Certified Information Security Manager (CISM)

Course Overview

This course teaches students about information security governance, information risk management, information security program development, and information security incident management.

Course Introduction 3m
Course Introduction

Domain 01 - Information Security Governance 3h 48m
Lesson 1: Information Security Governance Overview
Information Security Governance Overview
Importance of Information Security Governance
Outcomes of Information Security Governance
Lesson 2: Effective Information Security Governance
Business Goals and Objectives
Roles and Responsibilities of Senior Management
Governance, Risk Management and Compliance
Business Model for Information Security
Dynamic Interconnections
Lesson 3: Information Security Concepts and Technologies
Information Security Concepts and Technologies
Technologies
Lesson 4: Information Security Manager
Responsibilities
Senior Management Commitment
Obtaining Senior Management Commitment
Establishing Reporting and Communication Channels
Lesson 5: Scope and Charter of Information Security Governance
Assurance Process Integration and Convergence
Convergence
Governance and Third-Party Relationships
Lesson 6: Information Security Governance Metrics
Metrics
Effective Security Metrics
Security Implementation Metrics
Strategic Alignment
Risk Management
Value Delivery
Resource Management
Performance Measurement
Assurance Process Integration/Convergence
Lesson 7: Information Security Strategy Overview
Another View of Strategy

Lesson 8: Creating Information Security Strategy
Information Security Strategy
Common Pitfalls
Objectives of the Information Security Strategy
What is the Goal?
Defining Objectives
Business Linkages
Business Case Development
Business Case Objectives
The Desired State
COBIT
COBIT Controls
COBIT Framework
Capability Maturity Model
Balanced Scorecard
Architectural Approaches
ISO/IEC 27001 and 27002
Risk Objectives
Lesson 9: Determining Current State Of Security
Current Risk
BIA
Lesson 10: Information Security Strategy Development
Elements of a Strategy
The Roadmap
Strategy Resources and Constraints
Lesson 11: Strategy Resources
Policies and Standards
Definitions
Enterprise Information Security Architectures
Controls
Countermeasures
Technologies
Personnel
Organizational Structure
Employee Roles and Responsibilities
Skills
Audits
Compliance Enforcement
Threat Assessment
Vulnerability Assessment
Risk Assessment
Insurance
Business Impact Assessment
Outsourced Security Providers
Lesson 12: Strategy Constraints
Legal and Regulatory Requirements
Physical Constraints
The Security Strategy
Lesson 13: Action Plan to Implement Strategy
Gap Analysis

Policy Development
Standards Development
Training and Awareness
Action Plan Metrics
General Metric Considerations
CMM4 Statements
Objectives for CMM4
Domain 01 Review

Domain 02 - Information Risk Management 2h 25m
Lesson 1: Risk Management Overview
Types of Risk Analysis
The Importance of Risk Management
Risk Management Outcomes
Risk Management Strategy
Lesson 2: Good Information Security Risk Management
Context and Purpose
Scope and Charter
Assets
Other Risk Management Goals
Roles and Responsibilities
Lesson 3: Information Security Risk Management Concepts
Technologies
Lesson 4: Implementing Risk Management
The Risk Management Framework
The External Environment
The Internal Environment
The Risk Management Context
Gap Analysis
Other Organizational Support
Risk Analysis
Lesson 5: Risk Assessment
NIST Risk Assessment Methodology
Aggregated or Cascading Risk
Other Risk Assessment Approaches
Identification of Risks
Threats
Vulnerabilities
Risks
Analysis of Relevant Risks
Risk Analysis
Semi-Quantitative Analysis
Quantitative Analysis Example
Evaluation of Risks
Risk Treatment Options
Impact
Lesson 6: Controls Countermeasures
Controls
Residual Risk
Information Resource Valuation

Methods of Valuing Assets
Information Asset Classification
Determining Classification
Impact
Lesson 7: Recovery Time Objectives
Recovery Point Objectives
Service Delivery Objectives
Third-Party Service Providers
Working with Lifecycle Processes
IT System Development
Project Management
Lesson 8: Risk Monitoring and Communication
Risk Monitoring and Communication
Other Communications
Domain 02 Review

Domain 03 - Information Security Program Development 4h 9m
Lesson 1: Development of Information Security Program
Importance of the Program
Outcomes of Security Program Development
Effective Information Security Program Development
Lesson 2: Information Security Program Objectives
Program Objectives
Defining Objectives
Cross Organizational Responsibilities
Lesson 3: Information Security Program Development Concepts
Technology Resources
Information Security Manager
Lesson 4: Scope and Charter of Information Security Program Development
Assurance Function Integration
Challenges in Developing Information Security Program
Pitfalls
Objectives of the Security Program
Program Goals
The Steps of the Security Program
Defining the Roadmap
Elements of the Roadmap
Gap Analysis
Lesson 5: Information Security Management Framework
Security Management Framework
COBIT 5
ISO/IEC 27001
Lesson 6: Information Security Framework Components
Operational Components
Management Components
Administrative Components
Educational and Informational Components
Lesson 7: Information Security Program Resources
Resources
Documentation

Domain 04 - Information Security Incident Management 4h 20m

Lesson 1: Incident Management Overview
Incident Management Overview
Types of Events
Goals of Incident Management
Lesson 2: Incident Response Procedures
Incident Response Procedures
Importance of Incident Management
Outcomes of Incident Management
Incident Management
Concepts
Incident Management Systems
Lesson 3: Incident Management Organization
Incident Management Organization
Responsibilities
Senior Management Commitment
Lesson 4: Incident Management Resources
Policies and Standards
Incident Response Technology Concepts
Personnel
Roles and Responsibilities (eNotes)
Skills
Awareness and Education
Audits
Lesson 5: Incident Management Objectives
Defining Objectives
The Desired State
Strategic Alignment
Other Concerns
Lesson 6: Incident Management Metrics and Indicators
Implementation of the Security Program Management
Management Metrics and Monitoring
Other Security Monitoring Efforts
Lesson 7: Current State of Incident Response Capability
Threats
Vulnerabilities
Lesson 8: Developing an Incident Response Plan
Elements of an Incident Response Plan
Gap Analysis
BIA
Escalation Process for Effective IM
Help Desk Processes for Identifying Security Incidents
Incident Management and Response Teams
Organizing, Training, and Equipping the Response Staff
Incident Notification Process
Challenges in making an Incident Management Plan
Lesson 9: BCP/DRP
Goals of Recovery Operations
Choosing a Site Selection
Implementing the Strategy

Incident Management Response Teams
Network Service High-availability
Storage High-availability
Risk Transference
Other Response Recovery Plan Options
Lesson 10: Testing Response and Recovery Plans
Periodic Testing
Analyzing Test Results
Measuring the Test Results
Lesson 11: Executing the Plan
Updating the Plan
Intrusion Detection Policies
Who to Notify about an Incident
Recovery Operations
Other Recovery Operations
Forensic Investigation
Hacker / Penetration Methodology
Domain 04 Review
Course Closure

Total Duration: 14h 44m