AKYLADE

Cyber Risk Management Practitioner™ (A/CRMP™) Exam Objectives

Exam Code: CRP-001

EXAM DETAILS

EXAM NAME	AKYLADE Cyber Risk Management Practitioner™ (A/CRMP™)
QUESTION ITEMS	CRP-001
QUESTION ITEMS	40 scenario-based, multiple-choice questions
DURATION	120 minutes
PASSING SCORE	700 points on a scale of 100 to 900 points

EXAM DOMAINS

	DOMAIN	**EXAM COVERAGE**
1.0	Leading Risk Management	20%
2.0	Risk Identification and Analysis	22%
3.0	Risk Responses, Measures, and Controls	22%
4.0	Compliance and Authorization	11%
5.0	Risk Management Framework	25%

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: Leading Risk Management (20%)

1.1 Explain the creation, development, and leadership of cross-functional teams, which can effectively perform risk management functions within an organization.

- Foster culture
  - Risk awareness
  - Cyber resilience
  - Continuous improvement
  - Open communication
  - Team cohesion
  - Blame-free environment
- Manage organizational changes
  - Digital transformations
  - Successful adoptions
  - Minimize disruptions
- Plan succession of key roles
- Develop workforce
  - Identify
  - Train
  - Develop
  - Mentorship
  - Turnover
- Focus on ethical considerations
  - Management practices
  - Decision making
- Allocate and manage resources
  - Budget
  - Personnel
  - Technology
- Oversee contract negotiations

1.2 Given a scenario, develop and implement governance structures to streamline roles, responsibilities, and reporting mechanisms across an organization.

- Governance structures
  - Roles
  - Responsibilities
  - Reporting structure
    - Horizontal
    - Vertical
    - Ad hoc
- Security ambassador program
- Risk management integration across the organization
  - Strategy
  - Policies
  - Procedures
  - Processes
  - Decision-making
- Risk assessment methodologies
- Reporting frameworks
- Measurement of activities
  - Key performance indicator (KPI)
  - Critical success factor (CSF)
  - Metrics
  - Industry benchmarks

1.3 Summarize the effects that regulations, standards, and guidelines have on an organization's risk management activities.

- Regulations and contractual requirements
  - California consumer privacy act (CCPA)
  - Children's online privacy protection act (COPPA)
  - Cybersecurity information sharing act (CISA)
  - Electronic communication privacy act of 1986 (ECPA)
  - Federal information security management act (FISMA)
  - General data protection regulation (GDPR)
  - Gramm-Leach-Bliley act (GLBA)
  - Health insurance portability and accountability act (HIPAA)
  - Payment card industry data security standard (PCI DSS)
- Personal information protection and electronic documents act (PIPEDA)
- Sarbanes-Oxley Act (SOX)
- Service organization control type 2 (SOC 2)
- Service organization control type 3 (SOC 3)
- Standards and guidelines
  - NIST cybersecurity framework (CSF)
  - NIST SP 800-37r2
  - NIST SP 800-39
  - NIST SP 800-53
  - ISO/IEC 27001
  - ISO/IEC 27002
  - ISO/IEC 27017
  - ISO/IEC 27018
  - ISO/IEC 27701
  - TISAX
  - ITSG-33
  - AICPA trust services criteria (TSC)
  - Center for internet security (CIS) controls
- Compliance requirements
  - Risk identification
  - Risk assessment
  - Mitigation strategies
  - Monitoring and reporting
- Contractual requirements
  - Third-party auditing standards
    - SOC 2 type II
    - ISO 27001
    - SSAE 18
    - FedRAMP
    - StateRAMP
    - Defense federal acquisition regulation supplement (DFARS)
      - DFARS 252.204-7019
      - DFARS 252.204-7020
      - DFARS 252.204-7021
- Considerations
  - Data sovereignty
  - Penalties for non-compliance
  - Incentives for compliance

1.4 Given a scenario, effectively communicate, collaborate, and engage stakeholders about an organization's risk posture and mitigation strategies.

- Communicate
  - Organizational risk posture
  - Identified risks
  - Impact of identified risks
  - Risk mitigation efforts
  - Emerging risks
- Collaborate
  - Information sharing
  - Stakeholder buy-in
  - Best practices development
- Engage
  - Internal stakeholders
  - External stakeholders
- Unified risk management approach
  - Business units
  - Technology staff
  - Standard contractual clauses
- Work products for communication
  - Briefings
  - Dashboard
  - Executive summaries
  - Reports
  - Scorecards
  - White papers
  - Request for proposal (RFP)

1.5 Given a scenario, implement comprehensive cybersecurity training and exercises to enhance organizational risk management and improve employee awareness.

- Develop and facilitate awareness training
  - Cyber resilience
  - Cybersecurity
  - Privacy
  - Preventing social engineering
  - Risk management
- Conduct technology-specific training
  - Data loss prevention (DLP)
  - Anti-phishing campaigns
  - Passwordless authentication
- Exercise methodologies
  - Tabletop exercise
  - Checklist review
  - Parallel testing
  - Full testing
- Facilitate exercises
  - Continuity of operations
  - Disaster recovery
  - Incident response
  - Ransomware attack

1.6 Given a scenario, develop policies, guidelines, processes, and procedures to effectively implement an organization's risk management strategy.

- Access control
  - Access control auditing
  - Principle of least privilege
- Acceptable use policy
- Adopting emerging technology
- Business continuity (BC)
- Cloud security
- Configuration management
- Compliance monitoring
- Continuity of operations (COOP)
- Continuous improvement
  - Best practices
  - Feedback
  - Incident reviews
  - Lessons learned
- Data classification standard
- Data loss prevention
  - Intellectual property
  - Personally identifiable information (PII)
  - Protected health information (PHI)
  - Proprietary data
  - Sensitive information
- Deploying new technology
- Disaster recovery (DR)
- Encryption utilization
  - Data-at-rest
  - Data-in-transit
  - Data-in-use
- Identity and access management (IAM)
- Incident response
- Information security policy
- Information sharing
- Mobile devices
  - BYOD
  - COBO
  - COPE
  - CYOD
- Onboarding and offboarding personnel
- Physical security
- Privacy
- Remote work
- Social media utilization
- Supply chain management
- Third-party service providers
- Vendor selection

DOMAIN 2: Risk Identification and Analysis (22%)

2.1 Given a scenario, analyze and apply strategies to identify threats and vulnerabilities in organizational information systems and the environments in which they operate.

- Identification strategies
  - Threat modeling
    - MITRE ATT&CK framework
    - OCTAVE
    - OWASP Top 10
    - PASTA
    - STRIDE
    - Attack trees
  - Threat intelligence
    - Automated threat hunting
    - OSINT
    - Security information and event management
    - Threat intelligence feeds
    - Threat intelligence platforms
  - Common vulnerabilities and exposures (CVE)
  - Data flow diagram creation or analysis
  - Network traffic analysis
  - Log data analysis
  - Physical security audit results analysis
  - Organizational security policies and procedures review
  - Lessons learned review
  - Root cause analysis report review
- Critical infrastructure industries
  - Operational technology (OT)
  - Information technology (IT)
- Supply chain risks
- Third-party vendors and suppliers
  - External vendor questionnaires
- Third-party software and libraries
- Emerging technology risks
  - Artificial intelligence
  - Blockchain
  - Internet of things
  - Quantum computing

2.2 Given a scenario, assess and analyze how common threats and vulnerabilities may affect the risk posture of an organization's sensitive data.

- 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
  - Sabotage
- 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
        - End of life (EOL)
        - End of support (EOS)
    - Insecure network protocols or infrastructure
    - End-of-life systems
    - Legacy systems
- Legal and regulatory risks
    - Non-compliance with laws and regulations
    - Penalties for data breaches
    - Intellectual property theft
- 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
    - Inadequate incident response plans

2.3 Given a scenario, develop and implement a continuous risk assessment process that adapts to the evolving threat landscape and organizational changes.

- Automated tools
    - Automated exploitation
    - Configuration management
    - Data loss prevention
    - Endpoint detection and response
    - Mobile application management
    - Mobile device management
    - Network access control
    - Network analyzers
    - Network device discovery
    - Patch compliance
    - Phishing campaigns
    - Policy management
    - Security information and event management
    - Vulnerability scanners
    - Web application scanners
    - Wireless network scanners
- Manual techniques
    - Social engineering
    - Code reviews
    - Physical security testing
    - Custom exploit development

2.4 Given a scenario, analyze and prioritize security risks based on their likelihood of occurrence and impact to the organization's operations using quantitative, qualitative, or hybrid techniques.

- Qualitative risk analysis
  - Likelihood of a risk (risk probability)
  - Impact of a risk (risk consequence)
  - Risk matrix
  - Risk categorization
  - Risk prioritization
  - Techniques
    - Delphi technique
    - Expert judgment
    - Focus groups
    - Interviews
    - Modeling
    - Scenario analysis
    - Simulations
    - SWOT analysis
- Quantitative risk analysis
  - Single-loss expectancy (SLE)
  - 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

2.5 Given a scenario, perform assessments for new and existing systems and analyze the results to identify gaps in the organization's security posture.

- 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

2.6 Given a scenario, create a risk register to document an organization's identified risks, their characteristics, and the strategies implemented for responding to each risk.

- Components of a risk register
  - Risk identifier
  - Risk description
  - Risk probability (likelihood)
  - Risk consequence (impact)
  - Risk categorization
  - Risk prioritization
  - Risk owner
  - Risk response
  - Status

DOMAIN 3: Risk Responses, Measures, and Controls (22%)

3.1 Given a scenario, analyze and select an appropriate risk acceptance response when risk mitigation is not cost-effective or feasible.

- Air gapped systems
- BYOD use
- End-of-life hardware
- Legacy systems
- Low-impact vulnerabilities
- Low-sensitivity data
- Non-compliance with minor regulations
- Non-critical systems
- Outdated software
- Outsourcing of services
- Remote access
- Social media utilization
- Unpatched minor bugs

3.2 Given a scenario, analyze and select an appropriate risk avoidance strategy to eliminate or significantly reduce the potential for a risk to occur.

- Avoid cloud services
- Decommission vulnerable systems
- Disable unnecessary services
- Discontinue legacy application use
- Eliminate external USB access
- Insource services
- Segment the network
- Prohibit high-risk applications
- Prohibit remote access
- Restrict BYOD use
- Restrict internet access
- Uninstall unnecessary software

3.3 Given a scenario, analyze and select an appropriate risk transference response for a given risk during a risk assessment.

- Contractual agreements
    - Indemnification clause
    - Service level agreements
    - Third-party accountability
- Insurance types and coverage
    - Business interruption
    - Data breach
    - Errors and omissions (E&O)
    - Media liability
    - Network security liability
    - Privacy liability
    - Ransomware
    - Third-party liability
- Outsourcing
    - Cloud service providers
    - Managed security service providers
    - Managed service providers

3.4 Given a scenario, analyze and select appropriate risk mitigation measures and controls to reduce the likelihood or impact of identified risks.

- Access controls
- Access control lists
- Advanced threat detection and response
- Anti-virus/Anti-malware
- Application security testing
- Backup and recovery
- Cloud access security broker (CASB)
- Continuous monitoring
- Cryptographic key management
- Data loss prevention (DLP)
- Endpoint detection and response (EDR)
- Encryption
    - Data-at-rest
    - Data-in-transit
    - Data-in-processing
- Firewalls
- Identity and access management (IAM)
- Intrusion detection/protection system (IDS/IPS)
- Mobile application management (MAM)
- Mobile device management (MDM)
- Multi-factor authentication (MFA)
- Network access control (NAC)
- Network security groups
- Network segmentation
- Patch management
- Physical security measures
- Secure configuration practices
- Secure coding practices
- Security information and event management (SIEM)
- Supply chain visibility
- Web application firewall (WAF)
- Unified threat management (UTM)
- User and entity behavior analytics (UEBA)
- Virtual private cloud (VPC)
- Virtual private network (VPN)

3.5 Given a scenario, evaluate the cost-effectiveness of a proposed measure or security control.

- Initial costs
    - Purchase price
    - Installation fees
- Operational costs
    - Maintenance expenses
    - Staffing requirements
    - Training costs
- Indirect costs
    - Productivity losses
    - Downtime impact
- Lifecycle costs
    - Upgrade costs
    - Licensing fees
    - Depreciation
    - Replacement costs
- Analysis methods
    - Return on investment (ROI)
    - Risk-adjusted return on investment (RAROI)
    - Return on capital (ROC)
    - Total cost of ownership (TCO)
    - Cost-benefit analysis (CBA)
    - Payback period
    - Alternative solutions
    - Cost comparison

3.5 Given a scenario, schedule and conduct a routine risk, security, or compliance audit to assess an organization's measures and security controls against contractual requirements, regulations, or industry standards.

- Define objectives
- Schedule an audit
- Gather documentation
- Assess measures & controls
- Analyze findings
- Solicit feedback
- Prepare report
- Communicate results
- Develop plan of action
- Implement changes

DOMAIN 4: Compliance and Authorization (11%)

4.1 Given a scenario, conduct a gap assessment between an organization's current compliance state and their desired or target state against a given framework, regulation, or industry standard.

- Control objectives for information and related technologies (COBIT)
- Cybersecurity maturity model certification (CMMC)
- General data protection regulation (GDPR)
- ISO/IEC 27001
- ITIL maturity model
- NIST cybersecurity framework (CSF) profile
- Payment card industry data security standard (PCI DSS)
- Risk maturity model (RMM)
- Service organization control 2 (SOC 2)

4.2 Given a scenario, implement compliance considerations into an organization's overall cybersecurity risk management framework.

- Adapt organizational practices to requirements
- Adapt to changing regulatory landscape
- Address challenges to compliance
  - Cloud services
  - Data breach notifications
  - Export controls
  - Incident responses
  - Intellectual property
  - Legal interpretations
  - Mobile devices
  - Remote work
- Create detailed compliance checklists
- Design and implement compliance programs
  - Identify gaps
  - Ensure adherence
  - Implement action plans
  - Utilize automated toolsets
- Manage documentation and records
  - Assessments
  - Audit results
  - Dashboards
    - Percent of controls tested
    - Percent compliant
    - Remediation status
  - Gap analysis
  - Remediation actions
  - Security policies
  - Status reports
- Train workforce on compliance

4.3 Summarize internal and external auditing procedures for assessing compliance of measures and security controls.

- Internal audits
  - Purpose
  - Scope
  - Planning
  - Execution
  - Reporting
  - Remediation
- External audits
  - Purpose
  - Scope
  - Engagement with auditors
  - Documentation and evidence
  - Execution and observation
  - Findings review
  - Findings response
  - Remediation

4.4 Given a scenario, conduct authorization of systems and processes by making informed decisions about the risks associated with them.

- Define roles and responsibilities
- Document authorization decisions
- Prepare authorization packages
- Conduct risk assessments
- Integrate compliance considerations

DOMAIN 5: Risk Management Framework (25%)

5.1 Summarize the fundamental concepts associated with the Risk Management Framework (RMF).

- Steps of the risk management framework (RMF)
  - Prepare
  - Categorize
  - Select
  - Implement
  - Assess
  - Authorize
  - Monitor
- Organization-wide risk management approach
  - Level 1 - Organization
  - Level 2 - Mission/ business process
  - Level 3 - Information system
- Software development life cycle (SDLC)
  - Integrating RMF into the SDLC
- Information security
- Privacy considerations
- Information system and system elements
- Authorization boundaries
  - Complex systems
  - Software applications
  - External providers
- Requirements and controls
- Security and privacy posture
- Supply chain risk management
- Flexibility
- Timeline
- Continuous improvement
  - Best practices
  - Lessons learned
  - Feedback from stakeholders

5.2 Explain the roles and responsibilities of the key participants within various Risk Management Framework processes.

- Authorizing official
- Authorizing official designated representative
- Chief acquisition officer
- Chief information officer
- Common control provider
- Control assessor
- Enterprise architect
- Head of agency
- Information owner or steward
- Mission or business owner
- Risk executive (function)
- Security or privacy architect
- Senior accountable official for risk management
- Senior agency information security officer
- Senior agency official for privacy
- System administrator
- System owner
- System security or privacy officer
- System user
- Systems security or privacy engineer

5.3 Given a scenario, prepare an organization to manage security and privacy risks.

- Purpose of the prepare step
- Organization level tasks
    - Risk management roles
    - Risk management strategy
    - Risk assessment (organization)
    - Organizationally-tailored control baselines and cybersecurity framework profiles
    - Common control identification
    - Impact-level prioritization
    - Continuous monitoring strategy (organization)
- Information system level tasks
    - Mission or business focus
    - System stakeholders
    - Asset identification
    - Authorization boundary
    - Information types
    - Information life cycle
    - Risk assessment (system)
    - Requirements definition
    - Enterprise architecture
    - Requirements allocation
    - System registration

5.4 Given a scenario, categorize a system and the information it processes, stores, and transmits based on an impact analysis.

- Purpose of the categorize step
- Tasks
    - System description
    - Security categorization
    - Security categorization review and approval

5.5 Given a scenario, select the set of NIST SP 800-53 controls to protect the system based on a risk assessment.

- Purpose of the select step
- Tasks
    - Control selection
    - Control tailoring
    - Control allocation
    - Documentation of planned control implementations
    - Continuous monitoring strategy (system)
    - Plan review and approval

5.6 Given a scenario, implement security controls and document how the controls are deployed.

- Purpose of the implement step
- Tasks
    - Control implementation
    - Update control implementation information

5.7 Given a scenario, assess a system to determine if controls are in place, operating as intended, and producing the desired results.

- Purpose of the assess step
- Tasks
  - Assessor selection
  - Assessment plan
  - Control assessments
  - Assessment reports
  - Remediation actions
  - Plan of action and milestones

5.8 Given a scenario, make a risk-based decision to authorize a system to operate.

- Purpose of the authorize step
- Tasks
  - Authorization package
  - Risk analysis and determination
  - Risk response
  - Authorization decision
  - Authorization reporting
- Types of authorizations
  - Initial authorization
  - Ongoing authorization
  - Reauthorization
- Authorization package
  - Executive summary
  - Security and privacy plans
  - Security and privacy assessment reports
  - Plans of action and milestones
- Authorization decisions
  - Authorization to operate
  - Common control authorization
  - Authorization to use
  - Denial of authorization
- Event-driven triggers
- Significant changes
- Type authorization
- Facility authorization
- Conducting authorizations
  - Single authorizing official
  - Multiple authorizing officials
  - Joint authorizations

5.9 Given a scenario, continuously monitor the implementation of security controls and risks to a system.

- Purpose of the monitor step
- Tasks
  - System and environment changes
  - Ongoing assessments
  - Ongoing risk response
  - Authorization package updates
  - Security and privacy reporting
  - Ongoing authorization
  - System disposal