

## **CISSP - Certified Information Systems Security Professional**

The (ISC)<sup>2</sup> CISSP ® CBK ® Review Seminar is the most comprehensive, complete review of information systems security concepts and industry best practices. The (ISC)<sup>2</sup> CISSP CBK Review Seminars are held worldwide and usually have a five-day schedule, from Monday to Friday.

The Review Seminar:

- Offers a high-level review of the main topics.
- Identifies areas students need to study.
- Provides an overview of the scope of the field.

The course material, covering the 10 CISSP domains of the CBK, is redesigned and updated for every Review Seminar to reflect the latest information system security issues, concerns, and countermeasures. The following domains are covered in the seminar modules.

- Access Control - Access Controls are a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.
- 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.
- Business Continuity and Disaster Recovery Planning - This domain addresses the preservation and recovery of business operations in the event of outages.
- Cryptography - The Cryptography domain addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.
- 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.
- Legal, Regulations, Compliance, and Investigation - This domain addresses:
  - Computer crime laws and regulations
  - The measures and technologies used to investigate computer crime incidents
- 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 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.
- 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.

## *CISSP Certification*

- 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.
- Telecommunications and Network Security - The Telecommunications and Network 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

For more details please contact (ISC)<sup>2</sup> education partners in Malta:

Computer Domain  
Curate Schembri Street  
Mosta MST 1176

Tel: 21-433 688. 27-433 688

Email: [courses@computerdomain.net](mailto:courses@computerdomain.net)

Web site: [www.computerdomain.net](http://www.computerdomain.net)