CISSP 2025 Bootcamp Syllabus

The latest CISSP certification recognizes cybersecurity professionals with the knowledge, skills and abilities to lead an organization's information security program. The CISSP is ideal for experienced security practitioners, managers and executives interested in proving their knowledge across a wide array of security practices and principles, including those in the following positions:

- Chief Information Security Officer
- Chief Information Officer
- Director of Security
- IT Director/Manager
- Security Systems Engineer
- Security Analyst
- Security Manager
- Security Auditor
- Security Architect
- Security Consultant
- Network Architect

This 5-Day CISSP bootcamp lead by industry expert Michael J. Shannon will help the qualified candidate get the extra edge needed to be successful on the exam on the first attempts. This is a highly condensed and accelerated course for the professional who is close to taking the exam. **Course Session Breakouts:**

Day 1

Professional Ethics and Security Concepts

1.1 Understand, adhere to, and promote professional ethics (2-4 items)

      1.1.1 ISC2 Code of Professional Ethics

      1.1.2 Organizational code of ethics

1.2 Understand and apply security concepts

      1.2.1 Confidentiality, integrity, and availability, authenticity, and nonrepudiation (5 Pillars of Information Security)

Security Governance and Compliance Issues

1.3 Evaluate, apply, and sustain security governance principles

      1.3.1 Alignment of the security function to business strategy, goals, mission, and objectives

      1.3.2 Organizational processes (e.g., acquisitions, divestitures, governance committees)

      1.3.3 Organizational roles and responsibilities

1.3.4 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), Payment Card Industry (PCI), Federal Risk and Authorization Management Program (FedRAMP))

1.3.5 Due care/due diligence

1.4 Understand legal, regulatory, and compliance issues that pertain to information security in a holistic context

1.4.1 Cybercrimes and data breaches

1.4.2 Licensing and Intellectual Property requirements

1.4.3 Import/export controls

1.4.4 Transborder data flow

1.4.5 Issues related to privacy (e.g., General Data Protection Regulation (GDPR), California Consumer Privacy Act, Personal Information Protection Law, Protection of Personal Information Act)

1.4.6 Contractual, legal, industry standards, and regulatory requirements

Investigations and Policies

1.5 Understand requirements for investigation types (i.e., administrative, criminal, civil, regulatory, industry standards)

1.6 Develop, document, and implement security policy, standards, procedures, and guidelines

1.8 Contribute to and enforce personnel security policies and procedures

> 1.8.1 Candidate screening and hiring

> 1.8.2 Employment agreements and policy driven requirements

> 1.8.3 Onboarding, transfers, and termination processes

> 1.8.4 Vendor, consultant, and contractor agreements and controls **Risk**

management concepts

> 1.9.1 Threat and vulnerability identification

> 1.9.2 Risk analysis, assessment, and scope

> 1.9.3 Risk response and treatment (e.g., cybersecurity insurance)

> 1.9.4 Applicable types of controls (e.g., preventive, detection, corrective)

> 1.9.5 Control assessments (e.g., security and privacy)

> 1.9.6 Continuous monitoring and measurement

> 1.9.7 Reporting (e.g., internal, external)

> 1.9.8 Continuous improvement (e.g., risk maturity modeling)

> 1.9.9 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))

Threat Modeling, SCRM, and Security Awareness

1.10 Threat modeling concepts and methodologies

1.11 Apply supply chain risk management (SCRM) concepts

> 1.11.1 Risks associated with the acquisition of products and services from suppliers and providers (e.g., product tampering, counterfeits, implants)

> 1.11.2 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)

1.12 Establish and maintain a security awareness, education, and training program

1.12.1 Methods and techniques to increase awareness and training (e.g., social engineering, phishing, security champions, gamification)

1.12.2 Periodic content reviews to include emerging technologies and trends (e.g., cryptocurrency, artificial intelligence (AI), blockchain)

1.12.3 Program effectiveness evaluation

Asset Classification, Handling, and Provisioning

2.1.1 Data classification

2.1.2 Asset classification

2.2 Establish information and asset handling requirements

2.3 Provision information and assets securely

2.3.1 Information and asset ownership

2.3.2 Asset inventory (e.g., tangible, intangible)

2.3.3 Asset management

Day 2

Data Lifecycle, Controls and Compliance

2.4 Manage data lifecycle

2.4.1 Data roles (i.e., owners, controllers, custodians, processors, users/subjects)

2.4.2 Data collection

2.4.3 Data location

2.4.4 Data maintenance

2.4.5 Data retention (End of Life (EOL), End of Support)

2.4.6 Data remanence

2.4.7 Data destruction

2.6 Determine data security controls and compliance requirements

2.6.1 Data states (e.g., in use, in transit, at rest)

2.6.2 Scoping and tailoring

2.6.3 Standards selection

2.6.4 Data protection methods (e.g., Digital Rights Management (DRM), data loss prevention (DLP), cloud access security broker (CASB))

Secure Design Principles and Models

3.1 Research, implement, and manage engineering processes using secure design principles

   3.1.1 Threat modeling

   3.1.2 Least privilege

   3.1.3 Defense in depth

   3.1.4 Secure defaults

   3.1.5 Fail securely

   3.1.6 Segregation of Duties (SoD)

   3.1.7 Keep it simple and small

   3.1.8 Zero trust or trust but verify

   3.1.9 Privacy by design

   3.1.10 Shared responsibility

   3.1.11 Secure access service edge

3.2 Understand the fundamental concepts of security models (e.g., Biba, Star Model, BellLaPadula)

Vulnerabilities of Architectures, Designs, and Solution Elements

3.5 Assess and mitigate the vulnerabilities of security architectures, designs, and solution elements

   3.5.1 Client-based systems

   3.5.2 Server-based systems

   3.5.3 Database systems

   3.5.4 Cryptographic systems

   3.5.5 Operational Technology/industrial control systems (ICS)

   3.5.6 Cloud-based systems (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

   3.5.7 Distributed systems

   3.5.8 Internet of Things (IoT)

   3.5.9 Microservices (e.g., application programming interface (API))

   3.5.10 Containerization

   3.5.11 Serverless

   3.5.12 Embedded systems

3.5.13 High-Performance Computing systems

    3.5.14 Edge computing systems

    3.5.15 Virtualized systems

3.3 Select controls based upon systems security requirements

3.4 Understand security capabilities of Information Systems (e.g., memory protection, Trusted Platform Module (TPM), encryption/decryption)

Cryptology: Cryptographic Solutions and Cryptanalytic Attacks

3.6 Select and determine cryptographic solutions

    3.6.1 Cryptographic life cycle (e.g., keys, algorithm selection)

    3.6.2 Cryptographic methods (e.g., symmetric, asymmetric, elliptic curves, quantum)

    3.6.3 Public key infrastructure (PKI) (e.g., quantum key distribution)

    3.6.4 Key management practices (e.g., rotation)

    3.6.5 Digital signatures and digital certificates (e.g., non-repudiation, integrity)

3.7 Understand methods of cryptanalytic attacks

    3.7.1 Brute force

    3.7.2 Ciphertext only

    3.7.3 Known plaintext

    3.7.4 Frequency analysis

    3.7.5 Chosen ciphertext

    3.7.6 Implementation attacks

    3.7.7 Side-channel

    3.7.8 Fault injection

    3.7.9 Timing

    3.7.10 Man-in-the-middle (MITM)

    3.7.11 Pass the hash

    3.7.12 Kerberos exploitation

    3.7.13 Ransomware

Site and Facility Security

3.8 Apply security principles to site and facility design

3.9 Design site and facility security controls

3.9.1 Wiring closets/intermediate distribution frame

3.9.2 Server rooms/data centers

3.9.3 Media storage facilities

3.9.4 Evidence storage

3.9.5 Restricted and work area security

3.9.6 Utilities and Heating, Ventilation, and Air Conditioning (HVAC)

3.9.7 Environmental issues (e.g., natural disasters, man-made)

3.9.8 Fire prevention, detection, and suppression

3.9.9 Power (e.g., redundant, backup)

7.14 Implement and manage physical security

7.14.1 Perimeter security controls

7.14.2 Internal security controls

7.15 Address personnel safety and security concerns

7.15.1 Travel

7.15.2 Security training and awareness (e.g., insider threat, social media impacts, twofactor authentication (2FA) fatigue)

7.15.3 Emergency management

7.15.4 Duress

Day 3

Information System Lifecycle Management

3.10.1 Stakeholders needs and requirements

3.10.2 Requirements analysis

3.10.3 Architectural design

3.10.4 Development /implementation

3.10.5 Integration

3.10.6 Verification and validation

3.10.7 Transition/deployment

3.10.8 Operations and maintenance/sustainment

3.10.9 Retirement/disposal

Secure Design Principles in Network Architectures

4.1 Apply secure design principles in network architectures

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

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

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

4.1.4 Implications of multilayer protocols

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

4.1.6 Transport architecture (e.g., topology, data/control/management plane, cutthrough/store-and-forward)

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

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

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

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

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

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

4.1.13 Wireless networks (e.g., Bluetooth, Wi-Fi, Zigbee, satellite)

4.1.14 Cellular/mobile networks (e.g., 4G, 5G)

4.1.15 Content distribution networks (CDN)

4.1.16 Software defined networks (SDN), (e.g., application programming interface (API), Software-Defined Wide-Area Network, network functions virtualization)

4.1.17 Virtual Private Cloud (VPC)

4.1.18 Monitoring and management (e.g., network observability, traffic flow/shaping, capacity management, fault detection and handling)

Securing Network Components and Communication Channels

4.2 Securing Network Components and Communication Channels

      4.2.1 Operation of infrastructure (e.g., redundant power, warranty, support)

      4.2.2 Transmission media (e.g., physical security of media, signal propagation quality)

      4.2.3 Network Access Control (NAC) systems (e.g., physical, and virtual solutions)

      4.2.4 Endpoint security (e.g., host-based)

4.3 Implement secure communication channels according to design

      4.3.1 Voice, video, and collaboration (e.g., conferencing, Zoom rooms)

      4.3.2 Remote access (e.g., network administrative functions)

      4.3.3 Data communications (e.g., backhaul networks, satellite)

      4.3.4 Third-party connectivity (e.g., telecom providers, hardware support)

Controlling Asset Access and Device Identification and Authentication

5.1 Control physical and logical access to assets

      5.1.1 Information

      5.1.2 Systems

      5.1.3 Devices

      5.1.4 Facilities

      5.1.5 Applications

      5.1.6 Services

5.2 Design identification and authentication strategy (e.g., people, devices, and services)

      5.2.1 Groups and Roles

      5.2.2 Authentication, Authorization and Accounting (AAA) (e.g., multi-factor authentication (MFA), password-less authentication)

      5.2.3 Session management

      5.2.4 Registration, proofing, and establishment of identity

      5.2.5 Federated Identity Management (FIM)

      5.2.6 Credential management systems (e.g., Password vault)

      5.2.7 Single sign-on (SSO)

      5.2.8 Just-In-Time

5.6 Implement authentication systems

5.3 Federated identity with a third-party service

      5.3.1 On-premise

      5.3.2 Cloud

      5.3.3 Hybrid

Day 4

Authorization Mechanisms and Identity Management

5.4 Implement and manage authorization mechanisms

      5.4.1 Role-based access control (RBAC)

      5.4.2 Rule based access control

      5.4.3 Mandatory access control (MAC)

      5.4.4 Discretionary access control (DAC)

      5.4.5 Attribute-based access control (ABAC)

      5.4.6 Risk based access control

      5.4.7 Access policy enforcement (e.g., policy decision point, policy enforcement point)

5.5 Manage the identity and access provisioning lifecycle

      5.5.1 Account access review (e.g., user, system, service)

      5.5.2 Provisioning and deprovisioning (e.g., on/off boarding and transfers)

      5.5.3 Role definition and transition (e.g., people assigned to new roles)

      5.5.4 Privilege escalation (e.g., use of sudo, auditing its use)

      5.5.5 Service accounts management

Security Audit and Controls Testing

6.1 Design and validate assessment, test, and audit strategies

      6.1.1 Internal (e.g., within organization control)

      6.1.2 External (e.g., outside organization control)

      6.1.3 Third-party (e.g., outside of enterprise control)

      6.1.4 Location (e.g., on-premise, cloud, hybrid)

6.2 Conduct security controls testing

      6.2.1 Vulnerability assessment

      6.2.2 Penetration testing (e.g., red, blue, and/or purple team exercises)

      6.2.3 Log reviews

      6.2.4 Synthetic transactions/benchmarks

      6.2.5 Code review and testing

      6.2.6 Misuse case testing

      6.2.7 Coverage analysis

      6.2.8 Interface testing (e.g., user interface, network interface, application programming interface (API))

      6.2.9 Breach attack simulations

      6.2.10 Compliance checks

Collecting and Analyzing Security Process Data

6.3 Collect security process data (e.g., technical, and administrative)

      6.3.1 Account management

      6.3.2 Management review and approval

      6.3.3 Key performance and risk indicators

      6.3.4 Backup verification data

      6.3.5 Training and awareness

      6.3.6 Disaster recovery (DR) and Business Continuity (BC)

6.4 Analyze test output and generate report

      6.4.1 Remediation

      6.4.2 Exception handling

      6.4.3 Ethical disclosure

      6.5 Conduct or facilitate security audits

      6.5.1 Internal (e.g., within organization control)

      6.5.2 External (e.g., outside organization control)

      6.5.3 Third-party (e.g., outside of enterprise control)

      6.5.4 Location (e.g., on-premise, cloud, hybrid)

Logging, Monitoring, and Investigations

7.2 Conduct logging and monitoring activities

      7.2.1 Intrusion detection and prevention system (IDPS)

      7.2.2 Security information and event management (SIEM)

      7.2.3 Security orchestration, automation and response (SOAR)

      7.2.4 Continuous monitoring and tuning

      7.2.5 Egress monitoring

      7.2.6 Log management

      7.2.7 Threat intelligence (e.g., threat feeds, threat hunting)

      7.2.8 User and Entity Behavior Analytics

7.1 Understand and comply with investigations

      7.1.1 Evidence collection and handling

      7.1.2 Reporting and documentation

      7.1.3 Investigative techniques

      7.1.4 Digital forensics tools, tactics, and procedures

      7.1.5 Artifacts (e.g., data, computer, network, mobile device)

Foundational Security Operations and Resource Protection

7.3 Perform configuration management (CM) (e.g., provisioning, baselining, automation)

7.9 Understand and participate in change management processes

7.4 Apply foundational security operations concepts

      7.4.1 Need-to-know/least privilege

      7.4.2 Segregation of Duties (SoD) and responsibilities

      7.4.3 Privileged account management

      7.4.4 Job rotation

      7.4.5 Service-level agreements (SLA)

7.5 Apply resource protection

      7.5.1 Media management

      7.5.2 Media protection techniques

      7.5.3 Data at rest/data in transit

7.6 Conduct incident management

7.6.1 Detection

7.6.2 Response

7.6.3 Mitigation

7.6.4 Reporting

7.6.5 Recovery

7.6.6 Remediation

7.6.7 Lessons learned

Day 5

Operating Detection and Preventative Measures

7.7 Operate and maintain detection and preventative measures

7.7.1 Firewalls (e.g., next generation, web application, network)

7.7.2 Intrusion detection systems (IDS) and intrusion prevention systems (IPS)

7.7.3 Whitelisting/blacklisting

7.7.4 Third-party provided security services

7.7.5 Sandboxing

7.7.6 Honeypots/honeynets

7.7.7 Anti-malware

7.7.8 Machine learning and artificial intelligence (AI) based tools

7.8 Implement and support patch and vulnerability management

Business Continuity (BC) Planning and Exercises

7.13 Participate in Business Continuity (BC) planning and exercises

1.7 Identify, analyze, assess, prioritize, and implement Business Continuity (BC) requirements

1.7.1 Business impact analysis (BIA)

1.7.2 External dependencies

7.10 Implement recovery strategies

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

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

7.10.3 Multiple processing sites

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

Implement Disaster Recovery (DR)

7.11 Implement disaster recovery (DR) processes

       7.11.1 Response

       7.11.2 Personnel

       7.11.3 Communications (e.g., methods)

       7.11.4 Assessment

       7.11.5 Restoration

       7.11.6 Training and awareness

       7.11.7 Lessons learned

       7.12 Test disaster recovery plan (DRP)

       7.12.1 Read-through/tabletop

       7.12.2 Walkthrough

       7.12.3 Simulation

       7.12.4 Parallel

       7.12.5 Full interruption

       7.12.6 Communications (e.g., stakeholders, test status, regulators)

Securing the SDLC and Software Development Ecosystems

8.1 Understand and integrate security in the Software Development Life Cycle (SDLC)

       8.1.1 Development methodologies (e.g., Agile, Waterfall, DevOps, DevSecOps, Scaled Agile Framework)

       8.1.2 Maturity models (e.g., Capability Maturity Model (CMM), Software Assurance Maturity Model (SAMM))

       8.1.3 Operation and maintenance

       8.1.4 Change management

       8.1.5 Integrated Product Team

8.2 Identify and apply security controls in software development ecosystems

       8.2.1 Programming languages

8.2.2 Libraries

8.2.3 Tool sets

8.2.4 Integrated Development Environment

8.2.5 Runtime

8.2.6 Continuous Integration and Continuous Delivery (CI/CD)

8.2.7 Software Configuration Management

8.2.8 Code repositories

8.2.9 Application security testing (e.g., static application security testing (SAST), dynamic application security testing (DAST), software composition analysis, Interactive Application Security Test (IAST))

Assessing Software Security and Coding Guidelines

8.3 Assess the effectiveness of software security

8.3.1 Auditing and logging of changes

8.3.2 Risk analysis and mitigation

8.4 Assess security impact of acquired software

8.4.1 Commercial off-the-shelf (COTS)

8.4.2 Open source

8.4.3 Third-party

8.4.4 Managed services (e.g., enterprise applications)

8.4.5 Cloud services (e.g., Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS))

8.5 Define and apply secure coding guidelines and standards

8.5.1 Security weaknesses and vulnerabilities at the source-code level

8.5.2 Security of application programming interfaces (API)

8.5.3 Secure coding practices

8.5.4 Software-defined security