A/CCRF

AKYLADE

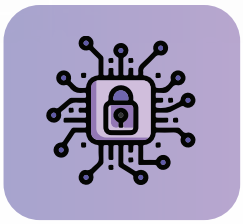
AKYLADE

CYBER RESILIENCE FUNDAMENTALS

EXAM NUMBER : CRF-002

The AKYLADE Certified Cyber Resilience Fundamentals (A/CCRF) [CRF-002] certification is designed to test your theoretical knowledge of the NIST Cybersecurity Framework (CSF) version 2.0 and how to plan, manage, and optimize the framework for use within your own organization. This includes

- Origin and original purpose of the framework
- Applicability of the framework across industries and sectors
- Three fundamental parts of the framework: the core, the implementation tiers, and the profiles
- Six functions (Govern, Identify, Protect, Detect, Respond, and Recover), 22 categories, and 106 subcategories
- Purpose, utility, and intended use of the implementation tiers, profiles, and informative references





DOMAIN 1	DOMAIN 2	DOMAIN 3	DOMAIN 4	DOMAIN 5
Framework Concepts (25%)	Framework Core (30%)	Implementation Tiers (10%)	Framework Profiles (15%)	Risk Management (20%)

Domain 1: Framework Concepts (25%)

Candidates must be able to understand the key concepts related to the NIST Cybersecurity Framework version 2.0

1.1 Identify key terms related to the NIST Cybersecurity Framework (2 questions)

- Cybersecurity
- Information security
- Information systems security
- Information assurance
- Cyber resilience
- Cybersecurity incident
- Stakeholder
- Supplier
- Critical infrastructure
- Threats
- Vulnerabilities
- Confidentiality
- Integrity
- Availability
- Non-repudiation
- Authentication

1.2 Summarize key aspects of the NIST Cybersecurity Framework (4 questions)

- Purpose of the NIST Cybersecurity Framework
- Components of the NIST Cybersecurity Framework
  - Framework core • Framework profiles • Implementation tiers
- Six functions of the NIST Cybersecurity Framework
  - Govern • Identify • Protect • Detect • Respond • Recover

1.3 Summarize how the NIST Cybersecurity Framework is different than other frameworks and certifications (3 questions)

- Applicable sectors and industries
  - Government
  - Healthcare
  - Financial services
  - Energy
  - Manufacturing
  - Retail
  - Transportation
  - Critical infrastructure
- Characteristics of the framework
  - Voluntary set of guidelines
  - Flexibility and adaptivity
  - Focus on risk instead of technical controls
  - Focus on risk instead of compliance requirements
  - Facilitate communication and collaboration
  - Continually improved and evolving
- Other frameworks and informative references
  - International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 and 27002
  - National Institute of Standards and Technology (NIST) Special Publications (SP 800-37, SP 800-53, SP-800-171, SP 800-218, and SP 800-221A)
  - Cyber Risk Institute (CRI) Profile
  - Center for Internet Security (CIS) Critical Security Controls
  - ITIL

- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards
- Federal Risk and Authorization Management Program (FedRAMP)
- Open Web Application Security Project (OWASP)
- Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Registry

1.4 Explain the benefits of achieving cyber resilience to key stakeholders (1 question)

- Development of the NIST Cybersecurity Framework
- History of the NIST Cybersecurity Framework
  - Executive Order 13636
  - Executive Order 13800
  - Executive Order 14028
  - Cybersecurity Enhancement Act of 2014
  - Relevance of NIST Cybersecurity Framework to contemporary cyber risks
  - Federal Information Security Modernization Act (FISMA) of 2014
  - Cybersecurity Information Sharing Act

Domain 2: Framework Core (30%)

Candidates must be able to understand the framework core as it relates to the NIST Cybersecurity Framework version 2.0

2.1 Explain the importance of the framework core (2 questions)

- Purpose of the framework core
- Usage of the framework core
- Benefits of the framework core
- Effectiveness of the framework core

2.2 Explain how categories are utilized with the six functions (5 questions)

- Govern (GV)
  - Organizational Control (GV.OC)
  - Risk Management Strategy (GV.RM)
  - Oversight (GV.OV)
  - Roles, Responsibilities, and Authorities (GV.RR)
  - Policy (GV.PO)
  - Cybersecurity Supply Chain Risk Management (GV.SC)
- Identify (ID)
  - Asset Management (ID.AM)
  - Risk Assessment (ID.RM)
  - Improvement (ID.IM)
- Protect (PR)
  - Identity Management, Authentication, and Access Control (PR.AA)
  - Awareness and Training (PR.AT)
  - Data Security (PR.DS)
  - Platform Security (PS.PR)
  - Technology Infrastructure Resilience (PR.IR)

- Detect (DE)
  - Continuous Monitoring (DE.CM)
  - Adverse Event Analysis (DE.AE)
- Respond (RS)
  - Incident Management (RS.MA)
  - Incident Analysis (RS.AN)
  - Incident Mitigation (RS.MI)
  - Incident Response Repoting and Communications (RS.CO)
- Recover (RC)
  - Incident Recovery Plan Execution (RC.RP)
  - Incident Recovery Communications (RC.CO)

2.3 Explain how subcategories are utilized with the six functions (3 questions)

- Govern (GV)
  - Organizational Control (GV.OC)
  - Risk Management Strategy (GV.RM)
  - Oversight (GV.OV)
  - Roles, Responsibilities, and Authorities (GV.RR)
  - Policy (GV.PO)
  - Cybersecurity Supply Chain Risk Management (GV.SC)
- Identify (ID)
  - Asset Management (ID.AM)
  - Risk Assessment (ID.RM)
  - Improvement (ID.IM)
- Protect (PR)
  - Identity Management, Authentication, and Access Control (PR.AA)
  - Awareness and Training (PR.AT)
  - Data Security (PR.DS)
  - Platform Security (PS.PR)
  - Technology Infrastructure Resilience (PR.IR)
- Detect (DE)
  - Continuous Monitoring (DE.CM)
  - Adverse Event Analysis (DE.AE)
- Respond (RS)
  - Incident Management (RS.MA)
  - Incident Analysis (RS.AN)
  - Incident Mitigation (RS.MI)
  - Incident Response Reporting and Communications (RS.CO)
- Recover (RC)
  - Incident Recovery Plan Execution (RC.RP)
  - Incident Recovery Communications (RC.CO)

2.4 Summarize how the NIST Cybersecurity Framework outcomes are related to controls provided by other publications (2 questions)

- International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001 and 27002
- National Institute of Standards and Technology (NIST) Special Publications (SP 800-37, SP 800-53, SP 800-171, SP 800-218, and SP 800-221A)
- Cyber Risk Institute (CRI) Profile
- Center for Internet Security (CIS) Critical Security Controls
- Payment Card Industry Data Security Standard (PCI-DSS)
- Health Insurance Portability and Accountability Act (HIPAA)
- North American Electric Reliability Corporation (NERC) Critical Infrastructure Protection (CIP) Standards
- Federal Risk and Authorization Management Program (FedRAMP)
- Open Web Application Security Project (OWASP)
- Cloud Security Alliance (CSA) Security, Trust, Assurance, and Risk (STAR) Registry
- ITIL

Domain 3: Implementation Tiers (10%)

Candidates must be able to understand the implementation tiers as they relate to the NIST Cybersecurity Framework version 2.0

3.1 Explain how implementation tiers are utilized in the NIST Cybersecurity Framework, including how they differ from a maturity model (1 question)

- NIST Cybersecurity Framework implementation tiers
- ISO/IEC 27001
- Capability Maturity Model Integration (CMMI)
- Cybersecurity Capability Maturity Model (C2M2)
- Cybersecurity Maturity Model Certification (CMMC)

3.2 Given a scenario, analyze an organization's implementation tier based on its current cybersecurity posture (2 questions)

- Tier 1 (Partial)
- Tier 2 (Risk Informed)
- Tier 3 (Repeatable)
- Tier 4 (Adaptive)

3.3 Given a scenario, recommend strategies for moving an organization between implementation tiers (1 question)

- Assess the current state
- Define the target state
- Develop a plan of action
- Implement the plan of action
- Monitor and adjust

Domain 4: Framework Profiles (15%)

Candidates must be able to understand the framework profiles as they relate to the NIST Cybersecurity Framework version 2.0

4.1 Summarize how profiles are used to tailor the NIST Cybersecurity Framework for varying risk management strategies (3 questions)

- Key components of a profile
  - Core functions
  - Categories
  - Subcategories
- Utilizing profiles
- Current profile versus target profile
- Map profiles to an organization's cybersecurity posture

4.2 Given a scenario, utilize a profile to tailor the NIST Cybersecurity Framework to specific organizational needs (2 questions)

- Tailor profiles to support risk management strategies
- Tailor profiles to support regulatory compliance requirements
- Utilize profiles to measure an organization's cybersecurity posture over time
- Identify relevant core functions, categories, and subcategories

4.3 Explain the use of profiles in the NIST Cybersecurity Framework (1 question)

- Profile templates
- Sector-specific profiles
  - Cyber Risk Institute (CRI) profile
  - Manufacturing Profile
  - Election Infrastructure Profile
  - Satellite Networks Profile
  - Smart Grid Profile
  - Connected Vehicle Profiles
  - Payroll Profile
  - Maritime Profile
  - Communications Profile

Domain 5: Risk Management (20%)

Candidates must be able to understand the key concepts related to risk management

5.1 Explain the fundamentals of risk management (2 questions)

- Risk analysis
  - Qualitative
    - Likelihood of a risk
    - Impact of a risk
  - Quantitative
    - Single-loss expectancy (SLE)
    - Annualized loss expectancy (ALE)
    - Annualized rate of occurrence (ARO)
  - Hybrid
- Risk appetite
- Risk tolerance
- Business impact analysis
  - Recovery time objective (RTO)
  - Recovery point objective (RPO)
  - Mean time to repair (MTTR)
  - Mean time between failures (MTBF)
  - Single point of failure
  - Mission essential functions
  - Identifying critical systems
- Financial analysis
  - Total cost of ownership (TCO)
  - Return on investment (ROI)
  - Return on assets (ROA)

5.2 Given a scenario, determine the appropriate risk response to a given threat or vulnerability (2 Questions)

- Risk Responses
  - Acceptance
  - Avoidance
  - Transference
  - Mitigation
- Types of Risk
  - Inherent risk
  - Residual risk
- Risk Register

5.3 Given a scenario, assess cybersecurity risk and recommend risk mitigations (4 Questions)

- Identify threats to an organization
- Identify vulnerabilities to an organization
- Identify risks to an organization
- Recommend specific risk mitigations
- Determine benefits of a particular risk mitigation
- Determine the trade-offs of a particular risk mitigation
- Evaluate the effectiveness of a particular risk mitigation
- Develop a risk management plan
- Develop a cybersecurity strategy