



CISSP: Applications & Systems Development Security



CISSP: Applications & Systems Development Security

1 Session –

3 Hours of Interactive Training

Applications & Systems Development Security is one of 10 domains comprising the Certified Information Systems Security Professional (CISSP) Common Body of Knowledge (CBK). In this CISSP certification prep course from LearnKey, expert instructor Michael Solomon goes over software development, databases, data storage, and common attacks that must be protected against. At the conclusion of this course, you will be familiar with the issues and concepts of the Application & System Development domain required to pass the CISSP exam.

Also Available:

- Test Prep

About The Author

Michael Solomon, CISSP, TICSA, is a security consultant and trainer. Since 1987 he has worked with more than 60 organizations including Earthlink, Nike, Lucent Technologies, BellSouth, and UPS. Solomon holds Computer Science from Emory University (1998), and has contributed to or co-authored information security certification study guides for Que, Sybex and other publishers.

Session 1

Section A: Application Issues

- Software Development
- Application Environments
- Malicious Code
- Agents
- Applets
- Objects

Section B: Databases & Data Warehousing

- Databases
- Relational Database
- Record Identification
- Query Language
- Data Warehouses
- Aggregation
- Interference
- Polymorphism

Section C: Data & Information Storage

- Data Handling
- Data Storage
- Virtual Memory
- Information Retrieval
- Knowledge-based Systems

Audit and Assurance Mechanisms

Section D: System Development Controls

- Coding Controls
- Development Life Cycle
- Design
- Certification
- Certification Standards

Section E: Security Development Controls

- Isolation Architecture
- Administration Control
- Design Control
- System Control
- Modes of Operation
- Integrity Levels
- Service Level Agreement

Section F: Malicious Code

- Overview
- Players
- Viruses
- Virus Types
- OS Vulnerability
- Other Malicious Code
- Anti-virus Protection

Section G: Methods of Attack

- Brute Force
- Social Engineering
- DoS/DDoS
- Spoofing
- Pseudo Flaw
- Buffer Overflows
- TOC/TOU
- Root Kits