Official ISC2 CBK Training for the CISSP

Official ISC2® Training Seminar for the Certified Information Systems Security Professional (CISSP®) provides a comprehensive review of the knowledge required to effectively design, engineer and manage the overall security posture of an organization. This training course will help students review and refresh their knowledge and identify areas they need to study for the CISSP exam. Content aligns with and comprehensively covers the eight domains of the ISC2 CISSP Common Body of Knowledge (CBK®), ensuring relevancy across all disciplines in the field of cybersecurity.

Official courseware is developed by ISC2 – creator of the CISSP CBK – to ensure your training is relevant and up-to-date. Our instructors are verified security experts who hold the CISSP and have completed intensive training to teach ISC2 content.

Training features:

- Instruction from an ISC2 Authorized Instructor
- Official ISC2 Student Training Guide
- Interactive flash cards to reinforce learning
- An applied scenario with 9 corresponding activities teaching you how to apply security concepts to a situation that CISSPs likely encounter in the workplace
- 8 discussions encouraging peer to peer interaction around key topics
- 71 content specific activities, including 6 case studies
- 9 end of chapter quizzes with answer explanation to assess comprehension
- 180 question post course assessment with answer explanation highlighting areas for further study

Who Should Attend

This training course is intended for professionals who have at least five years of cumulative, paid work experience in two or more of the eight domains of the ISC2 CISSP CBK and are pursuing CISSP training and certification to acquire the credibility and mobility to advance within their current information security careers. The training seminar is ideal for those working in positions such as, but not limited to:

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

- Security Director
- Network Architect

Course Domains

- Domain 1: Security and Risk Management
- Domain 2: Asset Security
- Domain 3: Security Architecture and Engineering
- Domain 4: Communication and Network Security
- Domain 5: Identity and Access Management (IAM)
- Domain 6: Security Assessment and Testing
- Domain 7: Security Operations
- Domain 8: Software Development Security

Course Objectives

After completing this course, the student will be able to:

- Apply fundamental concepts and methods related to the fields of information technology and security.
- Align overall organizational operational goals with security functions and implementations.
- Determine how to protect assets of the organization as they go through their lifecycle.
- Leverage the concepts, principles, structures, and standards used to design, implement, monitor, and secure operating systems, equipment, networks, applications, and those controls used to enforce various levels of confidentiality, integrity, and availability.
- Apply security design principles to select appropriate mitigations for vulnerabilities present in common information system types and architectures.
- Explain the importance of cryptography and the security services it can provide in today's digital and information age.
- Evaluate physical security elements relative to information security needs.
- Evaluate the elements that comprise communication and network security relative to information security needs.
- Leverage the concepts and architecture that define the associated technology and implementation systems and protocols at Open Systems Interconnection (OSI) model layers 1–7 to meet information security needs.
- Determine appropriate access control models to meet business security requirements.
- Apply physical and logical access controls to meet information security needs.
- Differentiate between primary methods for designing and validating test and audit strategies that support information security requirements.
- Apply appropriate security controls and countermeasures to optimize an organization's operational function and capacity.
- Assess information systems risks to an organization's operational endeavors.

- Determine appropriate controls to mitigate specific threats and vulnerabilities.
- Apply information systems security concepts to mitigate the risk of software and systems vulnerabilities throughout the systems' lifecycles.

Domains/Modules/Chapters

This course covers the following chapters and learning objectives:

Chapter 1: The Information Security Environment

- Justify an organizational code of ethics.
- Relate confidentiality, integrity, availability, non-repudiation, authenticity, privacy and safety to due care and due diligence.
- Relate information security governance to organizational business strategies, goals, missions, and objectives.
- Apply the concepts of cybercrime to data breaches and other information security compromises.
- Relate legal, contractual, and regulatory requirements for privacy and data protection to information security objectives.
- Relate transborder data movement and import-export issues to data protection, privacy, and intellectual property protection.

Chapter 2: Information Asset Security

- Relate the IT asset management and data security lifecycle models to information security.
- Explain the use of information classification and categorization, as two separate but related processes.
- Describe the different data states and their information security considerations.
- Describe the different roles involved in the use of information, and the security considerations for these roles.
- Describe the different types and categories of information security controls and their use.
- Select data security standards to meet organizational compliance requirements.

Chapter 3: Identity and Access Management (IAM)

- Explain the identity lifecycle as it applies to human and nonhuman users.
- Compare and contrast access control models, mechanisms, and concepts.
- Explain the role of authentication, authorization, and accounting in achieving information security goals and objectives.
- Explain how IAM implementations must protect physical and logical assets.
- Describe the role of credentials and the identity store in IAM systems.

Chapter 4: Security Architecture and Engineering

- Describe the major components of security engineering standards.
- Explain major architectural models for information security.
- Explain the security capabilities implemented in hardware and firmware.

- Apply security principles to different information systems architectures and their environments.
- Determine the best application of cryptographic approaches to solving organizational information security needs.
- Manage the use of certificates and digital signatures to meet organizational information security needs.
- Discover the implications of the failure to use cryptographic techniques to protect the supply chain.
- Apply different cryptographic management solutions to meet the organizational information security needs.
- Verify cryptographic solutions are working and meeting the evolving threat of the real world.
- Describe defenses against common cryptographic attacks.
- Develop a management checklist to determine the organization's cryptologic state of health and readiness.

Chapter 5: Communication and Network Security

- Describe the architectural characteristics, relevant technologies, protocols and security considerations of each of the layers in the OSI model.
- Explain the application of secure design practices in developing network infrastructure.
- Describe the evolution of methods to secure IP communications protocols.
- Explain the security implications of bound (cable and fiber) and unbound (wireless) network environments.
- Describe the evolution of, and security implications for, key network devices.
- Evaluate and contrast the security issues with voice communications in traditional and VoIP infrastructures.
- Describe and contrast the security considerations for key remote access technologies.
- Explain the security implications of software-defined networking (SDN) and network virtualization technologies.

Chapter 6: Software Development Security

- Recognize the many software elements that can put information systems security at risk.
- Identify and illustrate major causes of security weaknesses in source code.
- Illustrate major causes of security weaknesses in database and data warehouse systems.
- Explain the applicability of the OWASP framework to various web architectures.
- Select malware mitigation strategies appropriate to organizational information security needs.
- Contrast the ways that different software development methodologies, frameworks, and guidelines contribute to systems security.
- Explain the implementation of security controls for software development ecosystems.
- Choose an appropriate mix of security testing, assessment, controls, and management methods for different systems and applications environments.

Chapter 7: Security Assessment and Testing

- Describe the purpose, process, and objectives of formal and informal security assessment and testing.
- Apply professional and organizational ethics to security assessment and testing.
- Explain internal, external, and third-party assessment and testing.
- Explain management and governance issues related to planning and conducting security assessments.
- Explain the role of assessment in data-driven security decision-making.

Chapter 8: Security Operations

- Show how to efficiently and effectively gather and assess security data.
- Explain the security benefits of effective change management and change control.
- Develop incident response policies and plans.
- Link incident response to needs for security controls and their operational use.
- Relate security controls to improving and achieving required availability of information assets and systems.
- Understand the security and safety ramifications of various facilities, systems, and infrastructure characteristics.

Chapter 9: Putting It All Together

- Explain how governance frameworks and processes relate to the operational use of information security controls.
- Relate the process of conducting forensic investigations to information security operations.
- Relate business continuity and disaster recovery preparedness to information security operations.
- Explain how to use education, training, awareness, and engagement with all members of the organization as a way to strengthen and enforce information security processes.
- Show how to operationalize information systems and IT supply chain risk management.

Note: Throughout this course, exam domains may be covered in several chapters. Included in the course is a table indicating where the exam outline objectives are covered in this course.

ACE Credit

The Official ISC2 CBK Training Seminar for the CISSP has earned ACE CREDIT. Students who complete the course can apply for two hours of lower division credit at participating universities and colleges. For more information click here.