AKYLADE

Cyber Risk Management Foundation™ (A/CRMF™) Exam Objectives

Exam Code: CRF-001

EXAM DETAILS

EXAM NAME	AKYLADE Cyber Risk Management Foundation™ (A/CRMF™)
QUESTION ITEMS	CRF-001
QUESTION ITEMS	50 multiple-choice questions
DURATION	60 minutes
PASSING SCORE	700 points on a scale of 100 to 900 points

EXAM DOMAINS

	DOMAIN	EXAM COVERAGE
1.0	Risk Management Concepts	14%
2.0	Risk Strategy and Governance	23%
3.0	Risk Identification and Analysis	22%
4.0	Risk Response and Mitigation	25%
5.0	Risk Monitoring and Communication	16%

IMPORTANT NOTE:

AKYLADE continuously reviews and updates exam content to ensure that exams remain current, relevant, and secure. When necessary, AKYLADE may publish updated exams based on the existing exam objectives, but all related exam preparation materials will remain valid during a given exam's lifecycle. Under each objective, a list of bulleted examples has been provided to aid candidates during their studies. These lists are not exhaustive and serve as examples of technologies, processes, regulations, or tasks related to the relevant objective. Other examples may appear on the exam, even if they are not listed directly under the objective in this document.

DOMAIN 1: Risk Management Concepts (14%)

1.1 Summarize the risk management lifecycles, frameworks, and processes.

- Risk management lifecycle
  - Identify
  - Analyze
  - Prioritize
  - Treat
  - Monitor
  - Communicate
  - Document
- Risk management framework (NIST 800-37)
  - Prepare
  - Categorize
  - Select
  - Implement
  - Assess
  - Authorize
  - Monitor
- Risk management process (NIST SP 800-39)
  - Frame
  - Assess
  - Respond
  - Monitor
- ISO 27001
  - Define risk assessment methodology
  - Complete inventory of assets
  - Perform asset classification
  - Identify threats
  - Identify vulnerabilities
  - Evaluate risk
  - Treat risk
  - Document and report
  - Review and monitor

1.2 Explain the types of risk and risk responses which can be utilized by an organization.

- Risk responses
  - Acceptance
  - Avoidance
  - Transference
  - Mitigation
  - Exploitation
  - Enhancement
  - Sharing
  - Escalation
- Types of risk
  - Inherent risk
  - Residual risk
  - Control risk
  - Systemic risk
  - Operational risk
  - Strategic risk
  - Compliance risk
- Risk register
  - Risk identifier
  - Risk description
  - Risk probability (likelihood)
  - Risk consequence (impact)
  - Risk categorization
  - Risk prioritization
  - Risk owner
  - Risk response
  - Status

1.3 Given a scenario, conduct a qualitative, quantitative, or hybrid risk analysis.

- Qualitative risk analysis
  - Likelihood of a risk (risk probability)
  - Impact of a risk (risk consequence)
  - Ability to detect (speed of response)
  - Risk matrix
  - Risk categorization
  - Risk prioritization
  - Techniques
    - Interviews
    - Focus groups
    - Expert judgment
    - Delphi technique
    - SWOT analysis
    - Scenario analysis
- Quantitative risk analysis
  - Factor analysis of information risk (FAIR)
  - Single-loss expectancy (SLE)
    - Asset value (AV)
    - Exposure factor (EF)
  - Annualized loss expectancy (ALE)
  - Annualized rate of occurrence (ARO)
  - Value at risk (VAR)
  - Conditional value at risk (CVAR)
  - Loss distribution approach (LDA)
- Hybrid risk analysis

1.4 Explain the importance of training and awareness programs to mitigate risk within an organization.

- Provide annual cyber security awareness training
  - Remote work policies
  - Mobile device policies
  - Password management
  - Multi-factor authentication
  - Phishing
  - Pre-texting
  - Malware
- Secure software development lifecycle (SDLC) training
  - Secure coding best practices
  - Security testing best practices
  - DevSecOps integration
  - Open source security
  - Regulatory and compliance requirements
- Develop compliance training and awareness programs
- Incorporate risk management training into organizational processes
- Assess the effectiveness of organizational training

2.1 Given a scenario, explain how common threats and vulnerabilities may affect an organization's risk posture.

- Hostile cyber and physical attack risks
  - Unauthorized logical access to systems
  - Unauthorized physical access to systems
  - Distributed denial of service (DDoS) attacks
  - Malware (viruses, worms, Trojan horses)
  - Advanced persistent threats (APTs)
  - Ransomware
- Human errors and omissions risks
  - Accidental data deletion
  - Misconfiguration of a system's security
  - Unintentional disclosure of sensitive information
  - Use of default configurations
  - Poor password management
  - Ineffective use of multi-factor authentication
- Environmental and natural disaster risks
  - Earthquakes
  - Floods
  - Fires
  - Hurricanes
  - Power outages
- Supply chain risks
  - Counterfeit hardware/software
  - Tampered hardware/software
  - Poor manufacturing practices
  - Unauthorized production
  - Unknown security practices of external partners
  - Insecure integrations with third-party systems
- Internal organizational risks
  - Insider threats (malicious employees)
  - Espionage
  - Theft of physical devices
  - Social engineering attacks
- Technical risks
  - Software bugs or flaws
  - Lack of hardware-based security features
  - Hardware failures
  - Network failures
  - Outdated or unsupported software
  - Insecure network protocols or infrastructure
  - Technical debt
- Political, legal, and regulatory risks
  - Non-compliance with laws and regulations
  - Penalties for data breaches
  - Intellectual property theft
  - Changes in laws, tariffs, and governments
  - Embargoes and trade restrictions
  - Expropriate and nationalization of assets
- Reputational risks
  - Public perception of trustworthiness
  - Customer belief in quality or reliability
- Third-party and outsourcing risks
  - Dependency on external vendors
  - Third-party data breaches
  - Service provider vulnerabilities
  - Data confidentiality, integrity, and authenticity risks
  - Data corruption
  - Unauthorized data modification
  - On-path attacks
  - Lack of encryption use
    - Data-at-rest
    - Data-in-motion
    - Data-in-processing
- Operational technology (OT) and industrial control systems (ICS)
  - Insufficient system segmentation
  - Unsecure protocols
  - Weak authentication mechanisms
  - Poor user privilege management
  - Lack of real-time monitoring
  - Poorly understood system designs
  - Inadequate incident response plans

2.2 Given a scenario, identify assumptions that affect how risk is assessed, responded to, and monitored within the organization.

- Business impact analysis
- Recovery time objective (RTO)
- Recovery point objective (RPO)
- Maximum tolerable downtime (MTD)
- Work recovery time (WRT)
- Mean time to repair (MTTR)
- Mean time between failures (MTBF)
- Single point of failure (SPOF)
- Mission essential functions (MEF)
- Identifying critical systems
- Service level agreement (SLA)
- Impact categories
  - Operational
  - Financial
  - Legal
  - Reputational
  - Regulatory
- Financial analysis
  - Total cost of ownership (TCO)
  - Return on investment (ROI)
  - Return on assets (ROA)
  - Net present value (NPV)
  - Internal rate of return (IRR)
  - Cost-benefit analysis (CBA)
  - Payback period

2.3 Summarize constraints on the conduct of risk assessment, risk response, and risk monitoring activities within the organization.

- Financial
- Legal
  - General data protection regulation (GDPR)
  - California consumer privacy act (CCPA)
  - Health insurance portability and accountability act (HIPAA)
- Regulatory
- Contractual
- Organizational
- Governance structure
- International standards and guidelines
  - NIST cybersecurity framework
  - NIST risk management framework
  - ISO 27001/27002
  - PCI DSS
  - SOC 2

2.4 Given a scenario, identify the level of risk tolerance for an organization.

- Risk tolerance
  - Based on organizational culture
  - Different for each type of loss/compromise
  - Directly influenced by leaders/executives
- Risk appetite
- Risk profile
  - Organizational
  - Departmental
- Risk culture
- Risk capacity
- Risk threshold
- Risk aggregation
- Risk compounding

2.5 Given a scenario, consider the priorities and trade-offs considered by an organization when managing risk.

- Balancing risk reduction and the cost of controls
- Prioritizing and allocating limited resources
- Achieving compliance while maintaining flexibility
- Operational efficiency versus additional security measures
- Increased innovation while maintaining system stability
- Short-term goals versus long-term strategic objectives
- Risk appetite and risk tolerance versus potential opportunities
- Stakeholder perspectives and priorities

2.6 Explain how a comprehensive organizational risk management strategy is developed.

- Purpose of a strategy
- Elements of a strategy
    - Risk identification
    - Risk assessment
    - Risk response
    - Risk monitoring
- Integrating risk strategy
    - Into organizational processes
    - Into decision-making
- Supporting mission and business functions
- Implementing mechanisms for continuous improvement
- Role of senior leaders, executives, and stakeholders

DOMAIN 3: Risk Identification and Analysis (22%)

3.1 Given a scenario, identify threats and vulnerabilities in organizational information systems and the environments in which they operate.

- Threat modeling
  - MITRE ATT&CK framework
  - STRIDE
  - OCTAVE
  - PASTA
  - Attack trees
- Common vulnerabilities and exposures (CVE)
- Analyze network traffic
- Analyze log data
- Analyze results of physical security audits
- Review organizational security policies and procedures
- Identify operational technology (OT) and information technology (IT) interconnections

3.2 Given a scenario, determine the risk to organizational operations, assets, and personnel when a threat exploits a vulnerability.

- Common vulnerability scoring system (CVSS)
- Custom software development
- Development and operations (DevOps)
- Continuous integration and continuous deployment (CI/CD) pipelines
- Personnel security programs

3.3 Summarize the use of vulnerability assessment and penetration testing to validate the potential threats against known vulnerabilities.

- Automated tools
  - Vulnerability scanners
  - Network analyzers
  - Web application scanners
  - Automated exploitation toolsets
  - Configuration management toolsets
  - Phishing campaigns
- Manual techniques
  - Social engineering
  - Code reviews
  - Physical security testing
  - Custom exploit development

3.4 Given a scenario, analyze and prioritize security risks based on their likelihood of occurrence and impact to the organization's operations.

- Enterprise networks
- Wired
- Wireless
- Appliances
- Devices
- End-user workstations
- Mobile devices
- BYOD
- CYOD
- COPE
- COBO
- Remote access technologies
- Cloud computing
- Single vendor environments
- Multi-cloud environments
- Virtualized devices and networks
- Containerized systems
- Internet of things (IoT)
- Operational technology (OT)
- Industrial control systems (ICS)
- Supervisory control and data acquisition (SCADA)
- Cryptographic technologies
- Virtual and augmented reality
- Artificial intelligence
- Machine learning
- Social media platforms

3.5 Given a scenario, conduct assessments for new and existing systems.

- Asset inventory assessment
- Privacy impact assessment (PIA)
- Security risk assessment
- Physical security assessment
- Operational technology/Industrial control system risk assessment
- Cloud migration and pre-deployment assessment
  - Software as a service (SaaS)
  - Platform as a service (PaaS)
  - Infrastructure as a service (IaaS)
- Compliance assessment
- SOC 2 assessment
  - Description of a system (DoS)
- ISO/IEC 27001 assessment
  - Statement of applicability (SoA)
- Biometric implementation assessment
  - False rejection rate (FRR)
  - False acceptance rate (FAR)
  - Crossover error rate (CER)
- Third-party vendor assessment
- Social engineering

3.6 Given a scenario, assess an organization's data loss prevention strategy and systems.

- Purpose of the system
- Effectiveness of the system implementation
- Data identification and classification system
  - Sensitivity
  - Importance
  - Boundaries of the system
- Success metrics for the system
- Business requirements
  - Organizational needs
  - Organizational priorities
  - Data types to protect
    - Regulated data
    - Sensitive data
    - Intellectual property
    - Personally identifiable information (PII)
- Regulatory and compliance requirements

DOMAIN 4: Risk Response and Mitigation (25%)

4.1 Given a scenario, identify an appropriate risk response for a given risk determined during a risk assessment.

- Risk acceptance
- Risk avoidance
- Risk transference
- Risk mitigation

4.2 Given a scenario, evaluate alternative courses of action for responding to a given risk.

- Cost-benefit analysis
- Feasibility
- Resource availability
- Impact on business objectives
- Effectiveness of risk response
- Considerations
  - Compliance
  - Legal
  - Stakeholders
  - Risk appetite
  - Risk tolerance

4.3 Given a scenario, determine the appropriate measures and controls for responding to a given risk.

- Administrative controls
- Technical (logical) controls
- Physical controls
- Deterrent controls
- Preventative controls
- Detective controls
- Corrective controls
- Compensating controls

4.4 Given a scenario, implement the course of action selected to respond to a given risk.

- Develop a remediation plan
- Allocate resources
- Create a plan of actions and milestones (POA&M)
- Communicate with stakeholders
- Deploy measures and controls

AKYLADE

4.5 Given a scenario, develop an incident response plan, business continuity plan, or continuity of operations plan to address potential incidents.

- Incident response plans (IRP)
  - Purpose
  - Roles
  - Life cycle
    - Preparation
    - Detection & analysis
    - Containment, eradication, & recovery
    - Post-incident activity
  - Regulatory requirements
  - Operational technology considerations
  - Drills and simulations
- Business continuity plan (BCP)
  - Business impact analysis (BIA)
  - Backup strategies
  - Recovery strategies
  - Drills and simulations
- Continuity of operations plan (COOP)
  - Alternative sites
    - Hot sites
    - Warm sites
    - Cold sites
    - Mobile sites
    - Cloud sites
  - Drills and simulations

4.6 Evaluate the effectiveness of current risk mitigation measures and controls.

- Establish standard processes and procedures
- Vulnerability management
- Patch management
- Anti-virus and anti-malware solutions
- Physical security controls
- Penetration testing
- Data loss prevention system audits
- Identity and access management audits
- Conduct periodic testing of implemented measures and controls
- Report measures and controls deficiencies

DOMAIN 5: Risk Monitoring and Communication (16%)

5.1 Given a scenario, develop a risk monitoring strategy for an organization that includes the purpose, type, and frequency of monitoring activities.

- Risk exposure monitoring
  - Key risk indicator (KRI)
- Compliance monitoring
  - Metrics
  - Reporting mechanisms
- Effectiveness monitoring
  - Key performance indicator (KPI)
- Change monitoring

5.2 Given a scenario, monitor organizational information systems and environments on an ongoing basis to verify compliance, determine effectiveness of risk response measures, and identify changes.

- Design and deploy monitoring solutions
- Endpoint detection and response (EDR)
- Security information and event management (SIEM)
- Security orchestration, automation, and response (SOAR)
- Physical security measures and control monitoring solutions
- Operational technology monitoring solutions

5.3 Explain how to maintain clear communication across diverse teams and stakeholders.

- Ethical considerations
- Stakeholders
  - Roles and responsibilities
    - Responsible
    - Accountable
    - Consulted
    - Informed
  - Inform and communicate
    - Current risk posture
    - Emerging risks
    - Risk mitigation efforts
    - Measures and controls deficiencies
- Conduct an annual review of policies and standards
- Create security policy exceptions for approval
- Liaison between cybersecurity teams and regulatory bodies
- Integrate risk management
  - Project management
  - Change management
  - Service management
  - Vendor management
  - Supply chain management
- Communicate policies
  - Secure use of social media
  - Secure use of online services
- Prepare documentation
  - Risk response activities
  - Risk response decisions
  - Approved exceptions
  - Customer security questionnaires

5.4 Given a scenario, prepare for and conduct audits within an organization.

- Host kick-off meeting with stakeholders
- Create an audit artifact request list
- Develop a project plan
  - Planning
  - Execution
  - Reporting
- Prepare controls owners for audits
- Write narratives
- Create test procedures
  - Inspection
  - Observation
  - Analytical procedures
  - Produce verifiable evidence
- Conduct walkthroughs
- Conduct comprehensive security control assessments
- Create audit work products
- Organize and retain audit evidence
- Guide external auditors to remain within audit scope

5.5 Given a scenario, utilize a risk-based approach to conducting the authorization and accreditation process for information systems within an organization.

- Utilize a risk-based approach
- Define roles and responsibilities
- Review and approve new projects and technologies
- Facilitate the authorization process
- Facilitate the accreditation process
- Define procedures for reviewing and approving systems