

Conquering the Ten Domains of the (ISC)² CBK®

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.

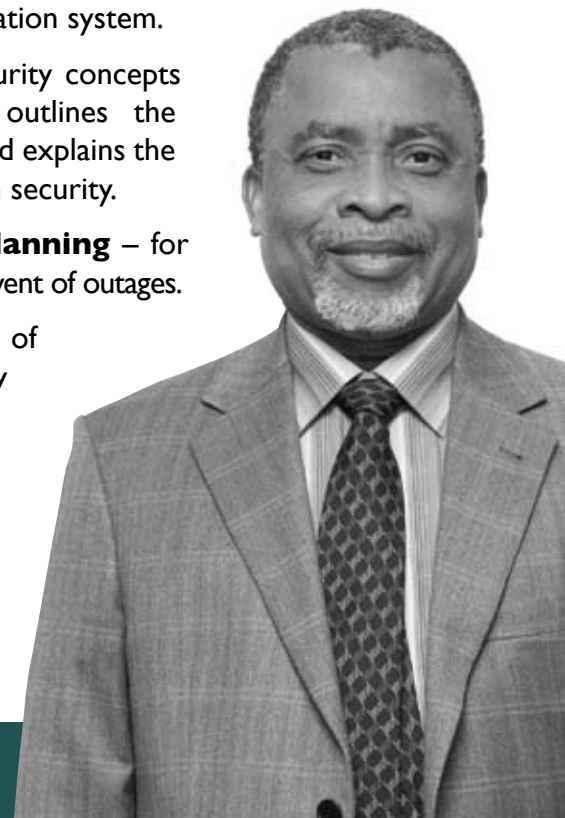
The Official (ISC)² CISSP CBK Review Seminar offers a high-level review of the main topics and identifies areas that students need to study and includes:

- Post-Seminar Self-Assessment
- 100% up-to-date material
- Contributions from CISSPs, (ISC)²-authorized instructors and subject matter experts
- An overview of the scope of the information security field

Official (ISC)² CBK Review Seminars are available throughout the world at (ISC)² facilities and through (ISC)² Authorized Education Affiliates. Each official class is taught by an authorized (ISC)² instructor to ensure the highest quality education. If your study time is limited, our online education offerings are available for your convenience.

The course material, covering the ten 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** - a collection of mechanisms that work together to create a security architecture to protect the assets of the information system.
- **Application 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.
- **Business Continuity and Disaster Recovery Planning** – for the preservation and recovery of business operations in the event of outages.
- **Cryptography** - the principles, means, and methods of disguising information to ensure its integrity, confidentiality and authenticity.
- **Information Security 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.

- **Legal, Regulations, Compliance and Investigation**

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

- **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.

- **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.

- **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.

- **Telecommunications and Network Security**

- 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

There are several organizations that teach (ISC)² review courses that make unauthorized claims of higher than average test scores and inflated pass rates. A candidate should be cautious since test scores or pass rates are never revealed. Be sure you are taking an Official (ISC)² CISSP® CBK® Review Seminar from an authorized provider.

For additional details on the CISSP Review Seminar, visit www.isc2.org/cissprevsem.

(ISC)² is the premier not-for-profit organization dedicated to certifying information security professionals around the globe. With tens of thousands of credentialed specialists worldwide, (ISC)² is dedicated to helping both the certified individual and their organization be successful in the information security industry. Indeed, our credentials are considered the Gold Standard in information security. So (ISC)² is the logical first contact for anyone serious about protecting information assets at an unsurpassed level of excellence.