Mile2 Cybersecurity Institute

Certified Information Systems Security Officer Accredited CISSO-A KSA Exam Blueprint (2026)

Blueprint Element	Description
Credential Name	Certified Information Systems Security Officer Accredited
Credential Abbreviation	CISSO-A
Document Type	Exam Blueprint
Revision Date	2026.04.23
Exam Length	2 hours
Number of Exam Items	100
Item Format	Multiple choice
Passing Score	62 out of 100 points
Exam Language	English
Testing Platform	ProctorU

1. Purpose of the CISSO-A Certification

The Certified Information Systems Security Officer Accredited certification validates the knowledge, skills, and abilities required to support, manage, and lead information security functions within an organization. The CISSO-A certification is designed for professionals who need to understand security governance, risk management, access control, cryptography, operations security, network security, secure software development, malware threats, business continuity, incident management, law, and ethics.

Successful candidates demonstrate the ability to understand security requirements, select appropriate controls, support organizational risk decisions, contribute to security operations, and align information security activities with business and regulatory expectations.

2. Candidate Profile

The CISSO-A certification is intended for individuals seeking to validate broad information security knowledge applicable to management, operations, auditing, technical oversight, and cybersecurity leadership roles. Candidates may include security officers, information security managers, auditors, systems administrators, network administrators, risk professionals, IT managers, and cybersecurity professionals preparing for expanded security responsibilities.

3. Experience Requirements

There are no minimum experience requirements to sit for the CISSO-A certification examination. The certification is available to candidates from various professional backgrounds who wish to demonstrate knowledge and skills in information systems security management and operations.

4. Accreditation Statement

CISSO-A is an accredited certification aligned with the requirements of ANSI/ISO/IEC 17024 for personnel certification. The certification is maintained through defined examination development, review, and governance processes intended to support fairness, validity, reliability, and continued relevance to the cybersecurity profession.

5. Job Task Analysis and Blueprint Maintenance

Mile2 maintains the CISSO-A certification through periodic review of the job role, body of knowledge, examination domains, and exam content. Job Task Analysis activities are used to evaluate the tasks, knowledge, skills, and abilities relevant to information security professionals and to ensure that the examination remains aligned with current industry practices and candidate expectations.

This blueprint is reviewed and updated as needed to maintain alignment with the approved CISSO-A Certification Scheme, job role expectations, examination requirements, and applicable certification body policies.

6. Relationship to the CISSO-A Certification Scheme

This CISSO-A Exam Blueprint is a controlled component of the broader CISSO-A Certification Scheme. The blueprint identifies the examination domains, content areas, item distribution, and assessment structure used to evaluate candidate knowledge, skills, and abilities.

The CISSO-A Certification Scheme remains the controlling document for certification scope, eligibility, competence requirements, assessment methodology, certification decision rules, recertification requirements, appeals, complaints, suspension, withdrawal, code of conduct, impartiality, examination security, and scheme maintenance.

7. Examination Information

Exam Element	Requirement
Exam duration	2 hours
Number of scored items	100
Item format	Multiple choice
Passing score	62 out of 100 points
Exam language	English
Delivery platform	ProctorU
Exam administration	Online proctored

8. CISSO-A Examination Domains and Weights

Domain	Number of Questions	Weight
01. Risk Management	7	7%
02. Security Management	10	10%
03. Cryptography	8	8%
04. Identification, Authentication, Authorization, and Accounting	11	11%
05. Data Security Management	6	6%
06. Operations Security	14	14%
07. Network Connections, Protocols, Devices, and Design	13	13%
08. IT and Business Security Architecture	8	8%
09. Secure Software Development	9	9%
10. Malware and Attacks	4	4%
11. Business Continuity, Disaster Recovery, Incident Management, Law, and Ethics	10	10%
Total	100	100%

9. CISSO-A Exam Blueprint Outline

Domain 1: Risk Management

Weight: 7% **Number of Questions:** 7

Candidates are expected to understand risk concepts, risk analysis, risk treatment, and the relationship between risk management and organizational security decision-making.

Knowledge and Skill Areas

1. Risk definitions and terminology
2. Business Impact Analysis
3. Risk management concepts and processes
4. Risk analysis, assessment, and scope definition
5. Risk response and treatment options
6. Continuous risk monitoring and measurement
7. Risk reporting
8. Continuous improvement
9. Risk management frameworks

Domain 2: Security Management

Weight: 10% **Number of Questions:** 10

Candidates are expected to understand security governance, management responsibilities, control selection, human resource considerations, legal and ethical responsibilities, and foundational security models.

Knowledge and Skill Areas

1. Understanding information security
2. Information Security Management System concepts
3. Security roles and responsibilities
4. Security governance and control frameworks
5. Human resource security considerations
6. Ethics and professional responsibilities
7. Legal and regulatory considerations
8. Due care and due diligence
9. Confidentiality, integrity, and availability
10. Security awareness and employee education
11. Selecting controls based on system security requirements
12. Trusted Computing Base concepts
13. Protection mechanisms
14. Security models, including Biba, Bell-LaPadula, and related models
15. Evaluation criteria

Domain 3: Cryptography

Weight: 8% **Number of Questions:** 8

Candidates are expected to understand cryptographic concepts, symmetric and asymmetric cryptography, hashing, digital signatures, hybrid cryptographic systems, common uses of cryptography, and cryptographic attacks.

Knowledge and Skill Areas

1. Cryptography terminology
2. Historical uses of cryptography
3. Cryptography foundations
4. Modern cryptography concepts

5. Symmetric cryptography
6. Asymmetric cryptography
7. Hashing
8. Hybrid cryptography
9. Digital signatures
10. Cryptography in use
11. Attacks against cryptographic systems

Domain 4: Identification, Authentication, Authorization, and Accounting

Weight: 11% **Number of Questions:** 11

Candidates are expected to understand identity management, authentication methods, authorization models, access control techniques, monitoring, auditing, logging, single sign-on, and federated identity.

Knowledge and Skill Areas

1. Identity management
2. Identity and access provisioning lifecycle
3. Authentication techniques
4. Authorization concepts
5. Role-based access control
6. Rule-based access control
7. Mandatory access control
8. Discretionary access control
9. Attribute-based access control
10. Risk-based access control
11. Access control models and techniques
12. Access control methods
13. Accounting, monitoring, auditing, and logging
14. Single sign-on
15. Federated identity

Domain 5: Data Security Management

Weight: 6% **Number of Questions:** 6

Candidates are expected to understand how data is identified, classified, stored, protected, retained, deleted, archived, and monitored throughout its lifecycle.

Knowledge and Skill Areas

1. Data lifecycle
2. Data discovery and classification
3. Data storage architectures and strategies
4. Data security architectures and strategies
5. Data retention, deletion, and archival policies
6. Data Security Posture Management

Domain 6: Operations Security

Weight: 14% **Number of Questions:** 14

Candidates are expected to understand the operational responsibilities, procedures, controls, and technologies needed to maintain secure systems and business operations.

Knowledge and Skill Areas

1. Administrative management responsibilities

2. Human resources management
3. Product implementation management
4. Redundancy and fault tolerance
5. Operations issues and responses
6. Threats to operations
7. Security assessments
8. Logging and monitoring activities
9. Configuration management
10. Change management
11. Foundational security operations concepts
12. Patch management
13. Physical security
14. Database models and terminology
15. Database security issues
16. Artificial intelligence considerations in security operations

Domain 7: Network Connections, Protocols, Devices, and Design

Weight: 13% **Number of Questions:** 13

Candidates are expected to understand network design, communication security, network devices, protocols, services, remote access technologies, wireless networks, and network-based attacks.

Knowledge and Skill Areas

1. Network connections
2. Network and communication security
3. Network topologies
4. Network cabling
5. LAN and WAN technologies
6. OSI model
7. Network devices
8. Network security devices and monitoring points
9. Ports, protocols, and services
10. Telephony
11. Virtual private networks
12. Wireless networks
13. Network-based attacks

Domain 8: IT and Business Security Architecture

Weight: 8% **Number of Questions:** 8

Candidates are expected to understand security architecture concepts, secure design principles, system threats, business security architecture, and the security implications of modern computing environments.

Knowledge and Skill Areas

1. Business security architecture
2. Security architecture frameworks
3. IT architecture
4. System threats
5. Secure design principles
6. Least privilege
7. Defense in depth
8. Secure defaults
9. Fail securely
10. Segregation of duties

11. Keep it simple and small
12. Zero Trust and trust-but-verify concepts
13. Privacy by design
14. Shared responsibility
15. Client-based systems
16. Server-based systems
17. Database systems
18. Cryptographic systems
19. Industrial Control Systems
20. Cloud-based systems, including SaaS, IaaS, and PaaS
21. Distributed systems
22. Internet of Things systems
23. Serverless systems
24. Embedded systems
25. High-performance computing systems
26. Edge computing systems
27. Virtualized systems

Domain 9: Secure Software Development

Weight: 9% **Number of Questions:** 9

Candidates are expected to understand software security concerns, secure development practices, web application security, and compliance considerations related to payment card environments.

Knowledge and Skill Areas

1. Software security concerns
2. Software development lifecycle security
3. Secure software development practices
4. Web application security
5. Application threats and vulnerabilities
6. Secure coding considerations
7. Software testing and validation concepts
8. PCI-DSS compliance considerations

Domain 10: Malware and Attacks

Weight: 4% **Number of Questions:** 4

Candidates are expected to understand common malware types, system attacks, application attacks, and the security implications of malicious activity.

Knowledge and Skill Areas

1. Common malware types
2. Malware behavior and impact
3. Attacks on applications
4. Attacks on systems
5. Defensive considerations for malware and attack activity

Domain 11: Business Continuity, Disaster Recovery, Incident Management, Law, and Ethics

Weight: 10% **Number of Questions:** 10

Candidates are expected to understand business continuity, disaster recovery, incident handling, evidence handling, legal considerations, and ethical responsibilities.

Knowledge and Skill Areas

1. Disaster recovery concepts
2. Disaster recovery project initiation
3. Business Impact Analysis and risk assessment
4. Recovery strategy selection
5. Disaster recovery plan development
6. Disaster recovery preparation
7. Business continuity management
8. Disaster recovery plan testing
9. Business continuity planning
10. Incident management
11. Computer crime concepts
12. Evidence handling
13. Incident management process
14. Legal considerations
15. Ethical considerations

10. Candidate Policy References

Candidates should refer to Mile2 certification policies for additional requirements related to exam registration, identification, proctoring, retakes, accommodations, appeals, complaints, certification use, code of conduct, recertification, suspension, and withdrawal.

11. Document Control Statement

This blueprint is maintained by Mile2 Cybersecurity Institute as a controlled examination specification for the CISSO-A certification. Updates to this blueprint are reviewed to ensure continued alignment with the approved CISSO-A Certification Scheme, examination requirements, candidate profile, job role expectations, and applicable certification body policies.