CERTIFIED INFORMATION SYSTEMS SECURITY PROFESSIONAL

DURATION: 5 DAYS

COURSE OVERVIEW

The Official (ISC)2® CISSP® CBK® Review Seminar is the most comprehensive, complete review of information systems security concepts and industry best practices, and the only review course endorsed by (ISC)2. Review Seminars are held worldwide and conducted by (ISC) 2-authorized instructors, each of whom is up-to-date on the latest information security-related developments and is an expert in the specific domains.

TARGET AUDIENCE

IT professionals seeking to enhance their careers and gain credibility as information security specialists

COURSE OBJECTIVES

Best-practice information security management practices, including IS technical skills, risk management and business continuity planning.

1. Access control and physical security
2. Cryptography
3. Security architecture for applications and networks.

COURSE CONTENT

1. Access Control - a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.
2. Application Development Security - addresses the important security concepts that apply to application software development. It outlines the environment where software is designed and developed and explains the critical role software plays in providing information system security.

3. Business Continuity and Disaster Recovery Planning – for the preservation and recovery of business operations in the event of outages.
4. Cryptography - the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.
5. Information Security Governance and Risk Management - the identification of an organization's information assets and the development, documentation, and implementation of policies, standards, procedures, and guidelines. Management tools such as data classification and risk assessment/analysis are used to identify threats, classify assets, and to rate system vulnerabilities so that effective controls can be implemented.
6. Legal, Regulations, Investigations and Compliance
7. Computer crime laws and regulations
8. The measures and technologies used to investigate computer crime incidents
9. Operations Security - used to identify the controls over hardware, media, and the operators and administrators with access privileges to any of these resources. Audit and monitoring are the mechanisms, tools, and facilities that permit the identification of security events and subsequent actions to identify the key elements and report the pertinent information to the appropriate individual, group, or process.
10. Physical (Environmental) Security - provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.
11. Security Architecture and Design - contains the concepts, principles, structures, and standards used to design, monitor, and secure operating systems, equipment, networks, applications and those controls used to enforce various levels of availability, integrity, and confidentiality.
12. Telecommunications and Network Security
13. Network structures
14. Transmission methods
15. Transport formats
16. Security measures used to provide availability, integrity, and confidentiality
17. Authentication for transmissions over private and public communications networks and media

COURSE PREREQUISITES

The Official (ISC) 2 CISSP CBK Review Seminar offers a high-level review of the main topics and
identifies areas that students need to study and includes:

1. Post-Seminar Self-Assessment
2. 100% up-to-date material
3. Contributions from CISSPs, (ISC)2 Authorized Instructors and subject matter experts
4. An overview of the scope of the information security field