 16.5	4	100% or 1
T0730	Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures.	Inform	16.1 - 16.6	3	90% or .9
T0746	Modify collection requirements as necessary.	Modify	3.8	3	90% or .9
T0780	Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans.	Provide	3.8	3	90% or .9
T0819	Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements.	Manage	3.7	3	90% or .9

NCWF JOB ROLE

All Source-Collection Requirements Manager

Job Role Description: Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Requirements Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0822	Submit information requests to collection requirement management section for processing as collection requests.	Deliver	3.7	3	90% or .9
T0830	Track status of information requests, including those processed as collection requests and production requirements, using established procedures.	Check	3.8	3	90% or .9
T0831	Translate collection requests into applicable discipline-specific collection requirements.	Translate	16.3	4	100% or 1
T0832	Use feedback results (e.g., lesson learned) to identify opportunities to improve collection management efficiency and effectiveness.	Identify	16.1 - 16.6	3	90% or .9
T0833	Validate requests for information according to established criteria.	Validate	16.4	4	100% or 1
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

All Source-Collection Requirements Manager

Job Role Description: Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Requirements Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0036	Knowledge of human-computer interaction principles.	N/A		
K0058	Knowledge of network traffic analysis methods.	6.2, 6.6, 7.11, 7.12, 9.3, 13.4, 14.2	4	100% or 1
K0431	Knowledge of evolving/emerging communications technologies.	1.1	3	80% or .8
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).	2.1 - 2.6	3	80% or .8
K0579	Knowledge of the organization, roles and responsibilities of higher, lower and adjacent sub-elements.	3.5	3	80% or .8
K0596	Knowledge of the request for information process.	3.9	4	100% or 1
K0369	Knowledge of basic malicious activity concepts (e.g., foot printing, scanning and enumeration).	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	4.2, 4.9, 4.11, 6.5, 6.6, 7.11	2	50% or .5
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)	N/A		
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.	N/A		
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	N/A		
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.	N/A		

NCWF JOB ROLE

All Source-Collection Requirements Manager

Job Role Description: Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Requirements Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0427	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).	N/A		
K0446	Knowledge of how modern wireless communications systems impact cyber operations.	13.1	3	90% or .9
K0561	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	8.1 - 8.4	3	90% or .9
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	2.1 - 2.6	4	100% or 1
K0480	Knowledge of malware.	7.7	3	90% or .9
K0610	Knowledge of virtualization products (VMware, Virtual PC).	N/A		
K0612	Knowledge of what constitutes a "threat" to a network.	1.2	3	90% or .9
K0353	Knowledge of all possible circumstances that would result in changing collection management authorities.	3.7, 3.10	3	90% or .9
K0361	Knowledge of asset availability, capabilities and limitations.	3.1	4	100% or 1
K0364	Knowledge of available databases and tools necessary to assess appropriate collection tasking.	3.7	4	100% or 1
K0366	Knowledge of basic computer components and architectures, including the functions of various peripherals.	N/A		
K0380	Knowledge of collaborative tools and environments.	1 - 16	4	100% or 1
K0382	Knowledge of collection capabilities and limitations.	3.7, 3.8	3	90% or .9
K0383	Knowledge of collection capabilities, accesses, performance specifications, and constraints utilized to satisfy collection plan.	3.7, 3.8	3	90% or .9
K0384	Knowledge of collection management functionality (e.g., positions, functions, responsibilities, products, reporting requirements).	3.1 - 3.10	3	90% or .9
K0386	Knowledge of collection management tools.	3.7	4	100% or 1
K0387	Knowledge of collection planning process and collection plan.	3.8	4	100% or 1
K0390	Knowledge of collection strategies.	3.8	4	100% or 1
K0401	Knowledge of criteria for evaluating collection products.	3.7, 3.8	4	100% or 1

NCWF JOB ROLE

All Source-Collection Requirements Manager

Job Role Description: Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Requirements Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0404	Knowledge of current collection requirements.	3.7	4	100% or 1
K0412	Knowledge of cyber lexicon/terminology	1.1 - 1.15	3	90% or .9
K0419	Knowledge of database administration and maintenance.	N/A		
K0421	Knowledge of databases, portals and associated dissemination vehicles.	N/A		
K0425	Knowledge of different organization objectives at all levels, including subordinate, lateral and higher.	3.1 - 3.10	4	100% or 1
K0435	Knowledge of fundamental cyber concepts, principles, limitations, and effects.	1.3	2	70% or .7
K0448	Knowledge of how to establish priorities for resources.	3.8, 3.10	4	100% or 1
K0453	Knowledge of indications and warning.	1 - 16	4	100% or 1
K0454	Knowledge of information needs.	3.1	4	100% or 1
K0467	Knowledge of internal and external partner organization capabilities and limitations (those with tasking, collection, processing, exploitation and dissemination responsibilities).	3.7	4	100% or 1
K0474	Knowledge of key cyber threat actors and their equities.	1.1, 1.2	3	90% or .9
K0475	Knowledge of key factors of the operational environment and threat.	1.1, 1.2	3	90% or .9
K0477	Knowledge of leadership's Intent and objectives.	3.8, 3.10	3	90% or .9
K0482	Knowledge of methods for ascertaining collection asset posture and availability.	3.8, 3.10	3	90% or .9
K0492	Knowledge of non-traditional collection methodologies.	4.1 - 4.13	4	100% or 1
K0495	Knowledge of ongoing and future operations.	3.8	4	100% or 1
K0496	Knowledge of operational asset constraints.	3.1	4	100% or 1
K0498	Knowledge of operational planning processes.	3.8	3	90% or .9
K0505	Knowledge of organization objectives and associated demand on collection management.	3.1	4	100% or 1
K0513	Knowledge of organizational priorities, legal authorities and requirements submission processes.	3.2, 3.7	4	100% or 1
K0521	Knowledge of priority information, how it is derived, where it is published, how to access, etc.	3.2	4	100% or 1

NCWF JOB ROLE

All Source-Collection Requirements Manager

Job Role Description: Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Requirements Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0526	Knowledge of research strategies and knowledge management.	3.1	3	90% or .9
K0527	Knowledge of risk management and mitigation strategies.	1.4	3	90% or .9
K0552	Knowledge of tasking mechanisms.	3.8, 3.10	4	100% or 1
K0554	Knowledge of tasking, collection, processing, exploitation and dissemination.	3.8, 3.10	4	100% or 1
K0558	Knowledge of the available tools and applications associated with collection requirements and collection management.	3.7	4	100% or 1
K0562	Knowledge of the capabilities and limitations of new and emerging collection capabilities, accesses and/or processes.	3.8	3	90% or .9
K0563	Knowledge of the capabilities, limitations and tasking methodologies of internal and external collections as they apply to planned cyber activities.	3.8	3	90% or .9
K0568	Knowledge of the definition of collection management and collection management authority.	N/A		
K0569	Knowledge of the existent tasking, collection, processing, exploitation and dissemination architecture.	3.7	3	90% or .9
K0570	Knowledge of the factors of threat that could impact collection operations.	1.2	3	90% or .9
K0580	Knowledge of the organization's established format for collection plan.	3.7	4	100% or 1
K0581	Knowledge of the organization's planning, operations and targeting cycles.	3.1, 3.7	4	100% or 1
K0584	Knowledge of the organizational policies/procedures for temporary transfer of collection authority.	3.1, 3.2, 3.4	4	100% or 1
K0587	Knowledge of the POC's, databases, tools and applications necessary to establish environment preparation and surveillance products.	3.7	4	100% or 1
K0588	Knowledge of the priority information requirements from subordinate, lateral and higher levels of the organization.	3.7, 3.9	4	100% or 1
K0605	Knowledge of tipping, cueing, mixing, and redundancy.	N/A		
S0304	Skill to access information on current assets available, usage.	3.7, 3.8	4	100% or 1
S0305	Skill to access the databases where plans/directives/guidance are maintained.	3.7	4	100% or 1

NCWF JOB ROLE

All Source-Collection Requirements Manager

Job Role Description: Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Requirements Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0316	Skill to associate Intelligence gaps to priority information requirements and observables.	3.7, 3.8	4	100% or 1
S0317	Skill to compare and contrast indicators/observables with requirements.	3.2	3	90% or .9
S0327	Skill to ensure that the collection strategy leverages all available resources.	3.8, 3.10	3	90% or .9
S0330	Skill to evaluate the capabilities, limitations and tasking methodologies of organic, theater, national, coalition and other collection capabilities.	3.7, 3.8	4	100% or 1
S0334	Skill to identify and apply tasking, collection, processing, exploitation and dissemination to associated collection disciplines.	4 - 15	4	100% or 1
S0335	Skill to identify Intelligence gaps.	3.7, 3.8	3	90% or .9
S0336	Skill to identify when priority information requirements are satisfied.	3.7, 3.8	3	90% or .9
S0339	Skill to interpret readiness reporting, its operational relevance and intelligence collection impact.	16.4, 16.5	3	90% or .9
S0344	Skill to prepare and deliver reports, presentations and briefings, to include using visual aids or presentation technology.	16.1 - 16.6	4	100% or 1
S0347	Skill to review performance specifications and historical information about collection assets.	16.4, 16.5	3	90% or .9
S0352	Skill to use collaborative tools and environments.	4 - 15	4	100% or 1
S0329	Skill to evaluate requests for information to determine if response information exists.	4 - 15	4	100% or 1
S0337	Skill to implement established procedures for evaluating collection management and operations activities.	3.8	4	100% or 1
S0346	Skill to resolve conflicting collection requirements.	4 - 15	4	100% or 1
S0348	Skill to specify collections and/or taskings that must be conducted in the near term.	4 - 15	4	100% or 1
S0353	Skill to use systems and/or tools to track collection requirements and determine whether or not they are satisfied.	4 - 15	4	100% or 1
A0069	Ability to apply collaborative skills and strategies.	3.1 - 3.10	4	100% or 1
A0070	Ability to apply critical reading/thinking skills.	4 - 15	4	100% or 1

NCWF JOB ROLE

All Source-Collection Requirements Manager

Job Role Description: Evaluates collection operations and develops effects-based collection requirements strategies using available sources and methods to improve collection. Develops, processes, validates, and coordinates submission of collection requirements. Evaluates performance of collection assets and collection operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by an All Source-Collection Requirements Manager. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .95 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
A0078	Ability to coordinate, collaborate and disseminate information to subordinate, lateral and higher-level organizations.	3.1 - 3.10	4	100% or 1
	Summary		**4**	**95% or .95**

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0734	Issue requests for information.	Check	3.8, 3.9	3	90% or .9
T0563	Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.	Provide	3.8	3	90% or .9
T0575	Coordinate for intelligence support to operational planning activities.	Coordinate	3.8	3	90% or .9
T0576	Assess all-source intelligence and recommend targets to support cyber operation objectives.	Assess	3.1 - 3.10, 4.1 - 4.13	3	90% or .9
T0579	Assess target vulnerabilities and/or operational capabilities to determine course of action.	Assess	5.1 - 5.6	4	100% or 1
T0581	Assist and advise inter-agency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.	Assist	16.5	3	90% or .9
T0587	Assist in the development and refinement of priority information requirements.	Assist	3.7, 3.8	3	90% or .9
T0590	Enable synchronization of intelligence support plans across partner organizations as required.	Check	3.7	3	90% or .9
T0592	Provide input to the identification of cyber-related success criteria.		N/A		
T0601	Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).		N/A		
T0627	Contribute to crisis action planning for cyber operations.	Contribute	3.8	3	90% or .9
T0628	Contribute to the development of the organization's decision support tools if necessary.	Contribute	3.7	3	90% or .9
T0630	Incorporate intelligence equities into the overall design of cyber operations plans.	Incorporate	3.1 - 3.10	4	100% or 1
T0636	Coordinate with intelligence planners to ensure collection managers receive information requirements.	Coordinate	3.7	3	90% or .9
T0637	Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks.	Coordinate	3.10	3	90% or .9

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0638	Coordinate, produce and track intelligence requirements.	Coordinate	3.1 - 3.10	4	100% or 1
T0639	Coordinate, synchronize and draft applicable intelligence sections of cyber operations plans.	Coordinate	3.7, 3.8	4	100% or 1
T0640	Uses intelligence estimates to counter potential target actions.	Counter	3.2	4	100% or 1
T0648	Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives.	Determine	3.3, 3.4	3	90% or .9
T0656	Develop and review intelligence guidance for integration into supporting cyber operations planning and execution.	Develop	3.8	3	90% or .9
T0659	Develop detailed intelligence support to cyber operations requirements.	Develop	3.1 - 3.10	3	90% or .9
T0667	Develop potential courses of action.	Develop	3.8	3	90% or .9
T0670	Develop, implement, and recommend changes to appropriate planning procedures and policies.	Develop	3.8	3	90% or .9
T0676	Draft cyber intelligence collection and production requirements.	Draft	3.7	4	100% or 1
T0680	Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.	Check	3.8	4	100% or 1
T0690	Evaluate intelligence estimates to support the planning cycle.	Evaluate	3.8	2	70% or .7
T0691	Evaluate the conditions that affect employment of available cyber intelligence capabilities.	Evaluate	3.1	4	100% or 1
T0705	Incorporate intelligence and counterintelligence to support plan development.	Incorporate	3.8, 3.9	3	90% or .9
T0709	Identify all available partner intelligence capabilities and limitations supporting cyber operations.	Identify	3.4, 3.7	3	90% or .9
T0711	Identify, draft, evaluate, and prioritize relevant intelligence or information requirements.	Identify	3.4, 3.7	3	90% or .9

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0719	Identify cyber intelligence gaps and shortfalls.	Identify	3.4, 3.7	3	90% or .9
T0726	Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production.	Identify	3.7	4	100% or 1
T0728	Provide input to or develop courses of action based on threat factors.	Provide	5.1 - 5.6	3	90% or .9
T0733	Interpret environment preparations assessments to determine a course of action.	Interprote	5.1 - 5.6	3	90% or .9
T0735	Lead and coordinate intelligence support to operational planning.	Coordinate	3.1	4	100% or 1
T0739	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Maintain	3.9	3	90% or .9
T0743	Maintain situational awareness to determine if changes to the operating environment require review of the plan.		N/A		
T0760	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	Provide	3.8, 3.10	3	90% or .9
T0763	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Conduct	3.1 - 3.10	3	90% or .9
T0772	Prepare for and provide subject matter expertise to exercises.	Prepare	1 - 16	3	70% or .7
T0784	Provide cyber focused guidance and advice on intelligence support plan inputs.	Provide	3.8	3	90% or .9
T0801	Recommend refinement, adaption, termination, and execution of operational plans as appropriate.	Recommend	3.8	3	90% or .9
T0808	Review and comprehend organizational leadership objectives and guidance for planning.	Review	3.1 - 3.10	3	90% or .9
T0816	Scope the cyber intelligence planning effort.	Scope	3.7	4	100% or 1
T0836	Document lessons learned that convey the results of events and/or exercises.	Document	16.4	4	100% or 1
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0036	Knowledge of human-computer interaction principles.	N/A		
K0173	Withdrawn – Integrated into K0499	N/A		
K0431	Knowledge of evolving/emerging communications technologies.	1.1	3	80% or .8
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).	N/A		
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	4.2, 4.9, 4.11, 6.5, 6.6, 7.11	2	50% or .5
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)	N/A		
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.	N/A		
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.	N/A		
K0427	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).	N/A		
K0446	Knowledge of how modern wireless communications systems impact cyber operations.	13.1	3	90% or .9
K0561	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	8.1 - 8.4	3	90% or .9
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	2.1 - 2.6	4	100% or 1

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0480	Knowledge of malware.	7.7	3	90% or .9
K0610	Knowledge of virtualization products (VMware, Virtual PC).	N/A		
K0612	Knowledge of what constitutes a "threat" to a network.	1.2	3	90% or .9
K0435	Knowledge of fundamental cyber concepts, principles, limitations, and effects.	1.3	2	70% or .7
K0471	Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).	2.1 - 2.6	2	50% or .5
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).	7.7	3	90% or .9
K0440	Knowledge of host-based security products and how they affect exploitation and vulnerability.	5.5, 7.13, 9.8	4	100% or 1
K0405	Knowledge of current computer-based intrusion sets.	9.2	3	90% or .9
K0348	Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).	N/A		
K0377	Knowledge of classification and control markings standards, policies and procedures.	N/A		
K0349	Knowledge of a wide range of concepts associated with websites (e.g., website types, administration, functions, software systems, etc.).	4.2, 4.8, 10.3, 11.5	4	100% or 1
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	1.10, 6.6, 7.6, 8.12, 9.4, 10.4, 10.5, 10.6, 10.7, 10.8, 10.10, 10.11, 10.12, 11.5, 12.3, 12.5, 13.5, 13.6, 13.8, 13.9, 14.3	4	100% or 1
K0370	Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	N/A		
K0436	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber attack, cyber defense), principles, capabilities, limitations, and effects.	1.1 - 1.15	4	100% or 1

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0379	Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.	4.1 - 4.13	4	100% or 1
K0403	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.	N/A		
K0460	Knowledge of intelligence preparation of the environment and similar processes.	4.3	3	70% or .7
K0464	Knowledge of intelligence support to planning, execution, and assessment.	4.1 - 4.13	3	70% or .7
K0556	Knowledge of telecommunications fundamentals.	N/A		
K0603	Knowledge of the ways in which targets or threats use the Internet.	1 - 16	4	100% or 1
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.	13.1 - 13.9	4	90% or .9
K0465	Knowledge of internal and external partner cyber operations capabilities and tools.	1 - 16	4	100% or 1
K0507	Knowledge of organization or partner exploitation of digital networks.	1 - 16	4	100% or 1
K0598	Knowledge of the structure and intent of organization specific plans, guidance and authorizations.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
K0511	Knowledge of organizational hierarchy and cyber decision making processes.	4.1 - 4.13	1	50% or .5
K0414	Knowledge of cyber operations support or enabling processes.	1.1 - 1.15	3	90% or .9
K0577	Knowledge of the intelligence frameworks, processes, and related systems.	4.1 - 4.13	3	50% or .5
K0347	Knowledge and understanding of operational design	N/A		
K0350	Knowledge of accepted organization planning systems.	3.7	4	100% or 1
K0352	Knowledge of all forms of intelligence support needs, topics, and focus areas.	1.1 - 1.15, 3.1 - 3.10	3	90% or .9
K0355	Knowledge of all-source reporting and dissemination procedures.	3.1 - 3.10, 16.1 - 16.6	3	90% or .9
K0358	Knowledge of analytical standards and the purpose of intelligence confidence levels.	1.6	3	90% or .9
K0374	Knowledge of basic structure, architecture, and design of modern digital and telephony networks.	N/A		
K0378	Knowledge of classification and control markings standards.	1.6	3	90% or .9
K0399	Knowledge of crisis action planning and time sensitive planning procedures.	3.8	3	90% or .9

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0400	Knowledge of crisis action planning for cyber operations.	3.8	3	90% or .9
K0408	Knowledge of cyber actions (i.e. cyber defense, information gathering, environment preparation, cyber attack) principles, capabilities, limitations, and effects.	1 - 16	4	100% or 1
K0411	Knowledge of cyber laws, legal considerations and their effect on cyber planning.	1.7	4	100% or 1
K0422	Knowledge of deconfliction processes and procedures.	1.12, 1.13	3	90% or .9
K0432	Knowledge of existing, emerging, and long-range issues related to cyber operations strategy, policy, and organization.	1.12	3	90% or .9
K0441	Knowledge of how collection requirements and information needs are translated, tracked, and prioritized across the extended enterprise.	1.12	3	90% or .9
K0455	Knowledge of information security concepts, facilitating technologies and methods.	1.3	3	90% or .9
K0456	Knowledge of intelligence capabilities and limitations.	N/A		
K0459	Knowledge of intelligence employment requirements (i.e., logistical, communications support, maneuverability, legal restrictions, etc.).	3.10	3	90% or .9
K0463	Knowledge of intelligence requirements tasking systems.	3.7	3	90% or .9
K0494	Knowledge of objectives, situation, operational environment, and the status and disposition of internal and external partner collection capabilities available to support planning.	3.1 - 3.10	3	90% or .9
K0501	Knowledge of organization cyber operations programs, strategies, and resources.	3.7	3	90% or .9
K0502	Knowledge of organization decision support tools and/or methods.	3.7	3	90% or .9
K0504	Knowledge of organization issues, objectives, and operations in cyber as well as regulations and policy directives governing cyber operations.	1.5, 1.6, 1.7, 3.1	3	90% or .9
K0506	Knowledge of organization objectives, leadership priorities, and decision-making risks.	3.1 - 3.10	3	90% or .9
K0508	Knowledge of organization policies and planning concepts for partnering with internal and/or external organizations.	3.2, 3.3, 3.4	3	90% or .9

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0512	Knowledge of organizational planning concepts.	3.8	3	90% or .9
K0514	Knowledge of organizational structures and associated intelligence capabilities.	3.1, 3.7	3	90% or .9
K0517	Knowledge of PIR approval process.	3.1	4	100% or 1
K0518	Knowledge of planning activity initiation.	3.8	4	100% or 1
K0519	Knowledge of planning timelines adaptive, crisis action, and time-sensitive planning.	3.8	4	100% or 1
K0525	Knowledge of required intelligence planning products associated with cyber operational planning.	3.7, 3.8	4	100% or 1
K0538	Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities	3.1, 3.7	4	100% or 1
K0566	Knowledge of the critical information requirements and how they're used in planning.	3.7, 3.10	3	90% or .9
K0572	Knowledge of the functions and capabilities of internal teams that emulate threat activities to benefit the organization.	3.5	3	90% or .9
K0575	Knowledge of the impacts of internal and external partner staffing estimates.	3.2	3	90% or .9
K0578	Knowledge of the intelligence requirements development and request for information processes.	3.4, 3.6, 3.7	4	100% or 1
K0582	Knowledge of the organizational planning and staffing process.	3.7, 3.10	3	90% or .9
K0585	Knowledge of the organizational structure as it pertains to full spectrum cyber operations, including the functions, responsibilities, and interrelationships among distinct internal elements.	3.1 - 3.10	3	90% or .9
K0586	Knowledge of the outputs of course of action and exercise analysis.	16.4	3	90% or .9
K0589	Knowledge of the process used to assess the performance and impact of operations.	3.8	3	90% or .9
K0590	Knowledge of the processes to synchronize operational assessment procedures with the critical information requirement process.	4 - 15	3	90% or .9
K0591	Knowledge of the production responsibilities and organic analysis and production capabilities.	N/A		
K0593	Knowledge of the range of cyber operations and their underlying intelligence support needs, topics, and focus areas.	N/A		
K0594	Knowledge of the relationships between end states, objectives, effects, lines of operation, etc.	16.4	3	90% or .9

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0595	Knowledge of the relationships of operational objectives, intelligence requirements, and intelligence production tasks.	16.4	3	90% or .9
K0602	Knowledge of the various collection disciplines and capabilities.	4 - 15	3	90% or .9
S0218	Skill in evaluating information for reliability, validity, and relevance.	1.1 - 1.15	4	100% or 1
S0203	Skill in defining and characterizing all pertinent aspects of the operational environment.	3.1 - 3.10	4	100% or 1
S0249	Skill in preparing and presenting briefings.	1 - 16	4	100% or 1
S0278	Skill in tailoring analysis to the necessary levels (e.g., classification and organizational).	5.1 - 5.6	3	90% or .9
S0296	Skill in utilizing feedback in order to improve processes, products, and services.	N/A		
S0297	Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).	N/A		
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	3.1 - 3.10	4	100% or 1
S0185	Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.	3.1 - 3.10	4	100% or 1
S0186	Skill in applying crisis planning procedures.	3.8	4	100% or 1
S0213	Skill in documenting and communicating complex technical and programmatic information.	16.4	4	100% or 1
S0250	Skill in preparing plans and related correspondence.	3.8, 3.9, 3.10	4	100% or 1
S0272	Skill in reviewing and editing intelligence products from various sources for cyber operations.	4.3, 4.4	4	100% or 1
S0273	Skill in reviewing and editing plans.	3.8	4	100% or 1
S0306	Skill to analyze strategic guidance for issues requiring clarification and/or additional guidance.	3.8, 3.9	3	90% or .9
S0307	Skill to analyze target or threat sources of strength and morale.	4.1 - 4.13	3	90% or .9
S0308	Skill to anticipate intelligence capability employment requirements.	3.5, 3.10	4	100% or 1
S0309	Skill to anticipate key target or threat activities which are likely to prompt a leadership decision.	5 - 15	4	100% or 1

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0310	Skill to apply analytical standards to evaluate intelligence products.	4.3, 4.4	3	90% or .9
S0312	Skill to apply the process used to assess the performance and impact of cyber operations.	3.8	3	90% or .9
S0314	Skill to articulate intelligence capabilities available to support execution of the plan.	3.8, 3.9	3	90% or .9
S0315	Skill to articulate the needs of joint planners to all-source analysts.	3.1 - 3.10, 4.1 - 4.13	3	90% or .9
S0318	Skill to conceptualize the entirety of the intelligence process in the multiple domains and dimensions.	4.1 - 4.13	4	100% or 1
S0319	Skill to convert intelligence requirements into intelligence production tasks.	4 - 15	4	100% or 1
S0320	Skill to coordinate the development of tailored intelligence products.	4.1 - 4.13	3	90% or .9
S0321	Skill to correlate intelligence priorities to the allocation of intelligence resources/assets.	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
S0322	Skill to craft indicators of operational progress/success.	5 - 15	3	90% or .9
S0323	Skill to create and maintain up-to-date planning documents and tracking of services/production.	16.1, .16.2, 16.3, 16.4, 16.5	4	100% or 1
S0331	Skill to express orally and in writing the relationship between intelligence capability limitations and decision making risk and impacts on the overall operation.	16.4, 16.5	4	100% or 1
S0333	Skill to graphically depict decision support materials containing intelligence and partner capability estimates.	16.4, 16.5	4	100% or 1
S0338	Skill to interpret planning guidance to discern level of analytical support required.	16.5	4	100% or 1
S0340	Skill to monitor target or threat situation and environmental factors.	5 - 15	4	100% or 1
S0341	Skill to monitor threat effects to partner capabilities and maintain a running estimate.	4.3, 4.4	3	90% or .9
S0343	Skill to orchestrate intelligence planning teams, coordinate collection and production support, and monitor status.	3.5, 3.10	3	90% or .9
S0345	Skill to relate intelligence resources/assets to anticipated intelligence requirements.	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
S0350	Skill to synchronize planning activities and required intelligence support.	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	4.1 - 4.13	3	90% or .9

NCWF JOB ROLE

Cyber Intel Planner

Job Role Description: Develops detailed intelligence plans to satisfy cyber operations requirements. Collaborates with cyber operations planners to identify, validate, and levy requirements for collection and analysis. Participates in targeting selection, validation, synchronization, and execution of cyber actions. Synchronizes intelligence activities to support organization objectives in cyberspace.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Intel Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
A0070	Ability to apply critical reading/thinking skills.	4 - 15	4	100% or 1
A0075	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.	3.1 - 3.10	3	90% or .9
A0085	Ability to exercise judgment when policies are not well-defined.	1.1 - 1.15	3	90% or .9
A0082	Ability to effectively collaborate via virtual teams.	3.1 - 3.10	3	90% or .9
A0074	Ability to collaborate effectively with others.	3.1 - 3.10	3	90% or .9
A0067	Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.	3.5, 3.10	3	90% or .9
A0068	Ability to apply approved planning development and staffing processes.	3.5, 3.6, 3.7, 3.8, 3.9, 3.10	4	100% or 1
A0077	Ability to coordinate cyber operations with other organization functions or support activities.	3.1 - 3.10, 4.1 - 4.13	3	90% or .9
A0081	Ability to develop or recommend planning solutions to problems and situations for which no precedent exists.	16.4, 16.5	4	100% or 1
A0090	Ability to identify external partners with common cyber operations interests.	4.3, 4.4	3	90% or .9
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.	1.5, 1.6, 1.7	4	100% or 1
A0096	Ability to interpret and understand complex and rapidly evolving concepts.	1.1	3	90% or .9
A0098	Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.	3.7, 3.8, 3.9, 3.10	3	90% or .9
A0105	Ability to tailor technical and planning information to a customer's level of understanding.	16.4	4	100% or 1
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

Cyber Ops Planner

Job Role Description: A Cyber Ops Planner develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Ops Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0734	Issue requests for information.	Check	3.8, 3.9	3	90% or .9
T0563	Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.	Provide	3.8	3	90% or .9
T0579	Assess target vulnerabilities and/or operational capabilities to determine course of action.	Assess	5.1 - 5.6	4	100% or 1
T0581	Assist and advise inter-agency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.	Assist	16.5	3	90% or .9
T0592	Provide input to the identification of cyber-related success criteria.		N/A		
T0627	Contribute to crisis action planning for cyber operations.	Contribute	3.8	3	90% or .9
T0628	Contribute to the development of the organization's decision support tools if necessary.	Contribute	3.7	3	90% or .9
T0640	Uses intelligence estimates to counter potential target actions.	Counter	3.2	4	100% or 1
T0648	Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives.	Determine	3.3, 3.4	3	90% or .9
T0667	Develop potential courses of action.	Develop	3.8	3	90% or .9
T0670	Develop, implement, and recommend changes to appropriate planning procedures and policies.	Develop	3.8	3	90% or .9
T0680	Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.	Check	3.8	4	100% or 1
T0690	Evaluate intelligence estimates to support the planning cycle.	Evaluate	3.8	2	70% or .7
T0719	Identify cyber intelligence gaps and shortfalls.	Identify	3.4, 3.7	3	90% or .9
T0733	Interpret environment preparations assessments to determine a course of action.	Interprote	5.1 - 5.6	3	90% or .9

NCWF JOB ROLE

Cyber Ops Planner

Job Role Description: A Cyber Ops Planner develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Ops Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0739	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Maintain	3.9	3	90% or .9
T0743	Maintain situational awareness to determine if changes to the operating environment require review of the plan.		N/A		
T0763	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Conduct	3.1 - 3.10	3	90% or .9
T0772	Prepare for and provide subject matter expertise to exercises.	Prepare	1 - 16	3	70% or .7
T0801	Recommend refinement, adaption, termination, and execution of operational plans as appropriate.	Recommend	3.8	3	90% or .9
T0836	Document lessons learned that convey the results of events and/or exercises.	Document	16.4	4	100% or 1
T0571	Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement.	Apply	1.5, 1.6, 1.7, 3.1 - 3.10	4	100% or 1
T0622	Develop, review and implement all levels of planning guidance in support of cyber operations.	Develop	3.8	3	90% or .9
T0635	Coordinate with intelligence and cyber defense partners to obtain relevant essential information.	Coordinate	3.9, 3.10	4	100% or 1
T0654	Develop and maintain deliberate and/or crisis plans.	Develop	3.8	3	90% or .9
T0655	Develop and review specific cyber operations guidance for integration into broader planning activities.	Develop	3.8	3	90% or .9
T0658	Develop cyber operations plans and guidance to ensure that execution and resource allocation decisions align with organization objectives.	Develop	3.8, 3.10	3	90% or .9
T0665	Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations.	Develop	1.6, 3.9	3	90% or .9
T0672	Devise, document, and validate cyber operation strategy, and planning documents.	Document	3.8	3	90% or .9

NCWF JOB ROLE

Cyber Ops Planner

Job Role Description: A Cyber Ops Planner develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Ops Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0679	Ensure operational planning efforts are effectively transitioned to current operations.	Check	3.1 - 3.10	3	90% or .9
T0699	Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.	Support	3.2, 3.3, 3.4, 3.6, 3.7, 3.9	4	100% or 1
T0703	Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities.	Collect	4 - 7	4	100% or 1
T0704	Incorporate cyber operations and communications security support plans into organization objectives.	Incorporate	3.8	3	90% or .9
T0732	Integrate cyber planning/targeting efforts with other organizations.	Integrate	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
T0741	Maintain situational awareness of cyber-related intelligence requirements and associated tasking.	Maintain	4.1 - 4.13	4	100% or 1
T0742	Maintain situational awareness of partner capabilities and activities.	Maintain	4.3, 4.4	3	90% or .9
T0747	Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.	Monitor	4.1 - 4.13, 5.1 - 5.6	3	90% or .9
T0764	Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	Provide	6.1 - 6.9 - 7.1 - 7.14	3	90% or .9
T0787	Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.	Provide	1.10, 1.11, 1.12,	3	90% or .9
T0791	Provide input to the administrative and logistical elements of an operational support plan.	Provide	3.7, 3.8, 3.9, 3.10	3	90% or .9
T0795	Provide planning support between internal and external partners.	Provide	3.7, 3.8, 3.9, 3.10	3	90% or .9
T0813	Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities.	Review	3.1 - 3.10	3	90% or .9
T0823	Submit or respond to requests for deconfliction of cyber operations.	Submit	1 - 16	3	90% or .9
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

Cyber Ops Planner

Job Role Description: A Cyber Ops Planner develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Ops Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0036	Knowledge of human-computer interaction principles.	N/A		
K0173	Withdrawn – Integrated into K0499	N/A		
K0431	Knowledge of evolving/emerging communications technologies.	1.1	3	80% or .8
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).	N/A		
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	4.2, 4.9, 4.11, 6.5, 6.6, 7.11	2	50% or .5
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)	N/A		
K0445	Knowledge of how modern digital and telephony networks impact cyber operations.	N/A		
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.	N/A		
K0446	Knowledge of how modern wireless communications systems impact cyber operations.	13.1	3	90% or .9
K0561	Knowledge of the basics of network security (e.g., encryption, firewalls, authentication, honey pots, perimeter protection).	8.1 - 8.4	3	90% or .9
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	2.1 - 2.6	4	100% or 1
K0480	Knowledge of malware.	7.7	3	90% or .9

NCWF JOB ROLE

Cyber Ops Planner

Job Role Description: A Cyber Ops Planner develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Ops Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0610	Knowledge of virtualization products (VMware, Virtual PC).	N/A		
K0612	Knowledge of what constitutes a "threat" to a network.	1.2	3	90% or .9
K0435	Knowledge of fundamental cyber concepts, principles, limitations, and effects.	1.3	2	70% or .7
K0471	Knowledge of internet network addressing (IP addresses, classless inter-domain routing, TCP/UDP port numbering).	2.1 - 2.6	2	50% or .5
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).	7.7	3	90% or .9
K0348	Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).	N/A		
K0377	Knowledge of classification and control markings standards, policies and procedures.	1.5, 1.6	4	100% or 1
K0349	Knowledge of a wide range of concepts associated with websites (e.g., website types, administration, functions, software systems, etc.).	4.2, 4.8, 10.3, 11.5	4	100% or 1
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	1.10, 6.6, 7.6, 8.12, 9.4, 10.4, 10.5, 10.6, 10.7, 10.8, 10.10, 10.11, 10.12, 11.5, 12.3, 12.5, 13.5, 13.6, 13.8, 13.9, 14.3	4	100% or 1
K0370	Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	N/A		
K0436	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber attack, cyber defense), principles, capabilities, limitations, and effects.	1.1 - 1.15	4	100% or 1
K0379	Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.	4.1 - 4.13	4	100% or 1
K0403	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.	N/A		
K0464	Knowledge of intelligence support to planning, execution, and assessment.	4.1 - 4.13	3	70% or .7

NCWF JOB ROLE

Cyber Ops Planner

Job Role Description: A Cyber Ops Planner develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Ops Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0556	Knowledge of telecommunications fundamentals.	N/A		
K0603	Knowledge of the ways in which targets or threats use the Internet.	1 - 16	4	100% or 1
K0614	Knowledge of wireless technologies (e.g., cellular, satellite, GSM) to include the basic structure, architecture, and design of modern wireless communications systems.	13.1 - 13.9	3	90% or .9
K0465	Knowledge of internal and external partner cyber operations capabilities and tools.	1 - 16	4	100% or 1
K0507	Knowledge of organization or partner exploitation of digital networks.	1 - 16	4	100% or 1
K0598	Knowledge of the structure and intent of organization specific plans, guidance and authorizations.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
K0511	Knowledge of organizational hierarchy and cyber decision making processes.	4.1 - 4.13	1	50% or .5
K0414	Knowledge of cyber operations support or enabling processes.	1.1 - 1.15	3	90% or .9
K0347	Knowledge and understanding of operational design	N/A		
K0350	Knowledge of accepted organization planning systems.	3.7	4	100% or 1
K0352	Knowledge of all forms of intelligence support needs, topics, and focus areas.	1.1 - 1.15, 3.1 - 3.10	3	90% or .9
K0374	Knowledge of basic structure, architecture, and design of modern digital and telephony networks.	N/A		
K0378	Knowledge of classification and control markings standards.	1.6	3	90% or .9
K0399	Knowledge of crisis action planning and time sensitive planning procedures.	3.8	3	90% or .9
K0400	Knowledge of crisis action planning for cyber operations.	3.8	3	90% or .9
K0408	Knowledge of cyber actions (i.e. cyber defense, information gathering, environment preparation, cyber attack) principles, capabilities, limitations, and effects.	1 - 16	4	100% or 1
K0411	Knowledge of cyber laws, legal considerations and their effect on cyber planning.	1.7	4	100% or 1
K0422	Knowledge of deconfliction processes and procedures.	1.12, 1.13	3	90% or .9
K0432	Knowledge of existing, emerging, and long-range issues related to cyber operations strategy, policy, and organization.	1.12	3	90% or .9

NCWF JOB ROLE

Cyber Ops Planner

Job Role Description: A Cyber Ops Planner develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Ops Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0455	Knowledge of information security concepts, facilitating technologies and methods.	1.3	3	90% or .9
K0494	Knowledge of objectives, situation, operational environment, and the status and disposition of internal and external partner collection capabilities available to support planning.	3.1 - 3.10	3	90% or .9
K0501	Knowledge of organization cyber operations programs, strategies, and resources.	3.7	3	90% or .9
K0502	Knowledge of organization decision support tools and/or methods.	3.7	3	90% or .9
K0504	Knowledge of organization issues, objectives, and operations in cyber as well as regulations and policy directives governing cyber operations.	1.5, 1.6, 1.7, 3.1	3	90% or .9
K0506	Knowledge of organization objectives, leadership priorities, and decision-making risks.	3.1 - 3.10	3	90% or .9
K0508	Knowledge of organization policies and planning concepts for partnering with internal and/or external organizations.	3.2, 3.3, 3.4	3	90% or .9
K0512	Knowledge of organizational planning concepts.	3.8	3	90% or .9
K0514	Knowledge of organizational structures and associated intelligence capabilities.	3.1, 3.7	3	90% or .9
K0518	Knowledge of planning activity initiation.	3.8	4	100% or 1
K0519	Knowledge of planning timelines adaptive, crisis action, and time-sensitive planning.	3.8	4	100% or 1
K0525	Knowledge of required intelligence planning products associated with cyber operational planning.	3.7, 3.8	4	100% or 1
K0538	Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities	3.1, 3.7	4	100% or 1
K0566	Knowledge of the critical information requirements and how they're used in planning.	3.7, 3.10	3	90% or .9
K0572	Knowledge of the functions and capabilities of internal teams that emulate threat activities to benefit the organization.	3.5	3	90% or .9
K0582	Knowledge of the organizational planning and staffing process.	3.7, 3.10	3	90% or .9
K0585	Knowledge of the organizational structure as it pertains to full spectrum cyber operations, including the functions, responsibilities, and interrelationships among distinct internal elements.	3.1 - 3.10	3	90% or .9
K0586	Knowledge of the outputs of course of action and exercise analysis.	16.4	3	90% or .9

NCWF JOB ROLE

Cyber Ops Planner

Job Role Description: A Cyber Ops Planner develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Ops Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0589	Knowledge of the process used to assess the performance and impact of operations.	3.8	3	90% or .9
K0590	Knowledge of the processes to synchronize operational assessment procedures with the critical information requirement process.	4 - 15	3	90% or .9
K0593	Knowledge of the range of cyber operations and their underlying intelligence support needs, topics, and focus areas.	N/A		
K0594	Knowledge of the relationships between end states, objectives, effects, lines of operation, etc.	16.4	3	90% or .9
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	N/A		
K0497	Knowledge of operational effectiveness assessment.	4.1 - 4.13	4	100% or 1
K0534	Knowledge of staff management, assignment, and allocation processes.	3.5, 3.8, 3.9, 3.10	4	100% or 1
K0576	Knowledge of the information environment.	4.1 - 4.13	3	90% or .9
K0597	Knowledge of the role of network operations in supporting and facilitating other organization operations.	N/A		
S0218	Skill in evaluating information for reliability, validity, and relevance.	1.1 - 1.15	4	100% or 1
S0249	Skill in preparing and presenting briefings.	1 - 16	4	100% or 1
S0296	Skill in utilizing feedback in order to improve processes, products, and services.	N/A		
S0297	Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).	N/A		
S0176	Skill in administrative planning activities, to include preparation of functional and specific support plans, preparing and managing correspondence, and staffing procedures.	3.1 - 3.10	4	100% or 1
S0185	Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.	3.1 - 3.10	4	100% or 1
S0186	Skill in applying crisis planning procedures.	3.8	4	100% or 1
S0213	Skill in documenting and communicating complex technical and programmatic information.	16.4	4	100% or 1
S0250	Skill in preparing plans and related correspondence.	3.8, 3.9, 3.10	4	100% or 1

NCWF JOB ROLE

Cyber Ops Planner

Job Role Description: A Cyber Ops Planner develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Ops Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0273	Skill in reviewing and editing plans.	3.8	4	100% or 1
S0309	Skill to anticipate key target or threat activities which are likely to prompt a leadership decision.	5 -15	4	100% or 1
S0312	Skill to apply the process used to assess the performance and impact of cyber operations.	3.8	3	90% or .9
S0322	Skill to craft indicators of operational progress/success.	5 -15	3	90% or .9
S0333	Skill to graphically depict decision support materials containing intelligence and partner capability estimates.	16.4, 16.5	4	100% or 1
S0209	Skill in developing and executing comprehensive cyber operations assessment programs for assessing and validating operational performance characteristics.	5 -15	4	100% or 1
S0326	Skill to distinguish between notional and actual resources and their applicability to the plan under development.	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
S0349	Skill to synchronize operational assessment procedures with the critical information requirement process.	3.1 - 3.10, 5.1 - 5.6	3	90% or .9
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	4.1 - 413	3	90% or .9
A0070	Ability to apply critical reading/thinking skills.	4 -15	4	100% or 1
A0075	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.	3.1 - 3.10	3	90% or .9
A0085	Ability to exercise judgment when policies are not well-defined.	1.1 - 1.15	3	90% or .9
A0082	Ability to effectively collaborate via virtual teams.	3.1 - 3.10	3	90% or .9
A0074	Ability to collaborate effectively with others.	3.1 - 3.10	3	90% or .9
A0067	Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.	3.5, 3.10	3	90% or .9
A0068	Ability to apply approved planning development and staffing processes.	3.5, 3.6, 3.7, 3.8, 3.9, 3.10	4	100% or 1
A0077	Ability to coordinate cyber operations with other organization functions or support activities.	3.1 - 3.10, 04	3	90% or .9

NCWF JOB ROLE

Cyber Ops Planner

Job Role Description: A Cyber Ops Planner develops detailed plans for the conduct or support of the applicable range of cyber operations through collaboration with other planners, operators and/or analysts. Participates in targeting selection, validation, synchronization, and enables integration during the execution of cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Ops Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
A0081	Ability to develop or recommend planning solutions to problems and situations for which no precedent exists.	16.4, 16.5	4	100% or 1
A0090	Ability to identify external partners with common cyber operations interests.	4.3, 4.4	3	90% or .9
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.	1.5, 1.6, 1.7	4	100% or 1
A0096	Ability to interpret and understand complex and rapidly evolving concepts.	1.1	3	90% or .9
A0098	Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.	3.7, 3.8, 3.9, 3.10	3	90% or .9
A0105	Ability to tailor technical and planning information to a customer's level of understanding.	16.4	4	100% or 1
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

Partner Integration Planner

Job Role Description: A Partner Integration Planner works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Partner Integration Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0581	Assist and advise inter-agency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.	Assist	16.5	3	90% or .9
T0627	Contribute to crisis action planning for cyber operations.	Contribute	3.8	3	90% or .9
T0670	Develop, implement, and recommend changes to appropriate planning procedures and policies.	Develop	3.8	3	90% or .9
T0739	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Maintain	3.9	3	90% or .9
T0763	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Conduct	3.1 - 3.10	3	90% or .9
T0772	Prepare for and provide subject matter expertise to exercises.	Prepare	1 - 16	3	70% or .7
T0836	Document lessons learned that convey the results of events and/or exercises.	Document	16.4	4	100% or 1
T0571	Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement.	Apply	1.5, 1.6, 1.7, 3.1 - 3.10	4	100% or 1
T0635	Coordinate with intelligence and cyber defense partners to obtain relevant essential information.	Coordinate	3.9, 3.10	4	100% or 1
T0665	Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations.	Develop	3.8	3	90% or .9
T0699	Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.	Support	3.2, 3.3, 3.4, 3.6, 3.7, 3.9	4	100% or 1
T0732	Integrate cyber planning/targeting efforts with other organizations.	Integrate	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
T0747	Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.	Monitor	4.1 - 4.13, 5.1 - 5.6	3	90% or .9
T0764	Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	Provide	6.1 - 6.9, 7.1 - 7.14	3	90% or .9

NCWF JOB ROLE

Partner Integration Planner

Job Role Description: A Partner Integration Planner works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Partner Integration Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0787	Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.	Provide	1.10, 1.11, 1.12,	3	90% or .9
T0795	Provide planning support between internal and external partners.	Provide	3.7, 3.8, 3.9, 3.10	3	90% or .9
T0823	Submit or respond to requests for deconfliction of cyber operations.	Submit	1 - 16	3	90% or .9
T0601	Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).		N/A		
T0760	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	Provide	3.8, 3.10	3	90% or .9
T0784	Provide cyber focused guidance and advice on intelligence support plan inputs.	Provide	3.8	3	90% or .9
T0629	Contribute to the development, staffing, and coordination of cyber operations policies, performance standards, plans and approval packages with appropriate internal and/or external decision makers.	Contribute	1.5, 1.6, 1.7, 3.5, 3.8, 3.9, 3.10	4	100% or 1
T0666	Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives.	Develop	1.5, 1.6, 1.7, 1.12	4	100% or 1
T0669	Develop strategy and processes for partner planning, operations, and capability development.	Develop	3.8	3	90% or .9
T0671	Develop, maintain, and assess cyber cooperation security agreements with external partners.	Develop	3.3, 3.4, 3.6, 3.7	4	100% or 1
T0700	Facilitate the sharing of "best practices" and "lessons learned" throughout the cyber operations community.	Facilitate	1.13	3	90% or .9
T0712	Identify and manage security cooperation priorities with external partners.	Identify	3.8, 3.9	3	90% or .9
T0729	Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities.	Inform	3.7, 3.8, 3.9, 3.10	3	90% or .9

NCWF JOB ROLE

Partner Integration Planner

Job Role Description: A Partner Integration Planner works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Partner Integration Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0759	Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.	Contribute	16.2	3	90% or .9
T0762	Provide subject matter expertise in course of action development.	Provide	3.8	3	90% or .9
T0766	Propose policy which governs interactions with external coordination groups.	Propose	1.5	3	90% or .9
T0817	Serve as a conduit of information from partner teams by identifying subject matter experts who can assist in the investigation of complex or unusual situations.	Support	3.7, 3.8, 3.9	3	90% or .9
T0818	Serve as a liaison with external partners.	Support	3.7	4	100% or 1
T0825	Synchronize cyber international engagement activities and associated resource requirements as appropriate.	Integrate	3.3, 3.4, 3.6, 3.7, 3.10	4	100% or 1
T0826	Synchronize cyber portions of security cooperation plans.	Integrate	3.8	3	90% or .9
	Summary			**3**	**90% or .9**

NCWF JOB ROLE

Partner Integration Planner

Job Role Description: A Partner Integration Planner works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Partner Integration Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0173	Withdrawn – Integrated into K0499	N/A		
K0431	Knowledge of evolving/emerging communications technologies.	1.1	3	80% or .8
K0417	Knowledge of data communications terminology (e.g., networking protocols, Ethernet, IP, encryption, optical devices, removable media).	N/A		
K0444	Knowledge of how internet applications work (SMTP email, web-based email, chat clients, VOIP).	4.2, 4.9, 4.11, 6.5, 6.6, 7.11	2	50% or .5
K0395	Knowledge of computer networking fundamentals (i.e., basic computer components of a network, types of networks, etc.)	N/A		
K0435	Knowledge of fundamental cyber concepts, principles, limitations, and effects.	1.3	2	70% or .7
K0392	Knowledge of common computer/network infections (virus, Trojan, etc.) and methods of infection (ports, attachments, etc.).	7.7	3	90% or .9
K0348	Knowledge of a wide range of basic communications media concepts and terminology (e.g., computer and telephone networks, satellite, cable, wireless).	N/A		
K0377	Knowledge of classification and control markings standards, policies and procedures.	1.5, 1.6	4	100% or 1

NCWF JOB ROLE

Partner Integration Planner

Job Role Description: A Partner Integration Planner works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Partner Integration Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0362	Knowledge of attack methods and techniques (DDoS, brute force, spoofing, etc.).	1.10, 6.6, 7.6, 8.12, 9.4, 10.4, 10.5, 10.6, 10.7, 10.8, 10.10, 10.11, 10.12, 11.5, 12.3, 12.5, 13.5, 13.6, 13.8, 13.9, 14.3	4	100% or 1
K0370	Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	N/A		
K0436	Knowledge of fundamental cyber operations concepts, terminology/lexicon (i.e., environment preparation, cyber attack, cyber defense), principles, capabilities, limitations, and effects.	1.1 - 1.15	4	100% or 1
K0379	Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.	4.1 - 4.13	4	100% or 1
K0403	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.	N/A		
K0465	Knowledge of internal and external partner cyber operations capabilities and tools.	1 - 16	4	100% or 1
K0507	Knowledge of organization or partner exploitation of digital networks.	1 - 16	4	100% or 1
K0598	Knowledge of the structure and intent of organization specific plans, guidance and authorizations.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
K0511	Knowledge of organizational hierarchy and cyber decision making processes.	N/A		
K0414	Knowledge of cyber operations support or enabling processes.	1.1 - 1.15	3	90% or .9
K0350	Knowledge of accepted organization planning systems.	3.7	4	100% or 1
K0374	Knowledge of basic structure, architecture, and design of modern digital and telephony networks.	N/A		
K0400	Knowledge of crisis action planning for cyber operations.	3.8	3	90% or .9
K0408	Knowledge of cyber actions (i.e. cyber defense, information gathering, environment preparation, cyber attack) principles, capabilities, limitations, and effects.	1 - 16	4	100% or 1
K0411	Knowledge of cyber laws, legal considerations and their effect on cyber planning.	1.7	4	100% or 1
K0422	Knowledge of deconfliction processes and procedures.	1.12, 1.13	3	90% or .9

NCWF JOB ROLE

Partner Integration Planner

Job Role Description: A Partner Integration Planner works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Partner Integration Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0432	Knowledge of existing, emerging, and long-range issues related to cyber operations strategy, policy, and organization.	1.12	3	90% or .9
K0455	Knowledge of information security concepts, facilitating technologies and methods.	1.3	3	90% or .9
K0501	Knowledge of organization cyber operations programs, strategies, and resources.	3.7	3	90% or .9
K0504	Knowledge of organization issues, objectives, and operations in cyber as well as regulations and policy directives governing cyber operations.	1.5, 1.6, 1.7, 3.1	3	90% or .9
K0506	Knowledge of organization objectives, leadership priorities, and decision-making risks.	3.1 - 3.10	3	90% or .9
K0508	Knowledge of organization policies and planning concepts for partnering with internal and/or external organizations.	3.2, 3.3, 3.4	3	90% or .9
K0512	Knowledge of organizational planning concepts.	3.8	3	90% or .9
K0514	Knowledge of organizational structures and associated intelligence capabilities.	3.1, 3.7	3	90% or .9
K0538	Knowledge of target and threat organization structures, critical capabilities, and critical vulnerabilities	3.1, 3.7	4	100% or 1
K0585	Knowledge of the organizational structure as it pertains to full spectrum cyber operations, including the functions, responsibilities, and interrelationships among distinct internal elements.	3.1 - 3.10	3	90% or .9
S0218	Skill in evaluating information for reliability, validity, and relevance.	1.1 - 1.15	4	100% or 1
S0249	Skill in preparing and presenting briefings.	1 - 16	4	100% or 1
S0296	Skill in utilizing feedback in order to improve processes, products, and services.	N/A		
S0297	Skill in utilizing virtual collaborative workspaces and/or tools (e.g., IWS, VTCs, chat rooms, SharePoint).	N/A		
S0185	Skill in applying analytical methods typically employed to support planning and to justify recommended strategies and courses of action.	3.1 - 3.10	4	100% or 1
S0186	Skill in applying crisis planning procedures.	3.8	4	100% or 1
S0213	Skill in documenting and communicating complex technical and programmatic information.	16.4	4	100% or 1
S0250	Skill in preparing plans and related correspondence.	3.8, 3.9, 3.10	4	100% or 1

NCWF JOB ROLE

Partner Integration Planner

Job Role Description: A Partner Integration Planner works to advance cooperation across organizational or national borders between cyber operations partners. Aids the integration of partner cyber teams by providing guidance, resources, and collaboration to develop best practices and facilitate organizational support for achieving objectives in integrated cyber actions.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Partner Integration Planner. ECSA maps to this job role at a Specialist level (level 3) with a correlation coefficient of .9 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0326	Skill to distinguish between notional and actual resources and their applicability to the plan under development.	3.1 - 3.10, 4.1 - 4.13	4	100% or 1
A0066	Ability to accurately and completely source all data used in intelligence, assessment and/or planning products.	4.1 - 4.13	3	90% or .9
A0070	Ability to apply critical reading/thinking skills.	4 - 15	4	100% or 1
A0075	Ability to communicate complex information, concepts, or ideas in a confident and well-organized manner through verbal, written, and/or visual means.	1.1 - 1.15, 3.1 - 3.10	4	100% or 1
A0089	Ability to function in a collaborative environment, seeking continuous consultation with other analysts and experts—both internal and external to the organization—in order to leverage analytical and technical expertise.	3.1 - 3.10	3	90% or .9
A0085	Ability to exercise judgment when policies are not well-defined.	1.1 - 1.15	3	90% or .9
A0082	Ability to effectively collaborate via virtual teams.	3.1 - 3.10	3	90% or .9
A0074	Ability to collaborate effectively with others.	3.1 - 3.10	3	90% or .9
A0067	Ability to adjust to and operate in a diverse, unpredictable, challenging, and fast-paced work environment.	3.5, 3.10	3	90% or .9
A0068	Ability to apply approved planning development and staffing processes.	3.5, 3.6, 3.7, 3.8, 3.9, 3.10	4	100% or 1
A0077	Ability to coordinate cyber operations with other organization functions or support activities.	3.1 - 3.10, 4.1 - 4.13	3	90% or .9
A0081	Ability to develop or recommend planning solutions to problems and situations for which no precedent exists.	16.4, 16.5	4	100% or 1
A0090	Ability to identify external partners with common cyber operations interests.	4.3, 4.4	3	90% or .9
A0094	Ability to interpret and apply laws, regulations, policies, and guidance relevant to organization cyber objectives.	1.5, 1.6, 1.7	4	100% or 1
A0096	Ability to interpret and understand complex and rapidly evolving concepts.	1.1	3	90% or .9
A0098	Ability to participate as a member of planning teams, coordination groups, and task forces as necessary.	3.7, 3.8, 3.9, 3.10	3	90% or .9
A0105	Ability to tailor technical and planning information to a customer's level of understanding.	16.4	4	100% or 1
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

Cyber Operator

Job Role Description: A Cyber Operator conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Operator. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0566	Analyze own operational architecture, tools, and procedures for ways to improve performance.	Analyze	3.7	3	90% or .9
T0567	Analyze target operational architecture for ways to gain access.	Analyze	6.3, 6.4, 6.5, 6.6, 6.7	4	100% or 1
T0598	Collaborate with development organizations to create and deploy the tools needed to achieve objectives.	Evaluate, Synthesize	4 -15	4	100% or 1
T0609	Conduct access enabling of wireless computer and digital networks.	Perform, Analyze	13.2	4	100% or 1
T0610	Conduct collection and processing of wireless computer and digital networks.	Perform, Analyze	13.3	4	100% or 1
T0612	Conduct exploitation of wireless computer and digital networks.	Perform, Analyze	13.4, 13.5, 13.6, 13.8, 13.9	4	100% or 1
T0616	Conduct network scouting and vulnerability analyses of systems within a network.	Perform, Analyze	5.1 - 5.6, 6.1 - 6.9, 7.1 - 7.14	4	100% or 1
T0618	Conduct on-net activities to control and exfiltrate data from deployed technologies.	Perform, Analyze	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
T0619	Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies.	Perform, Analyze	4.1 - 4.13, 6.1 - 6.9	4	100% or 1
T0620	Conduct open source data collection via various online tools.	Perform, Analyze	4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8, 4.9, 4.10	4	100% or 1
T0623	Conduct survey of computer and digital networks.	Perform, Analyze	3.10	3	90% or .9
T0643	Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).	Perform, Analyze	6.1 - 6.9, 7.1 - 7.14	4	100% or 1
T0644	Detect exploits against targeted networks and hosts and react accordingly.	Analyze, Evaluate	6.1 - 6.9, 7.1 - 7.14	4	100% or 1
T0664	Develop new techniques for gaining and keeping access to target systems.	Evaluate, Synthesize	7.4	4	100% or 1
T0677	Edit or execute simple scripts (e.g., PERL, VBS) on Windows and UNIX systems.	Perform, Analyze	N/A		
T0696	Exploit network devices, security devices, and/or terminals or environments using various methods or tools.	Perform, Analyze	7.6, 7.7, 7.8, 7.9, 7.12	4	100% or 1

NCWF JOB ROLE

Cyber Operator

Job Role Description: A Cyber Operator conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Operator. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
T0697	Facilitate access enabling by physical and/or wireless means.	Perform, Analyze	4.11	4	100% or 1
T0724	Identify potential points of strength and vulnerability within a network.	Analyze, Evaluate	5.1 - 5.6	4	100% or 1
T0740	Maintain situational awareness and functionality of organic operational infrastructure.	Perform, Analyze	5.1 - 5.6	4	100% or 1
T0756	Operate and maintain automated systems for gaining and maintaining access to target systems.	Perform, Analyze	7.4	3	90% or .9
T0768	Conduct cyber activities to degrade/remove information resident in computers and computer networks.	Perform, Analyze	7.7, 7.8, 7.9	3	90% or .9
T0774	Process exfiltrated data for analysis and/or dissemination to customers.	Perform, Analyze, Evaluate	16.3, 16.4	4	100% or 1
T0796	Provide real-time actionable geolocation information.	Perform, Analyze	4.2	4	100% or 1
T0804	Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects.	Perform, Analyze	16.3, 16.4	4	100% or 1
T0828	Test and evaluate locally developed tools for operational use.	Analyze, Evaluate	4 -15	4	100% or 1
T0829	Test internal developed tools and techniques against target tools.	Analyze, Evaluate	4 -15	4	100% or 1
	Summary			**4**	**95% or .95**

NCWF JOB ROLE

Cyber Operator

Job Role Description: A Cyber Operator conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Operator. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	1 - 16	4	90% or .9
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	1.10	4	90% or .9
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	1.7, 1.11	4	90% or .9
K0004	* Knowledge of cybersecurity principles.	1.2	4	90% or .9
K0005	* Knowledge of cyber threats and vulnerabilities.	1.3	4	90% or .9
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	1.1	4	90% or .9
K0142	Knowledge of collection management processes, capabilities, and limitations.	4.1 - 4.13	4	100% or 1
K0370	Knowledge of basic physical computer components and architecture, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	N/A		
K0379	Knowledge of client organizations, including information needs, objectives, structure, capabilities, etc.	4.1 - 4.13	4	100% or 1
K0403	Knowledge of cryptologic capabilities, limitations, and contributions to cyber operations.	N/A		
K0560	Knowledge of the basic structure, architecture, and design of modern communication networks.	N/A		
K0565	Knowledge of the common networking and routing protocols (e.g. TCP/IP), services (e.g., web, mail, DNS), and how they interact to provide network communications.	2.1 - 2.6	4	100% or 1
K0480	Knowledge of malware.	7.7	3	90% or .9
K0516	Knowledge of physical and logical network devices and infrastructure to include hubs, switches, routers, firewalls, etc.	N/A		
K0427	Knowledge of encryption algorithms and cyber capabilities/tools (e.g., SSL, PGP).	N/A		
K0440	Knowledge of host-based security products and how they affect exploitation and vulnerability.	5.5, 7.13, 9.8	4	100% or 1
K0430	Knowledge of evasion strategies and techniques.	9.5, 9.8	3	90% or .9
K0537	Knowledge of system administration concepts for the Unix/Linux and Windows operating systems (e.g., process management, directory structure, installed applications, Access Controls).	N/A		

NCWF JOB ROLE

Cyber Operator

Job Role Description: A Cyber Operator conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Operator. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0608	Knowledge of Unix/Linux and Windows operating systems structures and internals (e.g., process management, directory structure, installed applications).	N/A		
K0360	Knowledge of assembly code.	N/A		
K0363	Knowledge of auditing and logging procedures (including server-based logging).	N/A		
K0365	Knowledge of basic back-up and recovery procedures including different types of backups (e.g., full, incremental).	N/A		
K0372	Knowledge of basic programming concepts (e.g., levels, structures, compiled vs. interpreted languages).	N/A		
K0373	Knowledge of basic software applications (e.g., data storage and backup, database applications) and their vulnerabilities.	N/A		
K0375	Knowledge of basic wireless applications, including vulnerabilities in various types of wireless applications.	13.1 - 13.9	3	90% or .9
K0406	Knowledge of current software and methodologies for active defense and system hardening.	N/A		
K0420	Knowledge of database theory.	N/A		
K0423	Knowledge of deconfliction reporting to include external organization interaction.	16.1 - 16.6	4	100% or 1
K0428	Knowledge of encryption algorithms and tools for WLANs.	N/A		
K0429	Knowledge of enterprise-wide information management.	N/A		
K0433	Knowledge of forensic implications of operating system structure and operations.	N/A		
K0438	Knowledge of Global Systems for Mobile Communications (GSM) architecture.	N/A		
K0452	Knowledge of implementing Unix and Windows systems that provide radius authentication and logging, DNS, mail, web service, FTP server, DHCP, firewall, and SNMP.	N/A		
K0468	Knowledge of internal and external partner reporting.	16.1 - 16.6	4	100% or 1
K0481	Knowledge of methods and techniques used to detect various exploitation activities	6 - 15	3	90% or .9
K0485	Knowledge of network administration.	N/A		
K0486	Knowledge of network construction and topology.	N/A		

NCWF JOB ROLE

Cyber Operator

Job Role Description: A Cyber Operator conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Operator. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
K0528	Knowledge of satellite-based communication systems.	N/A		
K0530	Knowledge of security hardware and software options, including the network artifacts they induce and their effects on exploitation.	N/A		
K0531	Knowledge of security implications of software configurations.	N/A		
K0536	Knowledge of structure, approach, and strategy of exploitation tools (e.g., sniffers, keyloggers) and techniques (e.g., gaining backdoor access, collecting/exfiltrating data, conducting vulnerability analysis of other systems in the network).	5.1 - 5.6, 6.1 - 6.9, 7.1 - 7.14	4	100% or 1
K0573	Knowledge of the fundamentals of digital forensics in order to extract actionable intelligence.	N/A		
K0609	Knowledge of virtual machine technologies.	N/A		
S0062	Skill in analyzing memory dumps to extract information.	N/A		
S0183	Skill in analyzing terminal or environment collection data.	6.1 - 6.9	3	90% or .9
S0236	Skill in identifying the devices that work at each level of protocol models.	2.1 - 2.6	4	100% or 1
S0182	Skill in analyzing target communications internals and externals collected from wireless LANs.	16.3, 16.4	4	100% or 1
S0190	Skill in assessing current tools to identify needed improvements.	4 - 15	4	100% or 1
S0192	Skill in auditing firewalls, perimeters, routers, and intrusion detection systems.	8.6, 8.7, 8.8, 8.9, 8.10, 8.11, 8.12, 9.4, 9.5, 9.6	4	100% or 1
S0202	Skill in data mining techniques (e.g., searching file systems) and analysis.	11.5	2	70% or .7
S0206	Skill in determining installed patches on various operating systems and identifying patch signatures.	6.2	3	90% or .9
S0221	Skill in extracting information from packet captures.	7.10, 7.11, 8.2, 8.6, 8.8, 9.3, 9.5, 13.4	4	100% or 1
S0242	Skill in interpreting vulnerability scanner results to identify vulnerabilities.	5.5, 5.6	4	100% or 1
S0243	Skill in knowledge management, including technical documentation techniques (e.g., Wiki page).	16.1 - 16.6	3	90% or .9
S0252	Skill in processing collected data for follow-on analysis.	6 - 15	3	90% or .9

NCWF JOB ROLE

Cyber Operator

Job Role Description: A Cyber Operator conducts collection, processing, and/or geolocation of systems in order to exploit, locate, and/or track targets of interest. Performs network navigation, tactical forensic analysis, and, when directed, executing on-net operations.

Maps To: EC-Council Certified Security Analyst (ECSA)

Mapping Summary: Performance-based learning and evaluation in ECSA imparts specific KSAs that should be demonstrated by a Cyber Operator. ECSA maps to this job role at a Expert level (level 4) with a correlation coefficient of .95 on the framework Tasks and .9 on the KSA proficiency descriptions.

KSA

ID	Statement	ECSA Exam Objectives	NICE Proficiency	Relational Coefficient
S0255	Skill in providing real-time, actionable geolocation information utilizing target infrastructures.	4.2	3	90% or .9
S0257	Skill in reading, interpreting, writing, modifying, and executing simple scripts (e.g., PERL, VBS) on Windows and Unix systems (e.g., those that perform tasks like parsing large data files, automating manual tasks, and fetching/processing remote data).	N/A		
S0266	Skill in relevant programming languages (e.g., C++, Python, etc.).	N/A		
S0267	Skill in remote command line and Graphic User Interface (GUI) tool usage.	4 - 15	4	100% or 1
S0270	Skill in reverse engineering (e.g., hex editing, binary packaging utilities, debugging, and strings analysis) to identify function and ownership of remote tools.	N/A		
S0275	Skill in server administration.	N/A		
S0276	Skill in survey, collection, and analysis of wireless LAN metadata.	13.1, 13.2, 13.3, 13.4	4	100% or 1
S0281	Skill in technical writing.	16.1 - 16.6	4	100% or 1
S0282	Skill in testing and evaluating tools for implementation.	4 - 15	4	100% or 1
S0293	Skill in using tools, techniques, and procedures to remotely exploit and establish persistence on a target.	7.4, 7.5, 7.6, 7.7, 7.8, 7.9	4	100% or 1
S0295	Skill in using various open source data collection tools (online trade, DNS, mail, etc.).	4.1 - 4.13	4	100% or 1
S0298	Skill in verifying the integrity of all files.	N/A		
S0299	Skill in wireless network target analysis, templating, and geolocation.	13.1 - 13.9	4	100% or 1
A0095	Ability to interpret and translate customer requirements into operational action.	3.1 - 3.10	4	100% or 1
A0097	Ability to monitor system operations and react to events in response to triggers and/or observation of trends or unusual activity.	1 - 16	4	100% or 1
A0099	Ability to perform network collection tactics, techniques, and procedures to include decryption capabilities/tools.	6 -15	4	100% or 1
A0100	Ability to perform wireless collection procedures to include decryption capabilities/tools.	13.1 - 13.9	4	100% or 1
	Summary		**4**	**90% or .9**

THE NATIONAL CYBERSECURITY WORKFORCE FRAMEWORK

INVESTIGATE (IN)

Specialty areas responsible for investigating cybersecurity events or crimes related to information technology (IT) systems, networks, and digital evidence.

Cyber Investigation (CI)

Applies tactics, techniques, and procedures for a full range of investigative tools and processes to include but not limited to interview and interrogation techniques, surveillance, counter surveillance, and surveillance detection, and appropriately balances the benefits of prosecution versus intelligence gathering.

Digital Forensics (FO)

Collects, processes, preserves, analyzes, and presents computer-related evidence in support of network vulnerability mitigation and/or criminal, fraud, counterintelligence, or law enforcement investigations.

NCWF JOB ROLE

Cyber Crime Investigator

Job Role Description: A Cyber Crime Investigator identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Cyber Crime Investigator. CHFI maps to this job role at a Specialist level (level 4) with a correlation coefficient of 1 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CHFI Objectives	NICE Proficiency	Relational Coefficient
T0031	Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.	Synthesis	14.5, 14.6, 14.8	3	100% or 1
T0059	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the internet.	Creating, Synthesis	1.4,1.5, 2.5, 4.2, 4.3, 4.7, 5.3, 6.1, 6.2	4	100% or 1
T0096	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals).	Construct, Create	2.3, 14.5, 14.6, 14.8	3	95% or .95
T0103	Examine recovered data for information of relevance to the issue at hand.	Evaluate	2.7, 3.5, 5.3, 6.2, 6.3, 6.4, 6.5, 7.5, 11.5, 11.6, 11.7, 11.8, 13.8	4	100% or 1
T0104	Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.	Apply	7.1, 7.2, 7.3, 7.4, 7.5, 7.6, 7.7, 7.8, 8.3, 8.4, 8.5, 8.6, 8.7, 8.8	3	100% or 1
T0110	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.	Comprehension	2.3, 7.2, 12.8, 13.7, 1.4, 1.8,	3	100% or 1
T0112	Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.	Comprehension	1.4,1.5, 2.5, 4.2, 4.3, 4.7, 5.3, 6.1, 6.2, 5.1, 5.7, 5.8,	4	100% or 1
T0113	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Comprehension	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7,	4	100% or 1
T0114	Identify elements of proof of the crime.	Comprehension	1.4,1.5, 2.5, 4.2, 4.3, 4.7, 5.3, 6.1, 6.2	4	100% or 1
T0120	Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.	Comprehension	2.5, 2.6, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6	4	100% or 1
T0225	Secure the electronic device or information source.	Synthesis	2.4, 2.5, 2.6, 2.7, 4.4, 4.6,	4	100% or 1

NCWF JOB ROLE

Cyber Crime Investigator

Job Role Description: A Cyber Crime Investigator identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Cyber Crime Investigator. CHFI maps to this job role at a Specialist level (level 4) with a correlation coefficient of 1 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CHFI Objectives	NICE Proficiency	Relational Coefficient
T0241	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Synthesis	2.4, 2.5, 2.6, 2.7, 4.4, 4.6, 13.8, 4.2, 6.1, 6.7, 9.3,	3	100% or 1
T0343	Analyze the crisis situation to ensure public, personal, and resource protection.	Analyze	2.1, 4.1, 4.2, 4.4, 4.5, 4.6, 12.2,	2	95% or .95
T0346	Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation.		N/A		
T0360	Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.	Discover	5.1, 5.2, 5.3, 5.5, 5.6, 5.7, 8.2, 8.3, 8.5, 10.7, 11.2, 11.3, 11.5,	3	100% or 1
T0386	Provide criminal investigative support to trial counsel during the judicial process.	Evaluation	2.6, 14.2, 14.3, 14.4, 14.5, 14.8	3	100% or 1
T0423	Analyze computer-generated threats for counter intelligence or criminal activity.	Analyze	4.2, 4.3, 4.4, 5.3, 5.4, 5.5, 5.7, 6.1, 6.2, 6.3, 6.4, 8.2, 8.3, 8.4, 11.2, 11.3, 11.4,	4	100% or 1
T0430	Gather and preserve evidence used on the prosecution of computer crimes.	Synthesis	5.3, 13.8, 1.5, 2.3, 2.5, 2.6, 2.7, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7,	4	100% or 1
T0433	Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.	Synthesis	7.1, 7.5, 7.6, 7.8	4	100% or 1
T0453	Determine and develop leads and identify sources of information in order to identify and/or prosecute the responsible parties to an intrusion or other crimes.	Comprehension	1.4,1.5, 2.5, 4.2, 4.3, 4.7, 5.3, 6.1, 6.2,	3	95% or .95

NCWF JOB ROLE

Cyber Crime Investigator

Job Role Description: A Cyber Crime Investigator identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Cyber Crime Investigator. CHFI maps to this job role at a Specialist level (level 4) with a correlation coefficient of 1 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CHFI Objectives	NICE Proficiency	Relational Coefficient
T0471	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).	Synthesis	2.5, 2.6	4	100% or 1
T0479	Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property.	Synthesis	1.6, 1.7, 2.1, 4.6, 4.7, 11.4	2	95% or .95
T0523	Prepare reports to document the investigation following legal standards and require-ments.	Construct, Create	14.1, 14.2, 14.3, 14.4, 14.5, 14.6,	3	100% or 1
	Summary			**4**	**100% or 1**

NCWF JOB ROLE

Cyber Crime Investigator

Job Role Description: A Cyber Crime Investigator identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Cyber Crime Investigator. CHFI maps to this job role at a Specialist level (level 4) with a correlation coefficient of 1 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	5.5, 7.1, 3.3	3	50% or .5
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	N/A		
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	2.3, 7.2, 12.8, 13.7, 7.3, 1.4, 1.5, 14.3, 14.4,	3	50% or .5
K0004	* Knowledge of cybersecurity principles.	7.1,	3	95% or .95
K0005	* Knowledge of cyber threats and vulnerabilities.	8.3, 8.4, 10.2, 11.2, 13.1 8.2, 8.8	3	95% or .95
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	N/A	3	95% or .95
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	8.3, 8.4, 10.2, 11.2, 13.1 8.2, 8.8	3	95% or .95
K0114	Knowledge of electronic devices (e.g., computer systems/components, access control devices, digital cameras, electronic organizers, hard drives, memory cards, modems, network components, printers, removable storage devices, scanners, telephones, copiers, credit card skimmers, facsimile machines, global positioning systems [GPSs]).	5.3, 2.5, 4.2, 13.8, 3.3,	2	95% or .95
K0118	Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody).	2.4, 2.5, 2.6, 2.7, 4.4, 4.6	4	95% or .95
K0123	Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence).	1.4, 1.5, 14.3, 14.4,	4	95% or .95
K0128	Knowledge of types and collection of persistent data.	2.5, 6.1, 6.7, 9.3 , 5.3, 4.2, 13.8	2	95% or .95
K0144	Knowledge of social dynamics of computer attackers in a global context.	1.3, 1.8 5.6, 10.7	3	95% or .95

NCWF JOB ROLE

Cyber Crime Investigator

Job Role Description: A Cyber Crime Investigator identifies, collects, examines, and preserves evidence using controlled and documented analytical and investigative techniques.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Cyber Crime Investigator. CHFI maps to this job role at a Specialist level (level 4) with a correlation coefficient of 1 on the Framework tasks and a correlation coefficient of .95 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	2.3, 7.2, 12.8, 13.7	3	90% or .9
K0231	Knowledge of crisis management protocols, processes, and techniques.	1.3, 1.4, 1.5, 1.7, 5.8, 10.7	2	95% or .95
K0244	Knowledge of physical and physiological behaviors that may indicate suspicious or abnormal activity.	N/A		95% or .95
K0251	Knowledge of the judicial process, including the presentation of facts and evidence.	2.6, 2.8, 1.8, 12.8 14.2, 14.3, 14.6, 14.8	2	90% or .9
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	1.5, 2.3, 2.5, 2.6, 2.7, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7,	4	95% or .95
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	2.4, 2.5, 2.6, 2.7, 4.4, 4.6, 6.6	4	100% or 1
S0072	Skill in using scientific rules and methods to solve problems.	2.5, 2.6, 7.1, 7.2, 7.3, 7.4, 7.5, 7.6	1	95% or .95
S0086	Skill in evaluating the trustworthiness of the supplier and/or product.	2.3, 2.6, 3.3, 4.6, 7.5,	2	95% or .95
S0165	Skill in collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	2.4, 2.5, 2.6, 2.7, 4.4, 4.6, 6.6	4	100% or 1
	Summary		**3**	**95% or .95**

NCWF JOB ROLE

Forensics Analyst

Job Role Description: A Forensics Analyst conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Forensics Analyst. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CHFI Objectives	NICE Proficiency	Relational Coefficient
T0067	Develop architectures or system components consistent with technical specifications.	Develop	N/A	N/A	N/A
T0076	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.	Develop, Synthesize	2.2	**3**	75% or .75
T0096	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, and public relations professionals).	Construct, Create	2.3, 14.5, 14.6, 14.8	2	95% or .95
T0115	Identify information technology (IT) security program implications of new technologies or technology upgrades.	Comprehension	N/A	N/A	N/A
T0146	Manage the compilation, cataloging, caching, distribution, and retrieval of data.	Manage	N/A		
T0484	Document the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.	Synthesize	2.6, 4.3	**1**	30% or .3
T0220	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Synthesize	2.2	3	60% or .6
T0235	Translate functional requirements into technical solutions.		N/A		
T0273	Develop and document supply chain risks for critical system elements, as appropriate.	Develop, Synthesize	2.2, 13.1	3	60% or .6
T0297	Identify applications and operating systems of a network device based on network traffic.	Comprehension	7.2, 7.3, 7.6	**2**	50% or .5
T0398	Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.	Comprehension, Synthesize	11.7	3	80% or .8
T0401	Maintain deployable cyber defense toolkit (e.g. specialized cyber defense software/ hardware) to support IRT mission.	Manage	N/A	N/A	N/A
T0403	Read, interpret, write, modify, and execute simple scripts (e.g., PERL, VBS) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).	Interpret, Perform	N/A	N/A	N/A

NCWF JOB ROLE

Forensics Analyst

Job Role Description: A Forensics Analyst conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Forensics Analyst. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CHFI Objectives	NICE Proficiency	Relational Coefficient
T0411	Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.	Identify	N/A	N/A	N/A
T0425	Analyze organizational cyber policy.	Analyze	2.2, 13.1	**3**	90% or .9
T0421	Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files).	Synthesize	2.6, 4.3, 13.1	**2**	50% or .5
T0424	Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.	Analyze	10.6	**2**	60% or .6
T0440	Captures and integrates essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Create	N/A	N/A	N/A
T0482	Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.	Analyze	N/A	N/A	N/A
T0490	Install and configure database management systems and software.	Apply	N/A	N/A	N/A
T0507	Oversee installation, implementation, configuration, and support of system components.	Apply	N/A	N/A	N/A
T0274	Create auditable evidence of security measures.	Create	1.3, 4.1, 4.2, 4.3	**3**	80% or .8
T0059	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the internet.	Creating	1.4,1.5, 2.5, 4.2, 4.3, 4.7, 5.3, 6.1, 6.2,	**3**	80% or .8
T0541	Trace system requirements to design components and perform gap analysis.	Apply	N/A	N/A	N/A
T0558	Analyze user needs and requirements to plan and conduct system development.	Analyze	N/A	N/A	N/A
T0078	Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications.	Creating, Synthesis	2.2, 13.1	**2**	30% or .3
T0427	Analyze user needs and requirements to plan architecture.	Analyze	N/A	N/A	N/A
T0402	Effectively allocate storage capacity in the design of data management systems.	Analyze	N/A	N/A	N/A

NCWF JOB ROLE

Forensics Analyst

Job Role Description: A Forensics Analyst conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Forensics Analyst. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CHFI Objectives	NICE Proficiency	Relational Coefficient
T0419	Acquire and maintain a working knowledge of constitutional issues relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.	Synthesize	2.2, 7.2, 12.8, 13.1	**3**	80% or .8
T0420	Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).	Evaluate	11.1	**2**	80% or .8
T0542	Translate proposed capabilities into technical requirements.	Translate	N/A	N/A	
T0308	Analyze incident data for emerging trends.	Analyze	2.2, 3.8.	**2**	80% or .8
T0447	Design hardware, operating systems, and software applications to adequately address requirements.	Design	N/A	N/A	N/A
	Summary			**3**	**95% or .95**

NCWF JOB ROLE

Forensics Analyst

Job Role Description: A Forensics Analyst conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Forensics Analyst. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	5.5, 7.1, 3.3	2	50% or .5
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	N/A		
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	2.3, 7.2, 12.8, 13.7, 7.3, 1.4, 1.5, 14.3, 14.4,	3	50% or .5
K0004	* Knowledge of cybersecurity principles.	7.1,	3	95% or .95
K0005	* Knowledge of cyber threats and vulnerabilities.	8.3, 8.4, 10.2, 11.2, 13.1 8.2, 8.8	4	95% or .95
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	N/A		
K0017	Knowledge of concepts and practices of processing digital forensic data.	9.5, 9.7, 9.8, 7.2, 7.5, 7.6, 7.8, 4.5	4	95% or .95
K0021	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.	4.4	3	90% or .9
K0042	Knowledge of incident response and handling methodologies.	1.6, 2.4	2	95% or .95
K0060	Knowledge of operating systems.	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8	4	100% or 1
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	8.2, 8.3, 8.4, 8.8	3	80% or .8
K0077	Knowledge of server and client operating systems.	8.1, 8.2	4	95% or .95
K0078	Knowledge of server diagnostic tools and fault identification techniques.	N/A		
K0099	Knowledge of the common networking protocols (e.g., TCP/IP), services (e.g., web, mail, Domain Name Server), and how they interact to provide network communications.	7.1	3	80% or .8
K0109	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	3.3	4	95% or .95

NCWF JOB ROLE

Forensics Analyst

Job Role Description: A Forensics Analyst conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Forensics Analyst. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	3.6	4	95% or .95
K0118	Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody).	2.5, 2.6	4	95% or .95
K0119	Knowledge of hacking methodologies in Windows or Unix/Linux environment.	8.4, 7.1, 10.1, 13.1	3	90% or .9
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	6.1 to 6.8, 7.1	3	95% or .95
K0123	Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence).	1.5	4	95% or .95
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	5.3, 2.5, 4.2, 13.8	4	95% or .95
K0128	Knowledge of types and collection of persistent data.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 5.3, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6	2	50% or .5
K0131	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.	6.3	3	85% or .8
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	6.2, 6.4, 6.5, 6.6, 6.8, 7.2	4	95% or .95
K0133	Knowledge of types of digital forensics data and how to recognize them.	1.5	3	80% or .8
K0134	Knowledge of deployable forensics.	2.3, 2.5, 2.6, 2.7	2	40% or .4
K0145	Knowledge of security event correlation tools.	7.3	3	80% or .8
K0155	Knowledge of electronic evidence law.	2.3, 7.2, 12.8, 13.7	4	95% or .95
K0156	Knowledge of legal rules of evidence and court procedure.	2.8, 14.8	4	95% or .95
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	N/A		
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	2.3, 7.2, 12.8, 13.7	3	90% or .9

NCWF JOB ROLE

Forensics Analyst

Job Role Description: A Forensics Analyst conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Forensics Analyst. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	7.1	3	90% or .9
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	3.8, 13.8	4	95% or .95
K0183	Knowledge of reverse engineering concepts.	11.1 to 11.8	1	10% or .1
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8	4	95% or .95
K0185	Knowledge of common forensics tool configuration and support applications (e.g., VMWare, WIRESHARK).	7.6	3	80% or .8
K0186	Knowledge of debugging procedures and tools.	11.7	2	50% or .5
K0187	Knowledge of how different file types can be used for anomalous behavior.	3.8	2	50% or .5
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	11.7	2	50% or .5
K0189	Knowledge of virtual machine aware malware, debugger aware malware, and packing.	11.8	2	50% or .5
K0305	Knowledge of encryption algorithms, stenography, and other forms of data concealment.	5.2, 5.3, 5.4, 5.5, 5.6	3	80% or .8
S0032	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.	N/A		
S0046	Skill in performing packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	7.6	4	95% or .95
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	2.7, 7.4, 11.7	4	95% or .95
S0062	Skill in analyzing memory dumps to extract information.	6.2	3	80% or .8
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	13.8, 5.3, 6.2	3	80% or .8
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	5.3	3	80% or .8
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	5.3, 2.5, 4.2, 13.8	4	95% or .95
S0069	Skill in setting up a forensic workstation.	2.3, 13.7	4	95% or .95
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	3.8	3	85% or .85

NCWF JOB ROLE

Forensics Analyst

Job Role Description: A Forensics Analyst conducts deep-dive investigations on computer-based crimes establishing documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by a Forensics Analyst. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
S0073	Skill in using virtual machines.	3.6, 6.1	3	80% or .8
S0074	Skill in physically disassembling PCs.	N/A		
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8	4	95% or .95
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	11.1, 11.3, 11.5, 11.6, 11.7	3	90% or .9
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	9.5, 9.7, 9.8	3	85% or .85
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	2.7, 11.7	2	60% or .6
S0090	Skill in analyzing anomalous code as malicious or benign.	11.6, 11.7	3	80% or .8
S0091	Skill in analyzing volatile data.	4.2, 6.1, 6.7	4	95% or .95
S0092	Skill in identifying obfuscation techniques.	11.7	3	80% or .8
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.	11.7	2	60% or .6
A0005	Ability to decrypt digital data collections.	5.4	2	40% or .4
	Summary		**3**	**90% or .9**

NCWF JOB ROLE

Cyber Defense Forensics Analyst

Job Role Description: A Cyber Defense Forensics Analyst analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by this job role. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CHFI Objectives	NICE Proficiency	Relational Coefficient
T0027	Conduct analysis of log files, evidence, and other information in order to determine best methods for identifying the perpetrator(s) of a network intrusion.	Analyze	7.2, 7.5, 7.6, 7.8	4	95% or .95
T0036	Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.	Evaluate, Analyze	11.7	3	95% or .95
T0048	Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CD, PDA, mobile phones, GPS, and all tape formats.	Create	4.1, 4.2, 4.3, 4.4, 4.6, 4.7	4	90% or .9
T0049	Decrypt seized data using technical means.	Compute, Infer	5.2, 5.3, 5.4	1	90% or .9
T0075	Provide technical summary of findings in accordance with established reporting procedures.	Evaluate	14.1, 14.3, 14.4, 14.7	4	100% or 1
T0087	Ensure chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.	Evaluate	2.6, 4.4, 7.4	4	100% or 1
T0103	Examine recovered data for information of relevance to the issue at hand.	Evaluate	2.7, 5.3, 12.6	4	95% or .95
T0113	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Identify	4.5	3	95% or .95
T0165	Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.	Perform, Analyze	11.7	2	80% or .8
T0167	Perform file signature analysis.	Perform, Analyze	3.8	3	95% or .95
T0168	Perform hash comparison against established database.	Perform, Analyze	2.7	2	100% or 1
T0172	Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).	Perform, Analyze	4.2, 6.2, 6.4	3	100% or 1
T0173	Perform timeline analysis.	Perform, Analyze	7.1 to 7.4	3	95% or .95

NCWF JOB ROLE

Cyber Defense Forensics Analyst

Job Role Description: A Cyber Defense Forensics Analyst analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by this job role. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CHFI Objectives	NICE Proficiency	Relational Coefficient
T0175	Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).	Perform, Apply	N/A		
T0179	Perform static media analysis.	Perform, Analyze	3.1 to 3.8	3	95% or .95
T0182	Perform tier 1, 2, and 3 malware analysis.	Perform, Analyze	11.1, 11.3, 11.5, 11.6, 11.7	2	90% or .9
T0190	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).	Perform, Apply	4.4, 4.5	3	95% or .95
T0212	Provide technical assistance on digital evidence matters to appropriate personnel.	Provide	1.5, 3.1 to 3.8	1	95% or .95
T0216	Recognize and accurately report forensic artifacts indicative of a particular operating system.	Analyze	3.5, 14.1	4	95% or .95
T0240	Capture and analyze network traffic associated with malicious activities using network monitoring tools.	Perform, Analyze	7.4, 7.5, 7.6	4	100% or 1
T0241	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Apply	5.3, 2.5, 4.2, 13.8	3	100% or 1
T0253	Conduct cursory binary analysis.	Perform, Analyze	7.4, 9.8	2	100% or 1
T0279	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.	Explain	14.5, 14.8	3	95% or .95
T0285	Perform virus scanning on digital media.	Perform, Analyze	11.3	3	100% or 1
T0286	Perform file system forensic analysis.	Perform, Analyze	3.8, 3.1, 3.2	4	95% or .95
T0287	Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).	Perform, Analyze	2. 7, 4.4	4	95% or .95
T0288	Perform static malware analysis.	Perform, Analyze	11.7	4	95% or .95
T0289	Utilize deployable forensics tool kit to support operations as necessary.	Perform, Apply	4.7	2	100% or 1
T0312	Coordinate with intelligence analysts to correlate threat assessment data.	Analyze	2.3, 2.4, 7.3	2	95% or .95

NCWF JOB ROLE

Cyber Defense Forensics Analyst

Job Role Description: A Cyber Defense Forensics Analyst analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by this job role. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

TASK

ID	Statement	Bloom's Action Verbs	CHFI Objectives	NICE Proficiency	Relational Coefficient
T0396	Process image with appropriate tools depending on analyst's goals.	Perform, Analyze	13.8	2	95% or .95
T0397	Perform Windows registry analysis.	Perform, Analyze	6.2	3	100% or 1
T0398	Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.	Perform, Analyze	11.7	3	95% or .95
T0399	Enter media information into tracking database (e.g. Product Tracker Tool) for digital media that has been acquired.	Analyze	2.5	3	80% or .8
T0400	Correlate incident data and perform cyber defense reporting.	Analyze	7.3, 7.7, 2.8, 3.8	4	100% or 1
T0401	Maintain deployable cyber defense toolkit (e.g. specialized cyber defense software/ hardware) to support IRT mission.	Perform, Analyze	N/A		
T0432	Collect and analyze intrusion artifacts (e.g., source code, malware, and system con-figuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Analyze	11.1, 11.3, 11.6, 11.7	4	95% or .95
T0532	Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.	Evaluate	6.1, 6.7	4	95% or .95
T0543	Use data carving techniques (e.g., FTK-Foremost) to extract data for further analysis.	Apply	13.8	4	95% or .95
T0546	Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.	Create, Prepare	2.8, 4.8, 14.3	4	95% or .95
	Summary			**3**	**95% or .95**

NCWF JOB ROLE

Cyber Defense Forensics Analyst

Job Role Description: A Cyber Defense Forensics Analyst analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by this job role. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
K0001	* Knowledge of computer networking concepts and protocols, and network security methodologies.	5.5, 7.1, 3.3	3	50% or 5
K0002	* Knowledge of risk management processes (e.g., methods for assessing and mitigating risk).	N/A		
K0003	* Knowledge of national and international laws, regulations, policies, and ethics as they relate to cybersecurity.	2.3, 7.2, 12.8, 13.7, 7.3, 1.4, 1.5, 14.3, 14.4	3	50% or 5
K0004	* Knowledge of cybersecurity principles.	7.1	3	95% or .95
K0005	* Knowledge of cyber threats and vulnerabilities.	8.3, 8.4, 10.2, 11.2, 13.1 8.2, 8.8	3	95% or .95
K0006	* Knowledge of specific operational impacts of cybersecurity lapses.	N/A		
K0018	Knowledge of encryption algorithms (e.g., Internet Protocol Security [IPSEC], Advanced Encryption Standard [AES], Generic Routing Encapsulation [GRE], Internet Key Exchange [IKE], Message Digest Algorithm [MD5], Secure Hash Algorithm [SHA], Triple Data Encryption Standard [3DES]).	2.7, 3.6, 5.4, 5.5	2	95% or .95
K0021	Knowledge of data backup, types of backups (e.g., full, incremental), and recovery concepts and tools.	4.4	3	90% or .9
K0042	Knowledge of incident response and handling methodologies.	1.6, 2.4	2	95% or .95
K0060	Knowledge of operating systems.	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8	4	95% or .95
K0070	Knowledge of system and application security threats and vulnerabilities (e.g., buffer overflow, mobile code, cross-site scripting, Procedural Language/Structured Query Language [PL/SQL] and injections, race conditions, covert channel, replay, return-oriented attacks, malicious code).	8.2, 8.3, 8.4, 8.8	3	95% or .95
K0077	Knowledge of server and client operating systems.	8.1, 8.2	4	90% or .9
K0078	Knowledge of server diagnostic tools and fault identification techniques.	N/A		
K0099	Knowledge of the common networking protocols (e.g., TCP/IP), services (e.g., web, mail, Domain Name Server), and how they interact to provide network communications.	7.1	3	90% or .9

NCWF JOB ROLE

Cyber Defense Forensics Analyst

Job Role Description: A Cyber Defense Forensics Analyst analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by this job role. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
K0109	Knowledge of basic physical computer components and architectures, including the functions of various components and peripherals (e.g., CPUs, Network Interface Cards, data storage).	3.3	4	95% or .95
K0117	Knowledge of file system implementations (e.g., New Technology File System [NTFS], File Allocation Table [FAT], File Extension [EXT]).	3.6	4	95% or .95
K0118	Knowledge of processes for seizing and preserving digital evidence (e.g., chain of custody).	2.5, 2.6	4	100% or 1
K0119	Knowledge of hacking methodologies in Windows or Unix/Linux environment.	8.4, 7.1, 10.1, 13.1	3	90% or .9
K0122	Knowledge of investigative implications of hardware, Operating Systems, and network technologies.	6.1 to 6.8, 7.1	3	90% or .9
K0123	Knowledge of legal governance related to admissibility (e.g., Federal Rules of Evidence).	1.5	4	95% or .95
K0125	Knowledge of processes for collecting, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	5.3, 2.5, 4.2, 13.8	4	100% or 1
K0128	Knowledge of types and collection of persistent data.	4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 5.3, 6.1, 6.2, 6.3, 6.4, 6.5, 6.6	2	95% or .95
K0131	Knowledge of web mail collection, searching/analyzing techniques, tools, and cookies.	6.3	3	95% or .95
K0132	Knowledge of which system files (e.g., log files, registry files, configuration files) contain relevant information and where to find those system files.	6.2, 6.4, 6.5, 6.6, 6.8, 7.2	4	95% or .95
K0133	Knowledge of types of digital forensics data and how to recognize them.	1.5	3	95% or .95
K0134	Knowledge of deployable forensics.	2.3, 2.5, 2.6, 2.7	2	90% or .9
K0145	Knowledge of security event correlation tools.	7.3	3	90% or .9
K0155	Knowledge of electronic evidence law.	2.3, 7.2, 12.8, 13.7	4	90% or .9
K0156	Knowledge of legal rules of evidence and court procedure.	2.8, 14.8	4	90% or .9

NCWF JOB ROLE

Cyber Defense Forensics Analyst

Job Role Description: A Cyber Defense Forensics Analyst analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by this job role. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
K0167	Knowledge of basic system administration, network, and operating system hardening techniques.	N/A		
K0168	Knowledge of applicable laws (e.g., Electronic Communications Privacy Act, Foreign Intelligence Surveillance Act, Protect America Act, search and seizure laws, civil liberties and privacy laws), statutes (e.g., in Titles 10, 18, 32, 50 in U.S. Code), Presidential Directives, executive branch guidelines, and/or administrative/criminal legal guidelines and procedures relevant to work performed.	2.3, 7.2, 12.8, 13.7	3	90% or .9
K0179	Knowledge of network security architecture concepts including topology, protocols, components, and principles (e.g., application of defense-in-depth).	7.1	3	90% or .9
K0182	Knowledge of data carving tools and techniques (e.g., Foremost).	3.8, 13.8	4	90% or .9
K0183	Knowledge of reverse engineering concepts.	11.1 to 11.8	1	90% or .9
K0184	Knowledge of anti-forensics tactics, techniques, and procedures.	5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8	4	90% or .9
K0185	Knowledge of common forensics tool configuration and support applications (e.g., VMWare, WIRESHARK).	7.6	3	90% or .9
K0186	Knowledge of debugging procedures and tools.	11.7	2	90% or .9
K0187	Knowledge of how different file types can be used for anomalous behavior.	3.8	2	90% or .9
K0188	Knowledge of malware analysis tools (e.g., Oily Debug, Ida Pro).	11.7	2	90% or .9
K0189	Knowledge of virtual machine aware malware, debugger aware malware, and packing.	11.8	2	90% or .9
K0224	Knowledge of system administration concepts for Unix/Linux and/or Windows operating systems.	N/A		
K0254	Knowledge of binary analysis.	9.5, 9.7, 9.8	3	90% or .9
K0255	Knowledge of network architecture concepts including topology, protocols, and components.	7.1	3	90% or .9
K0301	Knowledge of packet-level analysis using appropriate tools (e.g., Wireshark, tcpdump).	7.6	4	90% or .9

NCWF JOB ROLE

Cyber Defense Forensics Analyst

Job Role Description: A Cyber Defense Forensics Analyst analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by this job role. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
K0304	Knowledge of basic concepts and practices of processing digital forensic data.	2.7	3	90% or .9
K0347	Knowledge and understanding of operational design	N/A		
S0032	Skill in developing, testing, and implementing network infrastructure contingency and recovery plans.	N/A		
S0047	Skill in preserving evidence integrity according to standard operating procedures or national standards.	2.7, 7.4, 11.7	4	90% or .9
S0062	Skill in analyzing memory dumps to extract information.	6.2	3	90% or .9
S0065	Skill in identifying and extracting data of forensic interest in diverse media (i.e., media forensics).	13.8, 5.3, 6.2	3	90% or .9
S0067	Skill in identifying, modifying, and manipulating applicable system components within Windows, Unix, or Linux (e.g., passwords, user accounts, files).	5.3	3	90% or .9
S0068	Skill in collecting, processing, packaging, transporting, and storing electronic evidence to avoid alteration, loss, physical damage, or destruction of data.	5.3, 2.5, 4.2, 13.8	4	90% or .9
S0069	Skill in setting up a forensic workstation.	2.3, 13.7	4	90% or .9
S0071	Skill in using forensic tool suites (e.g., EnCase, Sleuthkit, FTK).	3.8	3	90% or .9
S0073	Skill in using virtual machines.	3.6, 6.1	3	90% or .9
S0074	Skill in physically disassembling PCs.	N/A		
S0075	Skill in conducting forensic analyses in multiple operating system environments (e.g., mobile device systems).	6.1, 6.2, 6.3, 6.4, 6.5, 6.6, 6.7, 6.8, 13.1, 13.2, 13.3, 13.4, 13.5, 13.6, 13.7, 13.8	4	90% or .9
S0087	Skill in deep analysis of captured malicious code (e.g., malware forensics).	11.1, 11.3, 11.5, 11.6, 11.7	3	90% or .9
S0088	Skill in using binary analysis tools (e.g., Hexedit, command code xxd, hexdump).	9.5, 9.7, 9.8	3	90% or .9

NCWF JOB ROLE

Cyber Defense Forensics Analyst

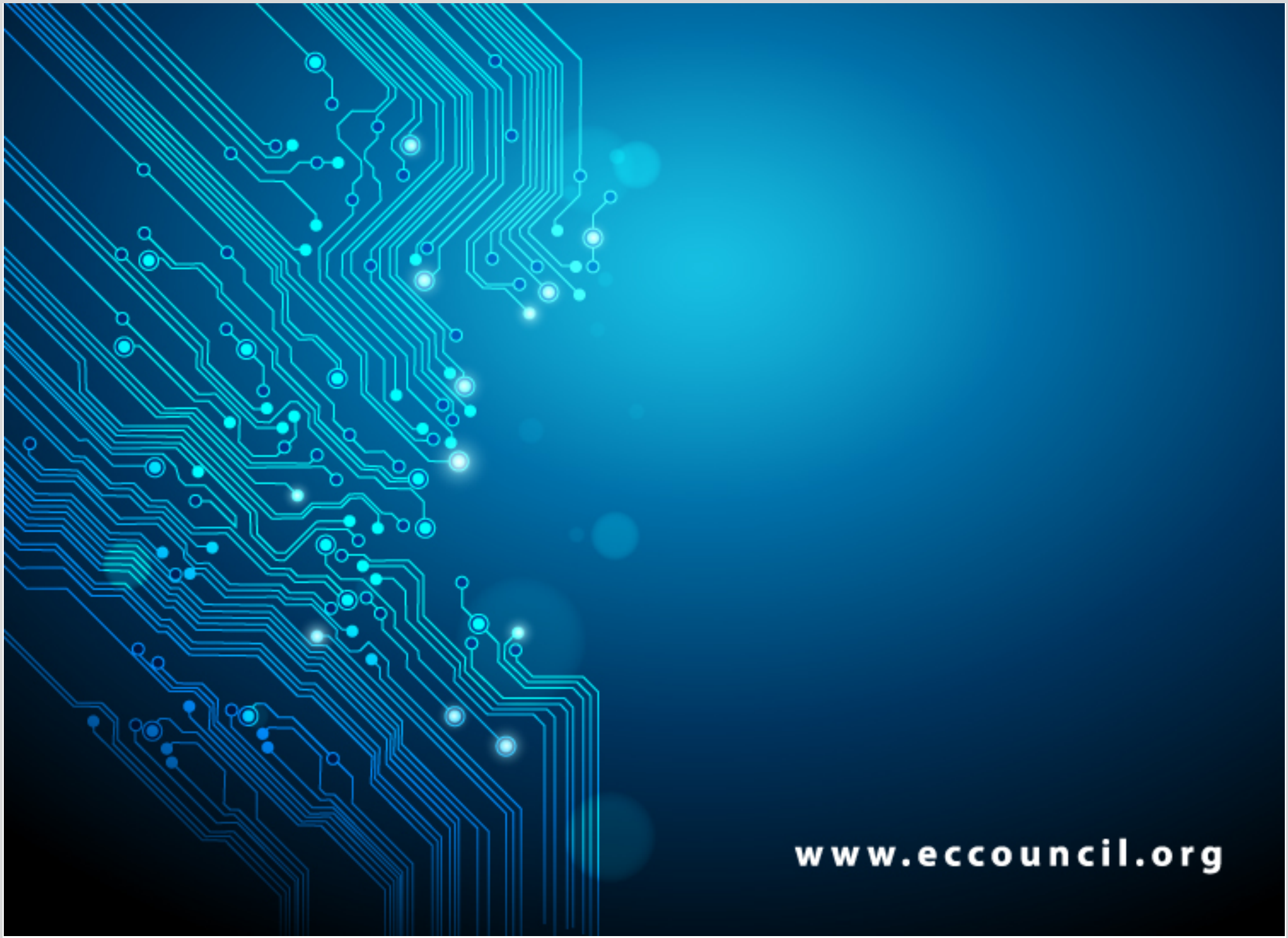
Job Role Description: A Cyber Defense Forensics Analyst analyzes digital evidence and investigates computer security incidents to derive useful information in support of system/network vulnerability mitigation.

Maps To: Computer Hacking Forensic Investigator (CHFI)

Mapping Summary: Performance-based learning and evaluation in CHFI imparts specific KSAs that should be demonstrated by this job role. CHFI maps to this job role at a Specialist level (level 3) with a correlation coefficient of .95 on the Framework tasks and a correlation coefficient of .9 on the KSA proficiency descriptions.

KSA

ID	Statement	CHFI Objectives	NICE Proficiency	Relational Coefficient
S0089	Skill in one-way hash functions (e.g., Secure Hash Algorithm [SHA], Message Digest Algorithm [MD5]).	2.7, 11.7	2	90% or .9
S0090	Skill in analyzing anomalous code as malicious or benign.	11.6, 11.7	3	90% or .9
S0091	Skill in analyzing volatile data.	4.2, 6.1, 6.7	4	90% or .9
S0092	Skill in identifying obfuscation techniques.	11.7	3	90% or .9
S0093	Skill in interpreting results of debugger to ascertain tactics, techniques, and procedures.	11.7	2	90% or .9
S0131	Skill in analyzing malware.	11.3, 11.7	3	90% or .9
S0132	Skill in conducting bit-level analysis.	N/A		
S0133	Skill in processing digital evidence, to include protecting and making legally sound copies of evidence.	2.5	3	90% or .9
A0005	Ability to decrypt digital data collections.	5.4	2	90% or .9
A0043	Ability to conduct forensic analyses in and for both Windows and Unix/Linux environments.	6.1-6.8	4	90% or .9
	Summary		**3**	**90% or .9**


www.eccouncil.org