Certified Information Systems Security Professional, Part 9 of 9: Systems 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: This series assumes a good understanding of enterprise networking and networking security. This is part 9 of a 9 part series.

Runtime: 02:14:58

Course description: This course covers security fundamentals, risk management, threat modeling. governance, compliance, ethics, policies, and personnel security. When complete you'll have a comprehensive understanding of how security integrates with all of these key areas of knowledge. This course is part of a series covering the ISC(2) Certified Information Systems Security Professional (CISSP).

Course outline:

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