

Course Outline: CISSP

Learning Method: Instructor-led Classroom Learning

Duration: 7.00 Day(s)/ 56 hrs

Overview:

CISSP® Review Seminar is the most comprehensive review seminar discussing information systems security industry best practices, known as the (ISC)² CBK®. The review seminar helps you review the 10 domains of the information security practice. It also serves as a strong learning tool for mastering concepts and topics related to all aspects of information systems security.

Who Should Attend:

Network Administrators, Engineers, Auditors
 Enterprise Server Architects
 IT Managers, Directors, Analysts, Administrators
 Info Sec. Officers, Security Policy Specialists

At Course Completion:

The CISSP(R) credential demonstrates that an IT professional understands not just system security but a full range of security for the automated information system. With a growing emphasis on IT security, (ISC)2-certified personnel are exactly what organizations need to make their infrastructure stronger. A person with this certification is not only familiar with the technology, but knows how it fits in and how to meld it together with an organization's business needs. Join now and find out why this particular certification is quickly gaining in popularity

Pre-requisite(s):

The CISSP® is targeted at professionals with at least 4 years experience in the information security field or 3 years experience and a college degree. This is a requirement - to complete your certification you must document this minimum level of experience. If you do not have this level of experience you should not consider enrollment in this program.

Phone: +357 70002770
www.computrain.com.cy



Outline:

Lesson 1: Access Control

Access controls are a collection of mechanisms that work together to create security architecture to protect the assets of the information system.

Lesson 2: Application Security

This domain 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.

Lesson 3: Business Continuity and Disaster Recovery Planning

The Business Continuity Plan (BCP) domain addresses the preservation and recovery of business operations in the event of outages.

Lesson 4: Cryptography

The cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.

Lesson 5: Information Security and Risk Management

Security management entails 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.

Lesson 6: Legal, Regulations, Compliance and Investigations

The Law, Investigations, and Ethics domain addresses:

- Computer crime laws and regulations
- The measures and technologies used to investigate computer crime incidents

Lesson 7: Operations Security

Operations Security is 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

Phone: +357 70002770
www.computrain.com.cy



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.

Lesson 8: Physical (Environmental) Security

The Physical (Environmental) Security domain provides protection techniques for the entire facility, from the outside perimeter to the inside office space, including all of the information system resources.

Lesson 9: Security Architecture and Design

The Security Architecture and Design domain 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.

Lesson 10: Telecommunications and Network Security

The telecommunications, network, and Internet security domain discusses the:

- Network Structures
- Transmission methods
- Transport formats
- Security measures used to provide availability, integrity, and confidentiality
- Authentication for transmissions over private and public communications networks and media.

Phone: +357 70002770
www.computrain.com.cy

