CISSP Certified Information Systems Security Professional

Meet the expert: Kevin is an international author, consultant and international >speaker. He is the official course development writer for ISC2 CISSP, ISACA CRISC

and mile2’s C)ISSO. Kevin has been educating IT professionals for over 30 years. He

also provides cyber security consulting and support services for organizations

around the world. Assisting them with setting up Information Security programs and

addressing areas ranging from in-depth risk analysis to policy creation and security

awareness.

Prerequisites: None

Runtime: 22:08:43

Course description: The Certified Information Systems Security Professional (CISSP) demonstrates a globally recognized standard of competence which covers critical topics in security today, including cloud computing, mobile security, application development security, risk management and more. The CISSP draws from a comprehensive, up-to-date, global common body of knowledge that ensures security leaders have a deep knowledge and understanding of new threats, technologies, regulations, standards, and practices.

This course is a brief Overview

Course outline:

Risk Definitions
- Introduction
- Risk Management Flow
- Risk Definitions
- What Is the Value of an Asset
- What Is a Threat Source/Agent
- What Is a Threat
- What Is a Vulnerability
- Examples of Non-Obvious Vulnerabilties
- What Is a Control
- What is Likelihood
- What Is Impact
- Control Effectiveness
- Summary

Risk Management
- Introduction
- Agenda
- Risk Management
- Risk Response and Monitoring
- Purpose of Risk Management
- Summary

Risk Assessment
- Introduction
- Risk Assessment
- Why Is Risk Assessment Difficult
- Different Approaches to Analysis
- Quantitative Analysis
- Threat Analysis and Annual Loss Expectency
- Quantitative Analysis Continued
- ALE Value Uses
- Qualitative Analysis: Likelihood
- Qualitative Analysis - Impact
- Qualitative Analysis - Risk Level
- Qualitative Analysis Steps
- Summary

Responding to Risk
- Introduction
- Completion of Risk Assessment
- Risk Response
- Management's Response to Identified Risks
- Summary

Understanding Security
- Introduction
- What Is Information Security
- What Is Information Security Continued
- The Information Security Triad
- Understanding the Business
- Summary

Security Controls
- Introduction
- Setting up a Security Program
- Enterprise Security Program
- Building a Foundation
- Planning Horizon Components
- Enterprise Security: The Business Requirements
- Enterprise Security Program Components
- Control Types
- "Soft" Controls
- Technical or Logical Controls
- Physical Controls
- Roadmap to Maturity
- Program Monitoring
- Summary

Roles and Responsibilities
- Introduction
- Senior Management's Role in Security
- Security Roles and Responsibilities
- Roles and Responsibilties
- Agenda
- Security Program Components
- Information Security Policy
- Security Policy Review
- Implementing Policy
- Summary

Human Resources
- Introduction
- Agenda
- Security and the Human Factors
- Employee Management
- Human Resources Issues
- Importance to Security
- Recruitment Issues
- Termination of Employment
- Human Resources Practices
- Types of Training
- Quality Training
- Informing Employees About Security
- Enforcement
- Security Enforcement Issues
- Summary
- Summary

Access Control Methodology
- Introduction
- Access Control Administration
- Accountability and Access Control
- Trusted Path
- Who Are You?

(Continued on page 2)

CISSP Certified Information Systems Security Professional

- Authentication Mechanism
- Strong Authentication
- Authorization
- Access Criteria
- Fraud Controls and Access Control Mechanisms
- Summary

Biometrics and Passwords
- Introduction
- Biometric Technology
- Biometrics Enrollment Process
- Downfalls to Biometric Use
- Biometrics Error Types
- Biometrics Diagram
- Biometric System Types
- Agenda
- Passwords and PINs
- Password Shoulds
- Password Attacks
- Countermeasures for Password Cracking
- Cognitive Password
- One-Time Password Authentication
- Agenda
- Synchronous Token
- Asynchronous Token Device
- Cryptographic Keys
- Passphrase Authentication
- Memory Cards and Smart Cards
- Summary

Single Sign-on
- Introduction
- Single Sign-on Technology
- Different Technologies
- Scripts and Directory Services
- Thin Clients
- Kerberos as a Single Sign-on Technology
- Tickets
- Kerberos Components Working Together
- Major Components of Kerberos
- Kerberos Authentication Steps
- Purpose of Kerberos
- Issues Pertaining to Kerberos
- SESAME as a Single Sign-on Technology
- Federated Authentication
- Summary

Intrusion Detection Systems
- Introduction
- Host-Based IDS
- Network-Based IDS Sensors
- Types of IDSs
- Behavior-Based IDS
- IDS Response Mechanisms
- IDS Issues
- Trapping an Intruder
- Summary
- Summary

Access Control Types
- Introduction
- Role of Access Control
- Definitions
- More Definitions
- Layers of Access Control
- Layers of Access Control Continued
- Access Control Mechanism Examples
- Access Control Characteristics
- Summary

More Access Control Types
- Introduction
- Preventative Control Types
- Administrative Controls
- Controlling Access
- Other Ways of Controlling Access
- Technical Access Controls
- Physical Access Controls
- Accountability
- Threats to Access Control
- Control Combinations
- Summary

Information Classification
- Introduction
- Information Classification
- Information Classification Criteria
- Declassifying Data
- Types of Classification Levels
- Summary

Access Control Models
- Introduction
- Models for Access
- Discretionary Access Control
- Enforcing a DAC Policy
- Mandatory Access Control Model
- MAC Enforcement Mechanism: Labels
- Where Are They Used?
- Role-Based Access Control
- Acquiring Rights and Permissions
- Rule-Based Access Control
- Access Control Matrix
- Access Control Administration
- Access Control Methods
- Network Access Control
- Policy on Network Services
- Remote Centralized Administration
- RADIUS Charcteristics
- TACACS+ Characteristics
- Diameter Characteristics
- Decentralized Access Control Administration
- Summary
- Summary

Trusted Computing Base
- Introduction
- System Protection: Trusted Computing Base
- System Protection: Reference Monitor
- Security Kernel Requirements
- Summary

Protection Mechanisms
- Introduction
- Security Modes of Operation
- System Protection: Levels of Trust
- System Protection: Process Isolation
- System Protection: Layering
- System Protection: Application Program Interface
- System Protection: Protection Rings
- What Does It Mean to Be in a Specific Ring
- Summary

Security Models
- Introduction
- Security Models
- Security Models Continued
- State Machine
- Information Flow
- Bell-LaPadula
- Rules of Bell-LaPadula
- Biba
- Clark-Wilson Model
- Non-Interference Model
- Brewer and Nash: Chinese Wall
- Take-Grant Model
- Summary

Evaluation Criteria
- Introduction
- Trusted Computer System Evaluation Criteria
- TCSEC Rating Breakdown
- Evaluation Criteria: ITSEC
- Comparison of Ratings
- ITSEC: Good and Bad
- Common Criteria
- Common Criteria Components
- First Set of Requirements
- Second Set of Requirements
- Package Ratings
- Common Criteria Outline
- Certification vs. Accreditation
- Summary
- Summary

Admin Responsibilities
- Introduction
- Operations Issues
- Role of Operations
- Administrator Access
- Computer Operations: System Administrators
- Security Administrator
- Operational Assurance
- Audit and Compliance
- Some Threats to Computer Operations
- Specific Operations Tasks
- Agenda
- Product Implementation Concerns
- Logs and Monitoring
- Records Management
- Change Control
- Resource Protection
- Contingency Planning
- System Controls
- Trusted Recovery
- Summary

Redundancy and Fault Tolerance
- Introduction
- Fault-Tolerance Mechanisms
- Duplexing, Mirroring, And Checkpointing
- Redundant Array of Independent Disks
- Fault Tolerance
- Redundancy Mechanism
- Backups
- Backup Types
- Summary

Operational Issues
- Introduction
- Remote Access
- Facsimilie Security
- Email Security
- Before Carrying out Vulnerability Testing
- Vulnerability Assessments
- Methology
- Penetration Testing
- Ethical Hacking
- Hack and Attack Strategies
- Protection Mechanism: Honeypot
- Summary

Threats to Operations
- Introduction
- Threats to Operations
- Data Leakage: Social Engineering
- Data Leakage - Object Reuse
- Object Reuse
- Why Not Just Delete the File or Format the Disk
- Data Leakage: Keystroke Logging
- Data Leakage: Emanation
- Controlling Data Leakage: TEMPEST
- Controlling Data Leakage: Control Zone
- Controlling Data Leakage: White Noise
- Summary
- Summary

Cryptography Terms

CISSP Certified Information Systems Security Professional

- Cryptography Objectives
- Cryptographic Definitions
- A Few More Definitions
- Some More Definitions
- Symmetric Cryptography: Use of Secret Keys
- Summary

Historical Uses of Cryptography
- Introduction
- Cryptography Uses Yesterday and Today
- Historical Uses of Symmetric Cryptography
- Scytale Cipher
- Substitution Cipher
- Caesar Cipher Example
- Vigenere Cipher
- Polyalphabetic Substitution and Vigenere Example
- Enigma Machine
- Vernam Cipher
- Running Key and Concealment
- Summary

Cryptography Foundations
- Introduction
- One-Time Pad Characteristics
- Binary Mathmatical Fuction
- Key and Algorithm Relationship
- 128-Bit Keys vs. 64-Bit Keys
- Breaking Cryptosystems: Brute Force
- Breaking Cryptosystems: Frequency Analysis
- Determining Strength in a Cryptosystem
- Characteristics of Strong Algorithms
- Open or Closed
- Summary

Modern Cryptography
- Introduction
- Types of Ciphers Used Today
- Encryption/Decryption Methods
- Symmetric Ciphers: Block Cipher
- S-Boxes Used in Block Ciphers
- Symmetric Ciphers: Stream Cipher
- Encryption Process and Symmetric Characteristics
- Strength of a Stream Cipher
- Let's Dive in Deeper
- Symmetric Key Cryptography
- Symmetric Key Management Issue
- Summary

Symmetric Algorithms
- Introduction
- Symmetric Algorithms Examples
- Symmetric Downfalls
- Secret vs. Session Keys
- Symmetric Algorithms: DES
- Evolution of DES
- Block Cipher Modes: CBC
- Symmetric Ciphers: AES
- Other Symmetric Algorithms
- Agenda
- MAC- Sender
- Hashing Algorithms
- Protecting the Integrity of Data
- Data Integrity Mechanisms
- Weakness in Using Only Hash Algorithms
- More Protection in Data Integrity
- Security Issues in Hashing
- Birthday Attack
- Summary
- Summary

Asymmetric Cryptography
- Introduction
- Asymmetric Cryptography
- Public Key Cryptography Advantages
- Asymmetric Algorithm Disadvantages
- Symmetric vs. Asymmetric
- Asymmetric Algorithms
- Asymmetric Algorithm: Diffie-Hellman
- Asymmetric Algorithms: RSA
- Asymmetric Algorithms: El Gamal and ECC
- Example of Hybrid Cryptography
- When to Use Which Key
- Using the Algorithm Types Together
- Digital Signatures
- Digital Signature and MAC Comparison
- What if You Need All of the Services?
- U.S. Government Standard
- Summary

Public Key Infrastructure
- Introduction
- Why Do We Need a PKI
- Environment
- PKI and Its Components
- CA and RA Roles
- Let's Walk Through an Example
- Digital Certificates
- What Do You Do with a Certificate?
- Components of PKI: Repository and CRLs
- Summary

Cryptography and Attacks
- Introduction
- Cryptography and Attacks
- Steganography
- Key Management
- Link vs. End-to-End Encryption
- End-to-End Encryption
- Email Standards
- Secure Protocols
- SSL and the OSI Model
- SSL Connection Setup
- Secure Email Standard
- SSH Security Protocol
- Network Layer Protection
- IPSec Key Management
- Key Issues Within IPSec
- IPSec Handshaking Process
- SAs in Use
- IPSec Is a Suite of Protocols
- IPSec Modes of Operation
- Attacks on Cryptosystems
- More Attacks
- Summary
- Summary

Network Communications Security
- Introduction
- Network Security Issues
- Network and Communications Security
- Communications Security
- Network Security Methods
- Network-Based Security Problems
- Summary

Network Topologies
- Introduction
- Network Topologies: Physical Layer
- Topology Type: Bus
- Topology Type: Ring
- Topology Type: Star
- Network Topologies: Mesh
- Summary of Topologies
- LAN Media Access Technologies
- One Goal of Media Access Technologies
- Transmission Types: Analog and Digital
- Transmission Types: Synchronous and Asynchronous
- Two Types of Carrier Sense Multiple Access
- Transmission Types: Number of Receivers
- Media Access Technologies: Ethernet
- Media Access Technologies: Token Passing
- Media Access Technologies: Polling
- Summary

Network Technologies and Cabling
- Introduction
- Cabling
- Cabling Types: Coaxial
- Cabling Types: Twisted Pair
- Cabling Issues: Plenium-Rated
- Types of Networks
- Network Technologies
- Network Configurations
- MAN Technologies: SONET
- Wide Area Network Technologies
- Cicuit Switching
- WAN Technologies: ISDN
- ISDN Service Types
- WAN Technologies: DSL
- WAN Technologies: Cable Modem
- Packet Switching
- WAN Technologies: Packet Switched
- Packet Switched Networks
- WAN Technologies: X.25
- WAN Technologies: Frame Relay
- WAN Technologies: ATM
- Multiplexing
- Permanent Virtual Circuits
- Summary

OSI Model
- Introduction
- OSI Model
- An Older Model
- Data Encapsulation
- OSI: Application Layer
- OSI: Presentation Layer
- OSI: Session Layer
- OSI: Transport Layer
- OSI: Network Layer
- OSI: Data Link Layer
- OSI: Physical Layer
- Protocols at Each Layer
- Summary

Network Devices
- Introduction
- Devices Work at Different Layers
- Networking Devices
- Repeater
- Hub
- Bridge
- Switch
- Virtual LAN
- Router
- Gateway
- Summary

Network Security Sentries
- Introduction
- Bastion Host
- Firewalls
- Firewall: First Line of Defense
- Firewall Types: Packet Filtering
- Firewall Types: Proxy Firewalls
- Firewall Types: Circuit-Level Proxy Firewall
- Type of Circuit-Level Proxy: SOCKS
- Firewall Types: Application-Layer Proxy
- Firewall Types: Stateful
- Firewall Types: Dymanic Packet-Filtering

(Continued on page 4)

CISSP Certified Information Systems Security Professional

- Firewall Types: Kernel Proxies
- Firewall Placement
- Firewall Architecture Types: Screened Host
- Firewall Architecture Types: Multi- or Dual-Homed
- Firewall Architecture Types: Screened Subnet
- IDS: Second Line of Defense
- IPS Last Line of Defense
- HIPS
- Unified Threat Management
- UTM Product Criteria
- Summary

Protocols and Services
- Introduction
- Protocols
- Port and Protocol Relationship
- Conceptual Use of Ports
- UDP vs. TCP
- TCP/IP Suite
- Protocols: ARP
- Protocols: ICMP
- Protocols: SNMP
- Protocols: SMTP
- Protocols: FTP, TFTP, and Telnet
- Protocols: RARP and BootP
- Network Service: DNS
- Network Service: NAT
- Summary
- Summary

Telephony
- Introduction
- PSTN
- Remote Access
- Dial-Up and Authentication Protocols
- Dial-Up Protocol: SLIP
- Dial-Up Protocol: PPP
- Auhtentication Protocols: PAP and CHAP
- Voice Over IP
- Private Branch Exchange
- PBX Vulnerabilities
- PBX Best Practices
- Summary

VPN
- Introduction
- Virtual Private Network Technologies
- What Is a Tunneling Protocol
- Tunneling Protocols: PPTP
- Tunneling Protocols: L2TP
- Tunneling Protocols: IPSec
- IPSec: Network Layer Protection
- IPSec
- SSL/TLS
- Summary

Wireless
- Introduction
- Wireless Technologies: Access Point
- Standards Comparison
- Wireless Network Topologies
- Wi-Fi Network Types
- Wireless Technologies: WTLS
- Wireless Technologies: Service Set ID
- Wireless Technologies: Authenticating to an AP
- Wireless Technologies: WEP
- Wireless Technologies: More WEP Woes
- How WPA Improves on WEP
- TKIP
- The WPA MIC Vulnerability
- 802.11i: WPA2
- WPA and WPA2 Mode Types
- WPA-PSK Encryption
- Wireless Technologies: WAP
- WTLS
- Summary

Network-Based Attacks
- Introduction
- Wireless Technologies: Common Attacks
- Wireless Technologies: War Driving
- Kismet
- Wireless Technologies: Countermeasures
- Network Based Attacks
- ARP Attacks and DDoS Issues
- Man-in-the-Middle
- Traceroute Operation
- Summary
- Summary

Security Architecture
- Introduction
- ESA Definition
- What Is Architecture?
- Architecture Components
- Objectives of Security Architecture
- Technology Domain Modeling
- Integrated Security is Designed Security
- Security by Design
- Summary

Architectural Models
- Introduction
- Architectural Models
- Virtual Machines
- Cloud Computing
- Summary

Components and Threats
- Introduction
- Memory Types
- Virtual Memory
- Memory Management
- Accessing Memory Securely
- Different States and System Functionality
- Types of Compromises
- Disclosing Data in an Unauthorized Manner
- Circumventing Access Controls
- Attacks
- Attack Type: Race Condition
- Attack Type: Data Validation
- Attacking Through Applications
- Buffer Overflow
- Attack Characteristics
- Attack Types
- More Attacks
- Host Name Resolution Attacks
- Even More Attacks
- Watching Network Traffic
- Traffic Analysis
- Cell Phone Cloning and Illegal Activities
- Summary
- Summary

Software Security Concerns
- Introduction
- How Did We Get Here
- Device vs. Software Security
- Why Are We Not Improving at a Higher Rate
- Usual Trend of Dealing with Security
- Where to Implement Security
- The Objective
- Systems Security
- Systems Security
- Programming Environment
- Security of Embedded Systems
- Summary

Software Lifecycle Process
- Introduction
- SDLC
- Integration of Risk Management into the SDLC
- Development Methodologies
- Maturity Models
- Secure Programming
- Programming Errors
- Security Issues
- Outsourced Development
- Trusted Program Modules
- Middleware
- Summary

Web Application Security
- Introduction
- OWASP Top Ten
- Modularity of Objects
- Object-Oriented Programming Characteristic
- Module Characteristics
- Linking Through COM
- Mobile Code with Active Content
- World Wide Web OLE
- ActiveX Security
- Java and Applets
- Common Gateway Interface
- Cookies
- PCI Requirements
- PA-DSS Requirements
- Vendor-Supplied Software
- Virtual Systems
- Virtualization Types
- Cloud Computing
- Summary
- Summary

Database Models
- Introduction
- Database Models
- Database Models: Hierarchical and Distributed
- Database Models: Relational
- Database Systems
- Database Models: Relational Components
- Foreign Key
- Database Component
- Database Security Mechanisms
- Database Data Integrity Controls
- Add-On Security
- Database Security Issues
- Controlling Access
- Database Integrity
- Data Warehousing
- Data Mining
- Summary

Software Development
- Introduction
- Artificial Intelligence
- Expert System Components
- Artificial Neural Networks
- Software Development Models
- Project Development: Phases III, IV, and V
- Project Development: Phases VI and VII
- Verification vs. Validation
- Evaluating the Resulting Product
- Controlling How Changes Take Place
- Change Control Process
- Administrative Controls
- Summary

Malware Attacks
- Introduction
- Malware Attacks
- Virus
- More Malware
- Rootkits and Backdoors
- DDoS Attack Types

(Continued on page 5)

CISSP Certified Information Systems Security Professional

- Escalation of Privilege
- DDoS Issues
- Buffer Overflow
- Mail Bombing and Email Links
- Phishing
- Replay Attack
- Cross-Site Scripting Attack
- Timing Attacks
- More Advanced Attacks
- Summary
- Summary

Project Initiation
- Introduction
- Phases of Plan
- Pieces of the BCP
- BCP Development
- Where Do We Start
- Why Is BCP a Hard Sell to Management
- Understanding the Organization
- BCP Committee
- Summary

Business Impact Analysis
- Introduction
- BCP Risk Analysis
- Identifying Threats and Vulnerabilties
- Categories
- How to Identify the Critical Company Functions
- Loss Criteria
- Interdependencies
- Choosing Offsite Services
- Functions' Resources
- Calculating MTD
- Recovery Point Objective
- Recovery Strategies
- What Items Need to Be Considered in a Recovery
- Facility Backups
- Compatibility Issues with Offsite Facility
- Which Do We Use?
- Choosing Site Location
- Other Offsite Approaches
- BCP Plans Become out of Date
- Summary
- Summary

Disaster Preparation
- Introduction
- Proper Planning
- Executive Succession Planning
- Preventing a Disaster
- Preventative Measures
- Backup/Redundancy Options
- Disk Shadowing
- Hierarchical Storage Management
- SAN
- Co-Location
- Other Options
- Summary

Development Plan
- Introduction
- Review: Results from the BIA
- Now What
- Priorities
- Plan Objectives
- Defining Roles
- The Plan
- Types of BC Plans
- Recovery
- Damage Assessment
- Coordination Procedures
- Sequence of Recovery Options
- Relocate to the Alternate Facility
- Restoration of Primary Site
- Return to Normal Operations
- Summary

Emergency Response
- Introduction
- Environment
- Operational Planning
- Emergency Response
- Revieing Insurance
- When Is the Danger Over
- Testing and Drills
- Types of Tests
- What Is Success
- Summary
- Summary

Incident Management
- Introduction
- Seriousness of Computer Crimes
- Incidents
- Incident Management Priorities
- Incident Response Capability
- Incident Management Requires
- Preparing for a Crime Before It Happens
- Incident Response Phases
- Summary

Law
- Introduction
- Types of Law
- Foundational Concepts of Law
- Common Laws: Criminal
- Common Laws: Civil
- Common Laws: Administrative
- Intellectual Property Laws
- Software Licensing
- Summary

Computer Crime
- Introduction
- Historic Examples of Computer Crimes
- Who Perpetrates These Crimes
- Types of Motivation for Attacks
- Telephone Fraud
- Identification Protection and Prosecution
- Computer Crime and Its Barriers
- Countries Working Together
- Security Principles for International Use
- Determine if a Crime Has Been Committed
- When Should Law Enforcement Get Involved
- Citizen vs. Law Enforcement Investigation
- Investigation of Any Crime
- Summary

Evidence Handling
- Introduction
- Role of Evidence in a Trial
- General Rules for Evidence
- Evidence Requirements
- Evidence Collection Topics
- Chain of Custody and Evidence Processing
- Evidence Types
- Hearsay Rule Exception
- Privacy of Sensitive Data
- Privacy Issues: US Laws as Examples
- European Union Principles on Privacy
- Employee Privacy Issues
- Computer Forensics
- Trying to Trap the Bad Guy
- Companies Can Be Found Liable
- Sets of Ethics
- Ethics
- Summary
- Summary

Physical Security
- Introduction
- Physical Security
- Physical Security: Threats
- Different Types of Threats and Planning
- Facility Site Selection
- Devices Will Fail
- Controlling Access
- External Boundary Protection
- Lock Types
- Facility Access and Piggybacking
- Securing Mobile Devices
- Entrance Protection
- Perimeter Protection
- Perimeter Security
- Types of Physical IDS
- Sensors
- Facility Attributes
- Electrical Power
- Problems with Steady Power Current
- Power Interference And Preventative Measures
- Environmental Considerations
- Fire Prevention
- Fire Detection
- Fire Types
- Supression Methods
- Fire Extinguishers
- Summary

Security and Risk Management
- Introduction
- Overview
- Confidentiality, Integrity, and Availability
- Security Governance Principles
- Compliance
- Legal and Regulatory Issues
- Ethics
- Business Continuity Requirements
- Personnel Security Policies
- Risk Management Concepts
- Threat Modeling
- Security Risk Considerations
- Education, Training, and Awareness
- Summary
- Summary

Asset Security
- Introduction
- Overview
- Classify Information and Supporting Assets
- Determine and Maintain Ownership
- Protect Privacy
- Ensure Appropriate Retention
- Determine Data Security Controls
- Establish Handling Requirements
- Summary
- Summary

Security Engineering
- Introduction
- Overview
- Engineering Processes
- Fundamental Concepts of Security Models
- Controls and Countermeasures
- Security Capabilites of Information Systems
- Mitgate Vulnerabilities
- Cryptography
- Security Principles
- Physical Security
- Summary

Communication and Network Security
- Introduction
- Overview
- Secure Network Architecture Design Principles

- Secure Network Components
- Secure Communications Channels
- Prevent or Mitigate Network Attacks
- Summary

Identity and Access Management
- Introduction
- Overview
- Physical and Logical Access to Assets
- Identification and Authorization
- Identity Services
- Authorization Mechanisms
- Access Control Attacks
- Summary
- Summary

Security Assessment Testing
- Introduction
- Overview
- Assessment and Test Strategies
- Security Control Testing
- Security Process Data
- Analyze and Report Test Outputs
- Summary
- Summary

Security Operations
- Introduction
- Overview
- Understanding Investigations
- Requirements for Investigation Types
- Logging and Monitoring Activities
- Resource Provisioning
- Foundational Security Operations Concepts
- Resource Protection Techniques
- Incident Management
- Preventative Measures
- Support Patch and Vulnerability Management
- Implement Recovery Strategies
- Disaster Recovery Processes
- Disaster Recovery Plans
- Business Continuity Planning
- Summary

Software Development Security
- Introduction
- Overview
- Security in the Software Development Lifecycle
- Security Controls in Development Environment
- Software Security Effectiveness
- Summary