# Certified Information Systems Security Professional, Part 1 of 9: Risk and Authentication



**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.

**Runtime:** 02:56:01

**Course description:** This course covers risk management and authentication. It will look at risk from a negative perspective or the likelihood of something bad happening. Topics covered will be plans, programs and infrastructure providing the foundation for all other domains including access control, validating, and verifying the use of resources. This course is part of a series covering the ISC(2) Certified Information Systems Security Professional or CISSP.

**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)*

# Certified Information Systems Security Professional, Part 1 of 9: Risk and Authentication



- 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