Mile2 Cybersecurity Certifications – C)ISSO Exam Blueprint

About CISSO

If you are looking for a comprehensive and highly regarded cybersecurity course, then the Certified Information Systems Security Officer (CISSO) is for you. The C)ISSO 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 can implement and maintain cost-effective security controls that are closely aligned with business and industry standards. The C)ISSO 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 (CISSO) 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 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

Experience Requirements

There are no minimum requirements needed to become a Certified Information Systems Security Officer (CISSO). Candidates can pursue the C)ISSO 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 certification is accessible to all aspiring information security professionals.

Accreditation

C)ISSO 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 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 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 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

C)ISSO Examination Weights

	Number of	Average
Domains (Exam A)	**Questions**	**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%**

	Number of	Average
Domains (Exam B)	**Questions**	**Weight**
01. Risk Management	9	9%
02. Security Management	14	14%
03. Identification, Authentication, Authorization and Accounting	12	12%
04. Operations Security	21	21%
05. Symmetric Cryptography, Asymmetric Cryptography and Hashing	4	4%
06. Network Concepts, Design and Attacks	11	11%
07. Enterprise Security Architecture and Attacks	6	6%
08. Software Development Security	4	4%
09. Malware and Attacks	3	3%
10. Business Continuity	6	6%
11. Incident Management, Law and Ethics	10	10%
	100	**100%**

CISSO Exam Blueprint

1. **Risk management**
    - a. Business Impact Analysis
    - b. External dependencies
    - c. Threat and vulnerability identification
    - d. Risk analysis, assessment, and scope
    - e. Risk response and treatment (e.g., cybersecurity insurance)
    - f. Continuous monitoring and measurement
    - g. Reporting (e.g., internal, external)
    - h. Continuous improvement (e.g., risk maturity modeling)
    - i. Risk frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Payment Card Industry (PCI))
    - j. Threat Modeling

2. **Security management**
    - a. Ethics
    - b. Law
        - i. Licensing and Intellectual Property requirements
        - ii. Import/export controls
        - iii. Transborder data flow
        - iv. Issues related to privacy (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act, Personal Information Protection Law, Protection of Personal Information Act)
        - v. Contractual, legal, industry standards, and regulatory requirements
    - c. CIA
    - d. Alignment of the security function to business strategy, goals, mission, and objectives
    - e. Organizational processes (e.g., acquisitions, divestitures, governance committees)
    - f. Organizational roles and responsibilities
    - g. Security control frameworks (e.g., International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Control Objectives for Information and Related Technology (COBIT), Sherwood Applied Business Security Architecture (SABSA), Service-Oriented Modeling Framework (SOMF), Payment Card Industry (PCI), Federal Risk and Authorization Management Program (FedRAMP))
    - h. Due care/due diligence
    - i. Applicable types of controls (e.g., preventive, detection, corrective)
    - j. Education of employees
        - i. Methods and techniques to increase awareness and training (e.g., social engineering, phishing, security champions, gamification)
        - ii. Periodic content reviews to include emerging technologies and trends (e.g., cryptocurrency, artificial intelligence (AI), blockchain)
        - iii. Program effectiveness evaluation
    - k. Select controls based upon systems security requirements
    - l. Security Models
        - i. Understand the fundamental concepts of security models (e.g., Biba, Star Model, Bell-LaPadula)
    - m. Evaluation Criteria

3. **Cryptography**
   a. Symmetric
   b. Asymmetric
   c. Select and determine cryptographic solutions
      i. Cryptographic life cycle (e.g., keys, algorithm selection)
      ii. Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)
      iii. Public key infrastructure (PKI) (e.g., quantum key distribution)

4. **Identification, Authentication, Authorization, and Accounting**
   a. Identification methods
   b. Authentication methods
   c. Authorization
      i. Role-based access control (RBAC)
      ii. Rule based access control
      iii. Mandatory access control (MAC)
      iv. Discretionary access control (DAC)
      v. Attribute-based access control (ABAC)
      vi. Risk based access control
      vii. Access policy enforcement (e.g., policy decision point, policy enforcement point)
   d. Accounting (Auditing, Logging)
   e. Control physical and logical access to assets
      i. Information
      ii. Systems
      iii. Devices
      iv. Facilities
      v. Applications
      vi. Services
   f. Design identification and authentication strategy (e.g., people, devices, and services)
      i. Groups and Roles
      ii. Authentication, Authorization and Accounting (AAA) (e.g., multi-factor authentication (MFA), password-less authentication)
      iii. Session management
      iv. Registration, proofing, and establishment of identity
      v. Federated Identity Management (FIM)
      vi. Credential management systems (e.g., Password vault)
      vii. Single sign-on (SSO)
      viii. Just-In-Time
   g. Federated identity with a third-party service
      i. On-premise
      ii. Cloud
      iii. Hybrid
      iv. SAML, OpenID Connect
   h. Manage the identity and access provisioning lifecycle
      i. Account access review (e.g., user, system, service)
      ii. Provisioning and deprovisioning (e.g., on /off boarding and transfers)
      iii. Role definition and transition (e.g., people assigned to new roles)
      iv. Privilege escalation (e.g., use of sudo, auditing its use)
      v. Service accounts management
   i. Implement authentication systems

5. **Data Security Management**
   a. Asset Management
      i. Identify and classify information and assets
         1. Data classification
         2. Asset Classification
      ii. Establish information and asset handling requirements
      iii. Provision information and assets securely
         1. Information and asset ownership
         2. Asset inventory (e.g., tangible, intangible)
         3. Asset management
      iv. Manage data lifecycle
         1. Data roles (i.e., owners, controllers, custodians, processors, users/subjects)
         2. Data collection
         3. Data location
         4. Data maintenance
         5. Data retention
         6. Data remanence
         7. Data destruction
      v. Ensure appropriate asset retention (e.g., End of Life (EOL), End of Support)
      vi. Determine data security controls and compliance requirements
         1. Data states (e.g., in use, in transit, at rest)
         2. Scoping and tailoring
         3. Standards selection
         4. Data protection methods (e.g., Digital Rights Management (DRM), Data Loss Prevention (DLP))
   b. Encryption Layers
   c. Other data security methods
   d. Data Security Posture Management (DSPM)

6. **Operations Security**
   a. HR Items
      i. Candidate screening and hiring
      ii. Employment agreements and policy driven requirements
      iii. Onboarding, transfers, and termination processes
      iv. Vendor, consultant, and contractor agreements and controls
   b. Manage the information system lifecycle
      i. Stakeholders needs and requirements
      ii. Requirements analysis
      iii. Architectural design
      iv. Development /implementation
      v. Integration
      vi. Verification and validation
      vii. Transition/deployment
      viii. Operations and maintenance/sustainment
      ix. Retirement/disposal
   c. Security Assessments
      i. Design and validate assessment, test, and audit strategies
         1. Internal (e.g., within organization control)
         2. External (e.g., outside organization control)
         3. Third-party (e.g., outside of enterprise control)
         4. Location (e.g., on-premises, cloud, hybrid)

- ii. Conduct security control testing
  1. Vulnerability assessment
  2. Penetration testing (e.g., red, blue, and/or purple team exercises)
  3. Log reviews
  4. Synthetic transactions/benchmarks
  5. Code review and testing
  6. Misuse case testing
  7. Coverage analysis
  8. Interface testing (e.g., user interface, network interface, application programming interface (API))
  9. Breach attack simulations
  10. Compliance checks
  11. Privacy
- iii. Collect security process data (e.g., technical and administrative)
  1. Account management
  2. Management review and approval
  3. Key performance and risk indicators
  4. Backup verification data
  5. Training and awareness
  6. Disaster Recovery (DR) and Business Continuity (BC)
- iv. Analyze test output and generate report
  1. Remediation
  2. Exception handling
  3. Ethical disclosure
- v. Conduct or facilitate security audits
  1. Internal (e.g., within organization control)
  2. External (e.g., outside organization control)
  3. Third-party (e.g., outside of enterprise control)
  4. Location (e.g., on-premises, cloud, hybrid

d. Conduct logging and monitoring activities
- i. Intrusion detection and prevention (IDPS)
- ii. Security Information and Event Management (SIEM)
- iii. Continuous monitoring and tuning
- iv. Egress monitoring
- v. Log management
- vi. Threat intelligence (e.g., threat feeds, threat hunting)
- vii. User and Entity Behavior Analytics (UEBA)

e. Perform Configuration Management (CM) (e.g., provisioning, baselining, automation)

f. Apply foundational security operations concepts
- i. Need-to-know/least privilege
- ii. Separation of Duties (SoD) and responsibilities
- iii. Privileged account management
- iv. Job rotation
- v. Service-level agreements (SLA)

g. Apply resource protection
- i. Media management
- ii. Media protection techniques
- iii. Data at rest/data in transit

h. Operate and maintain detection and preventative measures
- i. Firewalls (e.g., next generation, web application, network)
- ii. Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
- iii. Whitelisting/blacklisting
- iv. Third-party provided security services

v. Sandboxing

vi. Honeypots/honeynets

vii. Anti-malware

viii. Machine learning and Artificial Intelligence (AI) based tools

i. Implement and support patch and vulnerability management

j. Understand and participate in change management processes

k. Implement recovery strategies

i. Backup storage strategies (e.g., cloud storage, onsite, offsite)

ii. Recovery site strategies (e.g., cold vs. hot, resource capacity agreements)

iii. Multiple processing sites

iv. System resilience, high availability (HA), Quality of Service (QoS), and fault tolerance

l. Implement and manage physical security

i. Perimeter security controls

ii. Internal security controls

m. Address personnel safety and security concerns

i. Travel

ii. Security training and awareness (e.g., insider threat, social media impacts, two-factor authentication (2FA) fatigue)

iii. Emergency management

iv. Duress

n. Supply chain risk management (SCRM)

i. Risks associated with the acquisition of products and services from suppliers and providers (e.g., product tampering, counterfeits, implants)

o. Risk mitigations (e.g., third-party assessment and monitoring, minimum security requirements, service level requirements, silicon root of trust, physically unclonable function, software bill of materials)

7. Network Connections, Protocols, Devices, and Design

a. Apply secure design principles in network architectures

i. Open System Interconnection (OSI) and Transmission Control Protocol/Internet Protocol (TCP/IP) models

ii. Internet Protocol (IP) version 4 and 6 (IPv6) (e.g., unicast, broadcast, multicast, anycast)

iii. Secure protocols (e.g., Internet Protocol Security (IPSec), Secure Shell (SSH), Secure Sockets Layer (SSL)/ Transport Layer Security (TLS))

iv. Implications of multilayer protocols

v. Converged protocols (e.g., Internet Small Computer Systems Interface (iSCSI), Voice over Internet Protocol (VoIP), InfiniBand over Ethernet, Compute Express Link)

vi. Transport architecture (e.g., topology, data/control/management plane, cut-through/store-and-forward)

vii. Performance metrics (e.g., bandwidth, latency, jitter, throughput, signal-to-noise ratio)

viii. Traffic flows (e.g., north-south, east-west)

ix. Physical segmentation (e.g., in-band, out-of-band, air-gapped)

x. Logical segmentation (e.g., virtual local area networks (VLANs), virtual private networks (VPNs), virtual routing and forwarding, virtual domain)

xi. Micro-segmentation (e.g., network overlays/encapsulation; distributed firewalls, routers, intrusion detection system (IDS)/intrusion prevention system (IPS), zero trust)

xii. Edge networks (e.g., ingress/egress, peering)

  - xiii. Wireless networks (e.g., Bluetooth, Wi-Fi, Zigbee, satellite)
  - xiv. Cellular/mobile networks (e.g., 4G, 5G)
  - xv. Content distribution networks (CDN)
  - xvi. Software defined networks (SDN), (e.g., application programming interface (API), Software-Defined Wide- Area Network, network functions virtualization)
  - xvii. Virtual Private Cloud (VPC)
  - xviii. Monitoring and management (e.g., network observability, traffic flow/shaping, capacity management, fault detection and handling)
- b. Secure network components
  - i. Operation of infrastructure (e.g., redundant power, warranty, support)
  - ii. Transmission media (e.g., physical security of media, signal propagation quality)
  - iii. Network Access Control (NAC) systems (e.g., physical, and virtual solutions)
  - iv. Endpoint security (e.g., host-based)
- c. Implement secure communication channels according to design
  - i. Voice, video, and collaboration (e.g., conferencing, Zoom rooms)
  - ii. Remote access (e.g., network administrative functions)
  - iii. Data communications (e.g., backhaul networks, satellite)
  - iv. Third-party connectivity (e.g., telecom providers, hardware support)

8. I.T. and Business Security Architecture

- a. Enterprise Security Architectures Frameworks
  - i. dsds
- b. implement and manage using secure design principles
  - i. Threat modeling
  - ii. Least privilege
  - iii. Defense in depth
  - iv. Secure defaults
  - v. Fail securely
  - vi. Segregation of Duties (SoD)
  - vii. Keep it simple and small
  - viii. Zero trust or trust but verify
  - ix. Privacy by design
  - x. Shared responsibility
  - xi. Secure access service edge
- c. Understand security capabilities of Information Systems (IS)
  - i. memory protection
  - ii. Trusted Platform Module (TPM)
  - iii. Encryption/decryption
  - iv. Exploit prevention
- d. Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements
  - i. Client-based systems
  - ii. Server-based systems
  - iii. Database systems
  - iv. Cryptographic systems
  - v. Industrial Control Systems (ICS)
  - vi. Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
  - vii. Distributed systems
  - viii. Internet of Things (IoT)
  - ix. Microservices (e.g., application programming interface (API))

- x. Containerization
- xi. Serverless
- xii. Embedded systems
- xiii. High-Performance Computing systems
- xiv. Edge computing systems
- xv. Virtualized systems
- xvi. Artificial Intelligence

- e. Apply security principles to site and facility design
- f. Design site and facility security controls
  - i. Wiring closets/intermediate distribution facilities
  - ii. Server rooms/data centers
  - iii. Media storage facilities
  - iv. Evidence storage
  - v. Restricted and work area security
  - vi. Utilities and Heating, Ventilation, and Air Conditioning (HVAC)
  - vii. Environmental issues (e.g., natural disasters, man-made)
  - viii. Fire prevention, detection, and suppression
  - ix. Power (e.g., redundant, backup)

9. Secure Software Development

- a. Understand and integrate security in the Software Development Life Cycle (SDLC)
  - i. Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps, Scaled Agile Framework)
  - ii. Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))
  - iii. Operation and maintenance
  - iv. Change management
  - v. Integrated Product Team
- b. Identify and apply security controls in software development ecosystems
  - i. Programming languages
  - ii. Libraries
  - iii. Tool sets
  - iv. Integrated Development Environment
  - v. Runtime
  - vi. Continuous Integration and Continuous Delivery (CI/CD)
  - vii. Software configuration management (CM)
  - viii. Code repositories
  - ix. Application security testing (e.g., static application security testing (SAST), dynamic application security testing (DAST), software composition analysis, Interactive Application Security Test (IAST))
- c. Assess the effectiveness of software security
  - i. Auditing and logging of changes
  - ii. Risk analysis and mitigation
- d. Assess security impact of acquired software
  - i. Commercial-off-the-shelf (COTS)
  - ii. Open source
  - iii. Third-party
  - iv. Managed services (e.g., enterprise applications)
  - v. Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))
- e. Define and apply secure coding guidelines and standards
  - i. Security weaknesses and vulnerabilities at the source-code level
  - ii. Security of application programming interfaces (API)

- iii. Secure coding practices
- iv. Software-defined security

10. Malware and Attacks

- a. Common Malware
- b. Understand methods of cryptanalytic attacks
  - i. Brute force
  - ii. Ciphertext only
  - iii. Known plaintext
  - iv. Frequency analysis
  - v. Chosen ciphertext
  - vi. Implementation attacks
  - vii. Side-channel
  - viii. Fault injection
  - ix. Timing
  - x. Man-in-the-Middle (MITM)
  - xi. Pass the hash
  - xii. Kerberos exploitation
  - xiii. Ransomware
- c. Attacks on Applications
- d. Attacks on Systems
- e. Attacks on ?????

11. BCDR + IH

- a. BIA
- b. Implement Disaster Recovery (DR) processes
  - i. Response
  - ii. Personnel
  - iii. Communications (e.g., methods)
  - iv. Assessment
  - v. Restoration
  - vi. Training and awareness
  - vii. Lessons learned
- c. Test Disaster Recovery Plans (DRP)
  - i. Read-through/tabletop
  - ii. Walkthrough
  - iii. Simulation
  - iv. Parallel
  - v. Full interruption
  - vi. Communications (e.g., stakeholders, test status, regulators)
- d. Participate in Business Continuity (BC) planning and exercises
- e. Understand and comply with investigations
  - i. Evidence collection and handling
  - ii. Reporting and documentation
  - iii. Investigative techniques
  - iv. Digital forensics tools, tactics, and procedures
  - v. Artifacts (e.g., data, computer, network, mobile device)
- f. Cybercrimes and data breaches
- g. Conduct incident management
  - i. Detection
  - ii. Response
  - iii. Mitigation

iv. Reporting
v. Recovery
vi. Remediation
vii. Lessons learned