Certified Information Systems Auditor CISA, Part 5 of 5: Protecting Assets

Meet the expert: As a certified Microsoft Instructor, Ken has focused his career on various security aspects of computer and network technology since the early 1980s. He has offered a wide variety of IT training and high level consulting projects for Fortune 500 companies globally. Through the course of his extensive career, he has taught a full line of Microsoft, CompTIA, Cisco, and other high level IT Security curricula.

Prerequisites: This is part 5 of the series.

Runtime: 02:26:48

Course description: The objective of this course is to ensure enterprise security policies, standards procedures and controls will ensure confidentiality, integrity and availability of information assets. This course will cover standards and procedures, evaluate design and monitoring of systems, data classification, physical access, environmental controls and safeguards as well as retrieval and disposal of information assets. This course is part of a series covering the ISACA Certified Information Systems Auditor (CISA).

Course outline:

Importance of Information Security
- Introduction
- The Myth of Perfect Security
- Inventory and Classification of Information Assets
- Controls
- Privacy Management Issues
- Critical Success Factors to Info Sec Management
- Info Sec and External Parties
- Risks Related to External Parties
- Customers and Security
- Addressing Security and Third-Party Agreements
- Human Resources Security
- Human Resources Security Continued
- Computer Crime Issues and Exposures
- Computer Crime Issues and Exposures Continued
- Types of Computer Crimes
- Web-Based Technologies
- Security Incident Handling and Response
- Summary

Logical Access
- Introduction
- Logical Access Controls
- Logical Access and Points of Entry
- Logical Access Control Software
- Identification and Authentication
- Multifactor Authentication
- Features of Passwords
- Identification and Authentication Best Practices
- Token Devices and One-Time Passwords
- Effective Biometric Security
- Single Sign-On
- Authorization Issues
- Access Lists
- Common Connectivity Methods
- Remote Wireless Connections
- Access Issues with Mobile Technology
- Access Rights to System Logs
- Use of Intrusion Detection
- Dealing with Confidential Information
- Summary

Network Infrastructure Security
- Introduction
- LAN Security
- LAN Virtualization
- Client/Server Security
- Wireless Security Threats and Risk Mitigation
- Internet Vulnerabilities
- Network Security Threats
- Controls to Investigate
- Firewall Security Systems
- Common Attacks Against Firewalls
- Examples of Firewall Implementation
- Intrusion Detection
- Describing IDS and IPS Deployment
- Encryption
- Symmetric and Asymmetric Encryption
- Uses of Encryption
- Viruses
- Technical Controls Against Viruses
- Anti-Virus Software
- Voice Over IP
- Private Branch Exchange
- Summary

Auditing Info Sec Management Framework
- Introduction
- Auditing Info Sec Management Framework
- Auditing Logical Access
- Techniques for Testing Security
- Summary

Auditing Network Infrastructure Security
- Introduction
- Auditing Remote Access
- Network Penetration Test
- Types of Penetration Tests
- Full Network Assessment Reviews
- Authorized Network Configuration Changes
- Unauthorized Changes
- Computer Forensics
- Chain of Evidence
- Summary

Environmental Exposure and Physical Access
- Introduction
- Environmental Exposures and Controls
- Physical Access Exposures
- Physical Access Controls
- Auditing Physical Access
- Mobile Computing
- Summary