Pathways to a Satisfying Career in IT and Cybersecurity

An information session exploring how Network+, Security+, CySA+, and CISA certifications can open doors to rewarding technical, analytical, and audit-focused cybersecurity roles across private sector, government, and regulated industries.

SECURITY OPERATIONS

Security Operations & Analyst Roles

Security operations roles form the frontline defense against cyber threats. These positions involve continuous monitoring, threat detection, and incident response to protect organizational assets.

Core Analyst Positions

- Cybersecurity Analyst
- Security Analyst
- SOC Analyst (Tier I / Tier II)

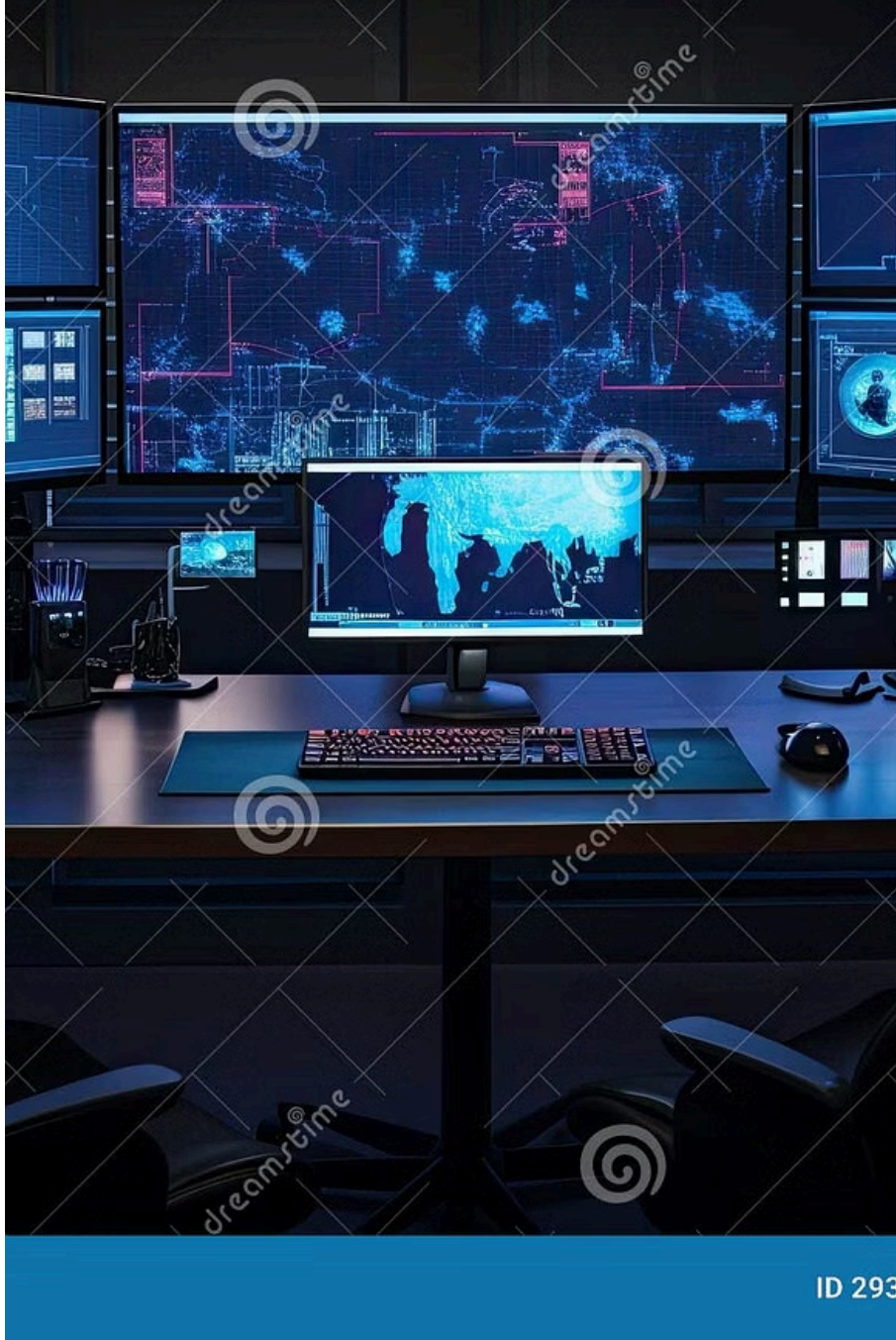
Specialized Defense Roles

- Cyber Defense Analyst
- Threat Detection Analyst
- Blue Team Analyst

Response Operations

- Incident Response Analyst

Leading the charge when security incidents occur



AUDIT & COMPLIANCE

Audit, Risk & Compliance (GRC) Roles

GRC professionals ensure organizations meet regulatory requirements and maintain robust security controls. These roles combine technical knowledge with policy expertise, making them essential in regulated industries and government sectors.

Key Responsibilities:

- Evaluating security controls and compliance frameworks
- Conducting audits and risk assessments
- Third-party vendor security reviews

Audit Specialists

Information Systems Auditor, IT Auditor, Cybersecurity Auditor

Risk Analysts

GRC Analyst, Risk & Compliance Analyst, Third-Party Risk Analyst

Controls Assessment

Information Assurance Analyst, Security Controls Assessor (SCA)

INFRASTRUCTURE SECURITY

Network & Infrastructure Security Roles

Network security professionals protect the backbone of organizational IT systems. These roles require deep understanding of network architecture, protocols, and security technologies to defend against sophisticated threats targeting infrastructure.

Network Security Analyst

Monitors and secures network traffic, implements firewalls, and manages intrusion detection systems to prevent unauthorized access.

Infrastructure Security Analyst

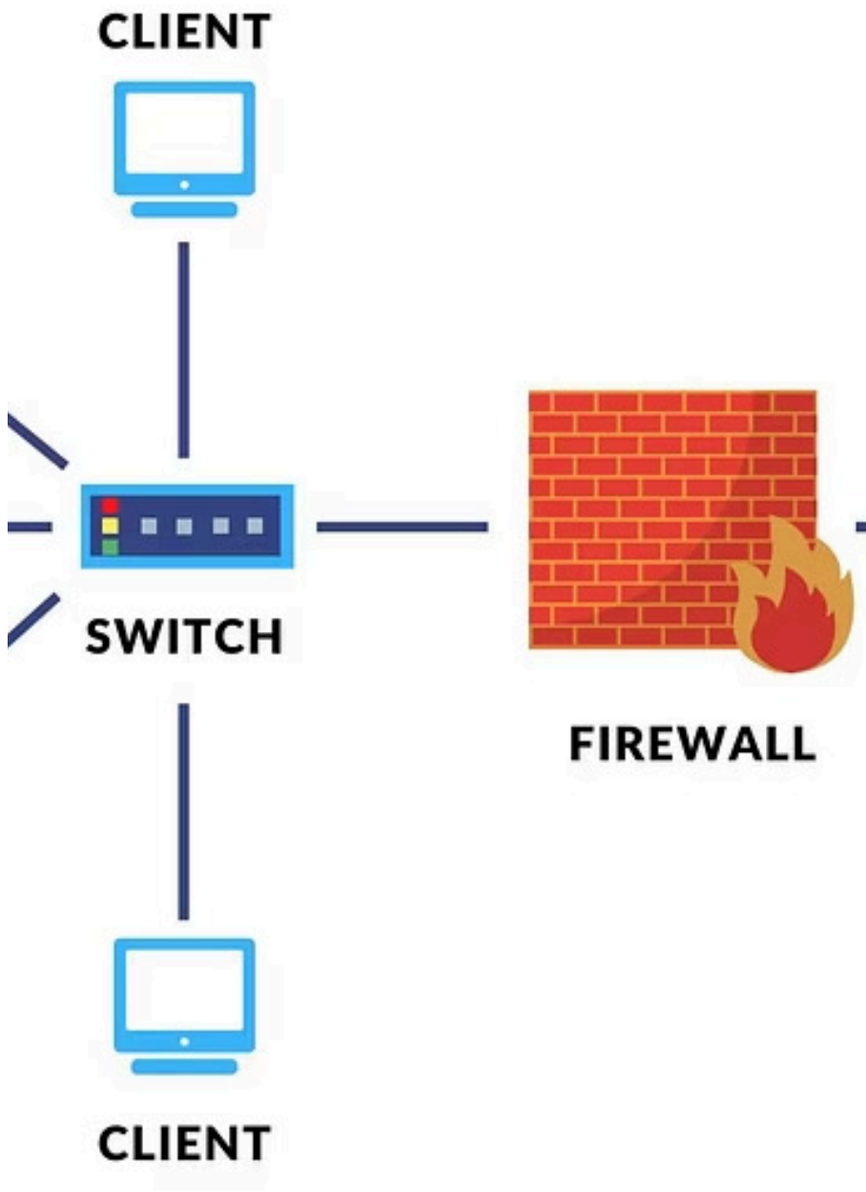
Focuses on protecting servers, databases, and cloud infrastructure with security controls and continuous monitoring.

Network Defense Analyst

Specializes in defensive strategies, threat hunting, and implementing security measures across network layers.

Security Operations Engineer

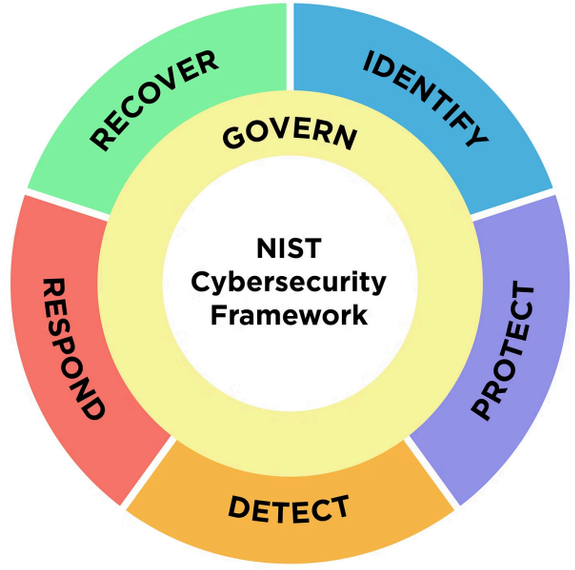
Junior-level role combining operational security with engineering tasks to maintain and improve security systems.



GOVERNMENT & DOD

Governance, Policy & Assurance Roles

Government and Department of Defense positions emphasize compliance with federal security frameworks, particularly NIST Risk Management Framework (RMF) and DoD directives. These roles are critical for maintaining security authorization and accreditation.



01

Information Assurance Specialist

Ensures systems meet security requirements and maintain authorization

02

RMF Analyst

Implements Risk Management Framework processes for federal systems

03

Security Control Assessor

Evaluates NIST controls and documents compliance status

04

Cyber Policy Analyst

Develops and interprets cybersecurity policies and procedures

CONSULTING

Consulting & Advisory Roles

Cybersecurity consulting offers variety and exposure to diverse organizations and challenges. Consultants assess security posture, recommend improvements, and help clients implement best practices across technology, processes, and governance.

Cybersecurity Consultant

Junior to mid-level positions advising clients on security strategy, architecture, and implementation. Requires strong communication skills alongside technical expertise.

IT Risk Consultant

Evaluates technology risks, develops mitigation strategies, and helps organizations align security investments with business objectives.

Security Assessment Consultant

Conducts comprehensive security assessments, penetration testing coordination, and vulnerability management programs for client organizations.

Cyber Risk Analyst

Quantifies cyber risk exposure, develops risk metrics, and provides data-driven recommendations for security program improvements.

CAREER ENTRY

Entry-to-Mid Level Titles

Starting your cybersecurity career often means beginning with entry-level or associate titles. These positions provide foundational experience while you build specialized skills. Experience requirements typically range from 0-3 years, with progression based on demonstrated capabilities.

Junior Cybersecurity Analyst

First step into security operations, learning monitoring, analysis, and response fundamentals under senior guidance.

Associate Information Security Analyst

Broader security responsibilities including policy implementation, user training, and security tool administration.

Associate IT Auditor

Supporting audit teams in control testing, evidence gathering, and compliance documentation preparation.

Cybersecurity Specialist

Focused expertise in specific security domains, ready for independent project work and technical decision-making.

DOD 8140 / 8570

Federal & Contractor-Aligned Titles

Department of Defense directive 8140 (formerly 8570) establishes certification requirements for cybersecurity positions. Your certification stack directly qualifies you for multiple DoD work roles, making you competitive for federal and contractor positions.

Cybersecurity Analyst (CSSP Analyst)

Cyber Security Service Provider role focused on protecting and defending DoD systems

Information Assurance Analyst (IAT / IAM)

Technical and management roles ensuring system security across classification levels

Security Controls Assessor (SCA)

Independent evaluation of security control effectiveness for authorization decisions

RMF Cybersecurity Analyst

Specialized in Risk Management Framework implementation and continuous monitoring

CERTIFICATION STRATEGY

Why These Certifications Work Well Together

Your certification portfolio creates a powerful combination that demonstrates comprehensive cybersecurity knowledge. Each credential builds upon the others, covering the full spectrum from foundational networking through advanced audit and analysis capabilities.

Network+

Strong networking and infrastructure foundation essential for understanding security at the protocol level

Security+

Baseline cybersecurity knowledge aligned with DoD 8140 requirements for government positions

CySA+

Detection, analysis, and incident response skills for SOC and threat hunting roles

CISA

Audit, controls, and compliance expertise focused on NIST frameworks and risk management

DC SALARY DATA

Security Operations & Analyst Roles

Washington, DC Metro Area Compensation

The Washington, DC metropolitan area offers competitive compensation for cybersecurity professionals, driven by high concentration of government agencies, defense contractors, and regulated industries. Salaries reflect the region's elevated cost of living and strong demand for qualified security talent.

$120K

Entry-Level Median

Cybersecurity Analyst with baseline certifications and 0-2 years experience

$140K

Mid-Level Average

Security Analyst with 3-5 years experience and specialized skills

$150K+

Senior Positions

Experienced analysts with advanced responsibilities and team leadership

Cybersecurity Specialist roles typically range from **$120,000 to $140,000+** annually, reflecting more focused security responsibilities and technical depth.

AUDIT & GRC SALARIES

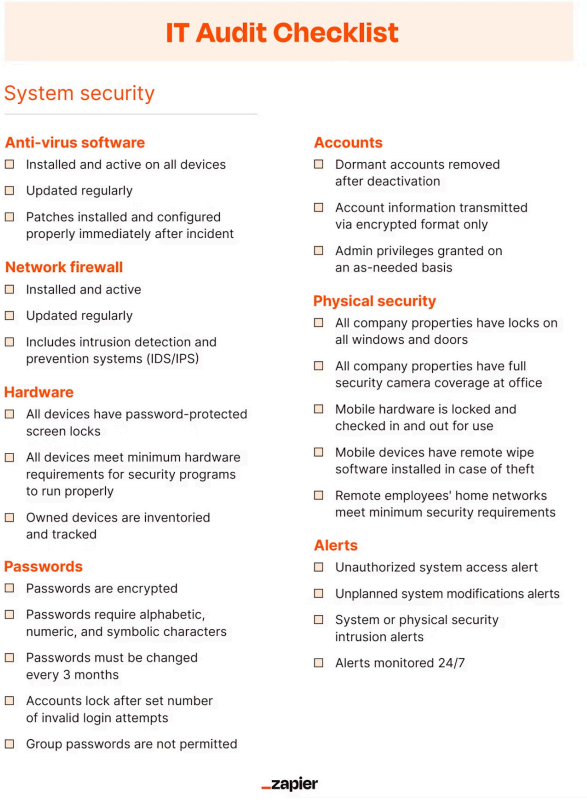
IT & Security Auditing / GRC Roles

DC Area Compensation for Audit Professionals

CISA certification significantly enhances earning potential in audit and governance roles. These positions command premium compensation due to specialized knowledge requirements and the critical nature of compliance work in government and regulated sectors.

Information Systems / IT Auditor

- Average base: **$90,000 – $105,000** annually
- With CISA + experience: **$105,000 – $130,000+**
- Senior auditors can exceed **$140,000**



IT Audit Checklist

System security

Anti-virus software
- ☐ Installed and active on all devices
- ☐ Updated regularly
- ☐ Patches installed and configured properly immediately after incident

Network firewall
- ☐ Installed and active
- ☐ Updated regularly
- ☐ Includes intrusion detection and prevention systems (IDS/IPS)

Hardware
- ☐ All devices have password-protected screen locks
- ☐ All devices meet minimum hardware requirements for security programs to run properly
- ☐ Owned devices are inventoried and tracked

Passwords
- ☐ Passwords are encrypted
- ☐ Passwords require alphabetic, numeric, and symbolic characters
- ☐ Passwords must be changed every 3 months
- ☐ Accounts lock after set number of invalid login attempts
- ☐ Group passwords are not permitted

Accounts
- ☐ Dormant accounts removed after deactivation
- ☐ Account information transmitted via encrypted format only
- ☐ Admin privileges granted on an as-needed basis

Physical security
- ☐ All company properties have locks on all windows and doors
- ☐ All company properties have full security camera coverage at office
- ☐ Mobile hardware is locked and checked in and out for use
- ☐ Mobile devices have remote wipe software installed in case of theft
- ☐ Remote employees' home networks meet minimum security requirements

Alerts
- ☐ Unauthorized system access alert
- ☐ Unplanned system modifications alerts
- ☐ System or physical security intrusion alerts
- ☐ Alerts monitored 24/7

_zapier

$150K

Cyber Security Auditor Median

DC metro median for combined audit and security expertise

$175K+

Senior Audit Positions

Experienced auditors with specialized industry knowledge

$125K

Entry Audit Range Start

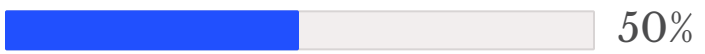
Starting compensation for cybersecurity auditors in DC

GRC COMPENSATION

Compliance, Risk & Governance Roles

DC Market Rates for GRC Professionals

Governance, Risk, and Compliance positions span a wide salary range based on experience level and responsibility scope. Entry-level GRC analysts start lower but can rapidly progress as they develop specialized knowledge in frameworks like NIST, ISO, and regulatory requirements.



Entry-Level Range

$70K-$90K for early-career GRC analysts building foundational experience

Experienced Professional

$90K-$120K+ with proven expertise in risk frameworks and compliance programs

Senior GRC Specialist

$120K+ for roles with program ownership and strategic responsibilities

Information Assurance and RMF Analyst positions, common in federal contracting, typically start around **$100,000+** depending on clearance level and specific duties.

FEDERAL EMPLOYMENT

Federal & Contract Pay Scales

Government Service (GS) Locality Compensation

Federal cybersecurity positions operate under the General Schedule (GS) pay system with DC locality adjustments. Most cybersecurity analysts and related positions fall within GS-12 through GS-14 grades, with advancement based on performance, time in grade, and increasing responsibilities.

GS-12

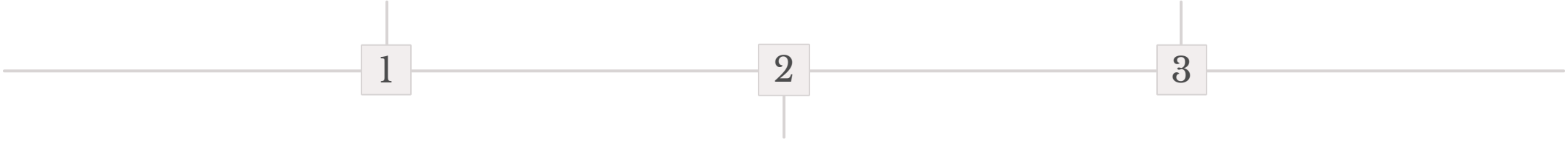
Entry-level federal cyber positions: **~$95,000-$115,000** with DC locality pay

GS-13

Experienced analysts and specialists: **~$115,000-$140,000** with progression through steps

GS-14

Senior positions and team leads: **~$135,000-$155,000+** at higher steps



Federal positions often include additional benefits: comprehensive health insurance, pension systems (FERS), Thrift Savings Plan matching, generous leave policies, and job security. Total compensation value exceeds base salary significantly.

SALARY SUMMARY

DC Metro Area Salary Overview

Role Category	Typical Salary Range (DC Metro)
Entry Cyber Analyst / SOC Analyst	~$110K – $130K
Cybersecurity Specialist	~$120K – $140K
IT/Information Systems Auditor	~$90K – $130K
Cyber Security Auditor	~$125K – $175K
Risk / GRC Analyst	~$70K – $120K
Federal Cyber / Audit Specialist (GS)	~$95K – $155K+

These ranges reflect current market conditions in the Washington, DC metropolitan area. Actual compensation varies based on specific employer, security clearance level, years of experience, specialized skills, and whether the position is private sector, federal government, or contractor-based.

YOUR PATH FORWARD

What This Means for Your Career

Your certification portfolio positions you competitively across multiple high-demand career tracks in the DC metro area. Each credential strengthens your candidacy for different role types while the combination demonstrates comprehensive cybersecurity knowledge.

Core SOC & Analyst Roles

Network+ and Security+ qualify you for security operations positions with above-average local salaries, giving you entry into the cybersecurity field with strong foundational credentials.

Detection & Analysis Positions

CySA+ adds valuable detection, analysis, and incident response capabilities, positioning you for SOC analyst roles with mid-range pay growth and advancement opportunities.

Audit, Risk & Compliance Track

CISA opens doors to audit and governance roles that can rival or exceed core analyst salaries, particularly valuable in DC's contracting and federal markets where compliance expertise is highly sought.

> The DC metropolitan area offers exceptional opportunities for cybersecurity professionals. Your certification foundation, combined with practical experience and continuous learning, positions you for a rewarding and financially stable career protecting critical systems and information assets.