A/CCRP

AKYLADE

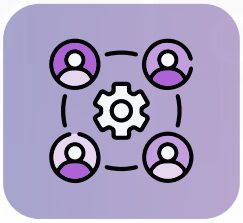
AKYLADE

CYBER RESILIENCE PRACTITIONER

EXAM NUMBER: CRP-002

The AKYLADE Certified Cyber Resilience Practitioner (A/CCRP) [CRP-002] certification is designed to test your practical knowledge of the NIST Cybersecurity Framework (CSF) version 2.0 and how to plan, implement, manage, and optimize the material aspects of the framework for use within your own organization using the Cyber Risk Management Action Plan (CR-MAP) process, including:

- Coordinating with management for organization buy-in and establishing risk profiles for organizations
- Discover top organizational cyber security risks using rigorous prioritization methods
- Create a personalized cyber security risk management strategy tailored to an organization's unique requirements
- Conduct maintenance and updating to the organization's cybersecurity risk posture and perform

DOMAIN 1	DOMAIN 2	DOMAIN 3	DOMAIN 4
CR-MAP Fundamentals 20%	CR-MAP Phase One: Determining Top Cyber Risks 36%	CR-MAP Phase Two: Create a CR-MAP 27%	CR-MAP Phase Three: Maintenance and Updates 17%

Domain 1: CR-MAP Fundamentals

Candidates must be able to explain and implement key concepts related to the CR-MAP

Objective 1.1

Explain how to best prepare for an assessment (1 question)

- Understand the target organization
- Create a project roadmap

Objective 1.2

Understand the CR-MAP process (1 question)

- Prepare needed documents
- Contextualize plans in relation to the target organization

Objective 1.3

Given a scenario, coordinate with management to achieve organizational buy-in (2 questions)

- Provide adequate answers to management questions
- Communicate potential business impacts of cyber security incidents
- Communicate complex technical topics in laymens terms
- Create communication plans to achieve buy-in

Objective 1.4

Explain the relationship between the NIST Cybersecurity Framework (CSF) version 2.0 and the Cyber Risk Management Action Plan (CR-MAP) process (1 question)

- Understand how CR-MAP questions relate to NIST Cybersecurity Framework outcomes
- Understand how CR-MAP zero to ten scale relates to the NIST Cybersecurity Framework

Objective 1.5

Given a scenario, establish risk profiles for an organization (1 question)

- Match the target organization to details in the NIST Cybersecurity Framework risk profiles

Domain 2: CR-MAP Phase One – Determining Top Cyber Risks

Candidates must be able to conduct CR-MAP Phase One actions to determine the top cyber risks that a given organization is facing

Objective 2.1

Given a scenario, determine the appropriate stakeholders and create a list of interviewees to identify cyber risks (2 questions)

- Consider their role / technical ability
- Consider their geographic location / branch

Objective 2.2

Given a scenario, conduct interviews and record responses to identify top cyber risks (2 questions)

- Present questions in unbiased manner
- Provide example answers to questions
- Record interviewee notes

Objective 2.3

Given a scenario, analyze network diagrams to identify cyber risks (1 question)

- Review subnetting/VLANs configurations
- Review Firewall/DMZ configurations
- Review VPN configurations
- Review legacy system data

Objective 2.4

Given a scenario, assess any missing details after gathering data and remediate the missing details (2 questions)

- Review qualitative data
- Review quantitative data
- Conduct additional interviews as needed

Objective 2.5

Given a scenario, create and present the top cyber risks report for the organization (1 question)

- Show the top 5 cyber risks in aggregate
- Show the top 5 cyber risks by business unit in aggregate
- Create themes to help contextualize top cyber risks
- Generate high level remediation advice for each top cyber risk item presented

Objective 2.6

Given a scenario, generate a custom questionnaire for the organization (1 question)

- Assign questions to both technical and non-technical interviewees
- Remove questions that are not applicable to target organization

Objective 2.7

Given a scenario, create charts to visually explain the top cyber risk categories to the organization (1 question)

- Create radar or spider charts
- Create bar graphs and pie charts
- Analyze raw data

Objective 2.8

Given a scenario, set the organization's target scores for alignment with the NIST Cybersecurity Framework (1 question)

- Understand how the CR-MAP zero to ten scale relates to the NIST Cybersecurity Framework
- Explain why target scores are an important aspect of goal setting

Domain 3: CR-MAP Phase Two – Create a Cyber Risk Management Action Plan

Candidates must be able to conduct CR-MAP Phase Two actions to create a Cyber Risk Management Action Plan (CR-MAP)

Objective 3.1

Given a scenario, verify how each top risk is covered by the mitigation roadmap (1 question)

Objective 3.2

Given a scenario, rate each mitigation's business value based on the Business Value Model (1 question)

- Financial returns
- Technical risk mitigation
- Legal risk mitigation
- Reliability of operations

Objective 3.3

Given a scenario, create custom mitigations based on organization questionnaire and interviews (2 questions)

Objective 3.4

Given a scenario, create standard operating procedures (SOPs) for custom mitigation and control (1 question)

- Understand and know how to implement every mitigation/control recommended to the target organization
- Recommend contractors for mitigations/controls you cannot advise on

Objective 3.5

Given a scenario, generate a cost estimate for each mitigation and control (1 question)

- Understand the common costs associated with given mitigations and controls

Objective 3.6

Given a scenario, create an implementation roadmap for the organization (2 questions)

- Assign mitigations to specific organizational units
- Group mitigations by owner type
- Generate a Gannt chart with the availability of each organizational unit
- Understand resource limitations
  - Time - Money - Skilled personnel

Domain 4: CR-MAP Phase Three – Maintenance and Updates

Candidates must be able to conduct CR-MAP Phase Three actions to maintain and update the organization's Cyber Risk Management Action Plan (CR-MAP)

Objective 4.1

Given a scenario, assist leadership in assigning mitigations and controls to internal and external parties (1 question)

Objective 4.2

Given a scenario, generate updated top cyber risk presentations as mitigations and controls are implemented (2 questions)

- Review completed mitigations
- Determine numeric score assigned to each mitigation
- Update charts and the top cyber risks with new numeric data

Objective 4.3

Given a scenario, explain which mitigations and controls have been proposed and what they accomplish (1 question)

- Understand recommended mitigations
- Understand recommended controls
  - Technical controls
  - Administrative controls
  - Physical controls
  - Preventative controls
  - Detective controls
  - Corrective controls

Objective 4.4

Given a scenario, conduct ongoing reviews and maintenance of the organization's cyber resiliency (1 question)

- Create post-assessment communication plan
- Update roadmap based on periodic reviews