Mile2 Cybersecurity Certifications – C)ISSO-A KSA Exam Blueprint

About CISSO-A

If you are looking for a comprehensive and highly regarded cybersecurity course, then the **Certified Information Systems Security Officer Accredited (CISSO-A)** is for you. The **C)ISSO-A** will prepare you with a broad range of knowledge and skills required of a security officer. However, these skills can be applied across a broad range of role-based careers.

A **C)ISSO-A** can implement and maintain cost-effective security controls that are closely aligned with business and industry standards. The **C)ISSO-A** certification course is an ideal way to increase knowledge, expertise, and skills for managers, auditors, and INFOSEC professionals.

Renowned worldwide, the **Certified Information Systems Security Officer Accredited (CISSO-A)** credential offers unparalleled validation of an individual's ability to manage and lead the security functions of an organization.

This certification ensures that professionals possess both the technical depth and managerial competence to effectively handle an organization's security strategy and operations.

The **C)ISSO-A** Common Body of Knowledge (CBK®) covers a wide array of topics, ensuring that it remains relevant to all areas within the information security field. Successful candidates will demonstrate proficiency in the following eleven domains:

- Risk Management
- Security Management
- Identification, Authentication, Authorization and Accounting
- Operations Security
- Symmetric Cryptography, Asymmetric Cryptography and Hashing
- Network Concepts, Design and Attacks
- Enterprise Security Architecture and Attacks
- Software Development Security
- Malware and Attacks
- Business Continuity
- Incident Management, Law and Ethics

Mile2 Cybersecurity Certifications – C)ISSO-A KSA Exam Blueprint

Experience Requirements

There are no minimum requirements needed to become a **Certified Information Systems Security Officer Accredited (CISSO-A)**. Candidates can pursue the **C)ISSO-A** certification without prior experience. This allows individuals from various backgrounds and levels of expertise to gain the knowledge and skills required to effectively design, engineer, and manage the overall security posture of an organization. Whether you are new to the field or looking to enhance your existing skills, the **C)ISSO-A** certification is accessible to all aspiring information security professionals.

Accreditation

C)ISSO-A was the first credential in the field of information security to meet the stringent requirements of ANSI/ISO/IEC Standard 17024.

Job Task Analysis (JTA)

Mile2 is committed to ensuring the **C)ISSO-A** certification remains relevant to its members. Regularly conducted Job Task Analyses (JTA) systematically and critically assess the tasks performed by security professionals in the **C)ISSO-A** field. The findings from these analyses are used to update the examination, ensuring that candidates are evaluated on the most pertinent topics and responsibilities faced by today's information security professionals.

C)ISSO-A Examination Information

We use ProctorU to conduct our exams. ProctorU is an online proctoring service that allows candidates to take their exams securely from any location. This service ensures the integrity of the examination process by monitoring candidates through a combination of live proctors and advanced technology. By using ProctorU, we provide flexibility and convenience while maintaining high standards of security and compliance for our certification exams.

Length of Exam	**2 Hours**
Number of items	100
Item format	Multiple choice
Passing grade	62 out of 100 points
Exam language availability	English
Testing center	ProctorU Platform

Mile2 Cybersecurity Certifications – C)ISSO-A KSA Exam Blueprint

C)ISSO-A Examination Weights

Domains	Number of Questions	Average Weight
01. Risk Management	7	7%
02. Security Management	10	10%
03. Identification, Authentication, Authorization and Accounting	11	11%
04. Operations Security	15	15%
05. Symmetric Cryptography, Asymmetric Cryptography and Hashing	8	8%
06. Network Concepts, Design and Attacks	14	14%
07. Enterprise Security Architecture and Attacks	6	6%
08. Software Development Security	10	10%
09. Malware and Attacks	4	4%
10. Business Continuity	7	7%
11. Incident Management, Law and Ethics	8	8%
	100	**100%**

CISSO-A Exam Blueprint

1. **Risk management**

    a. Risk Definitions
    b. Business Impact Analysis
    c. Risk Management
    d. Risk analysis, assessment, and scope
    e. Risk response and treatment
    f. Continuous monitoring and measurement
    g. Reporting
    h. Continuous improvement
    i. Risk frameworks

2. **Security Management**

    a. Understanding Security
    b. Information Security Management System
    c. Roles and Responsibilities
    d. Security Frameworks
    e. Human Resources
    f. Ethics
    g. Laws
    h. Due care/due diligence
    i. CIA
    j. Education of employees
    k. Select controls based upon systems security requirements
    l. Trusted Computing Base
    m. Protection Mechanisms
    n. Security Models
        i. Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)
    o. Evaluation Criteria

3. **Cryptography**

    a. Symmetric
        i. Cryptography terms
        ii. Historical Uses of Cryptography
        iii. Cryptography Foundations
        iv. Modern Cryptography
        v. Hashing

    b. Asymmetric
        i. Asymmetric Cryptography
        ii. Hybrid Cryptography
        iii. Digital Signatures
        iv. Cryptography in Use
        v. Attacks against Cryptography

4. **Identification, Authentication, Authorization, and Accounting**

    a. Identity Management
        i. Manage the identity and access provisioning lifecycle
    b. Authentication Techniques
    c. Authorization
        i. Access control types and characteristics
            1. Role-based access control (RBAC)
            2. Rule based access control
            3. Mandatory access control (MAC)
            4. Discretionary access control (DAC)
            5. Attribute-based access control (ABAC)
            6. Risk based access control
    d. Access Control Models and Techniques
    e. Access Control Methods
    f. Accounting (Monitoring, Auditing, Logging)
    g. Single Sign-On
    h. Federated identity

5. **Data Security Management**
    a. Data Lifecycle
    b. Data Discovery and Classification
    c. Data Storage Architectures and Strategies
    d. Data Security Architectures and Strategies
    e. Data Retention, Deletion, and Archival Policies
    f. Data Security Posture Management (DSPM)

6. **Operations Security**

    a. Administrative Management Responsibilities
    b. Human Resources Management
    c. Product Implementation management
    d. Redundancy and Fault Tolerance
    e. Operations Issues and Responses
    f. Threat to Operations
    g. Security Assessments
    h. Conduct logging and monitoring activities
    i. Perform Configuration Management (CM)
    j. Perform Change Management
    k. Utilize foundational security operations concepts
    l. Implement and support patch management
    m. Implement and manage physical security
    n. Database Models and Terminology
    o. Database Security Issues
    p. Artificial Intelligence

7. **Network Connections, Protocols, Devices, and Design**

    a. Network Connections
    b. Network and Communication Security
    c. Network Topologies
    d. Network Cabling
    e. LAN and WAN
    f. OSI Model
    g. Network Devices
    h. Network Security Sentries
    i. Ports, Protocols, and Services

j. Telephony
k. VPN's
l. Wireless Networks
m. Network Based Attacks

8. I.T. and Business Security Architecture

a. Business Security Architecture
    i. Frameworks
b. I.T. Architecture
c. System Threats
d. Use secure design principles
    i. Least privilege
    ii. Defense in depth
    iii. Secure defaults
    iv. Fail securely
    v. Segregation of Duties (SoD)
    vi. Keep it simple and small
    vii. Zero trust or trust but verify
    viii. Privacy by design
    ix. Shared responsibility
    x. Client-based systems
    xi. Server-based systems
    xii. Database systems
    xiii. Cryptographic systems
    xiv. Industrial Control Systems (ICS)
    xv. Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
    xvi. Distributed systems
    xvii. Internet of Things (IoT)
    xviii. Serverless
    xix. Embedded systems
    xx. High-Performance Computing systems
    xxi. Edge computing systems
    xxii. Virtualized systems

9. **Secure Software Development**

    a. Software Security Concerns
    b. Software Lifecycle Development Process
    c. Web Application Security
    d. PCI-DSS Compliance

10. **Malware and Attacks**

    a. Common Malware
    b. Attacks on Applications
    c. Attacks on Systems

11. **BCDR + IH**

    a. Disaster Recovery (DR)
        i. Project Initiation
        ii. Business Impact Analysis and Risk Assessment
        iii. Determining Recovery Strategies
        iv. Writing the Plan
        v. Preparing for the Disaster
        vi. Business Continuity Management
        vii. Test Disaster Recovery Plans (DRP)
    b. Business Continuity (BC) Planning
    c. Incident Management
        i. Computer Crime
        ii. Evidence Handling
        iii. Incident Management Process