Certified Information Security Manager CISM, Part 3 of 4: Security Program Development

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 3 of the series

Runtime: 04:05:21

Course description: This course covers how to plan, design, and implement an Information Security policy and to coordinate a set of activities, project and initiatives to implement the Information Security strategy. This course is part of a series covering the ISACA Certified Information Security Manager (CISM).

Course outline:

Develop Information Security Program
• Introduction
• The Importance of Security Programs
• Security Program Development Outcomes
• Effective Security Program Development
• Cross-Organizational Responsibilities
• Information Security Program Objectives
• Program Objectives
• Program Objectives Continued
• Defining Objectives
• Defining Objectives Continued
• Summary

Technology Resources
• Introduction
• Technology Resources
• Techology Resources Continued
• Information Security Manager
• Summary

Info Sec Management Scope and Charter
• Introduction
• Assurance Function Integration
• Program Development Challenges
• Other Pitfalls
• Implementation of Strategy
• Program Goals
• The Steps of the Security Program
• Defining the Roadmap
• Defining the Roadman Continued
• Elements of the Roadmap

• Elements of the Roadmap Continued
• General Controls
• Gap Analysis
• Summary

Info Sec Management Framework
• Introduction
• Info Sec Management Framework
• Security Management Framework
• COBIT 5
• ISO/IEC 27001
• Summary

Framework Concepts
• Introduction
• Info Sec Framework Components
• Operational Components
• Operational Components Continued
• Management Components
• Administrative Components
• Educational and Informational Components
• Summary

Program Resources Part 1
• Introduction
• Resource Examples
• Documentation
• Enterprise Architecture
• Enterprise Architecture Continued
• Controls
• Common Control Practices
• Common Control Practices Continued
• Countermeasures

• Technology Constraints
• Technologies Continued
• Summary

Program Resources Part 2
• Introduction
• Content Filtering
• Personnel Roles and Responsibilities
• Personnel Skills
• Security Awareness
• Awareness Training
• Formal Audits
• Compliance Enforcement
• Project Risk Analysis
• Verifying Compliance
• Other Sources of Information
• Program Budgeting
• Program Budgeting Continued
• Summary

Implementing an Info Sec Program
• Introduction
• Policy Compliance
• Standards
• Training and Education
• ISACA Control Objectives
• Third-Party Service Providers
• Third-Party Security
• Integrating Security into the Lifecyle Process
• Monitoring and Communication
• Documentation

• The Plan of Action
• Summary

Info Sec Architecture
• Introduction
• Managing Complexity
• Managing Complexity Continued
• Objectives of Information Security Architecture
• Physical Security
• Summary

Info Sec Program Metrics
• Introduction
• Info Sec Program Deployment Metrics
• Metrics Considerations
• Strategic Alignment
• Value Delivery
• Resource Management
• Assurance Process Integration
• Performance Measurement
• Security Baseline
• Summary

Info Sec Activities
• Introduction
• Security Activities Overview
• IS Liason Responsibilities
• IS Liason Responsibilities Continued
• Cross-Organizational Responsibilities
• Security Reviews and Audits
• Management of Security Technology
• Due Diligence
• Compliance Monitoring and Enforcement

Certified Information Security Manager CISM, Part 3 of 4: Security Program Development

- Assessment of Risk and Impact
- Outsourcing and Service Providers
- Cloud Computing
- Cloud Computing Continued
- Integration with IT Processes
- Summary