

# CISM - Certified Information Security Manager

## Domain 01 - Information Security Governance

### **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 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**

---

### **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
- 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**

---

## **Lesson 1: Development of Information Security Program**

- Importance of the Program
- Outcomes of Security Program Development
- Effective Information Security Program Development
- Cross Organizational Responsibilities

## **Lesson 2: Information Security Program Development Concepts**

- Technology Resources
- Information Security Manager

## **Lesson 3: 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 4: Information Security Program Resources**

- Resources
- Documentation
- Enterprise Architecture
- Controls as Strategy Implementation Resources
- Common Control Practices
- Countermeasures
- Technologies
- Personnel
- Security Awareness
- Awareness Topics
- Formal Audits
- Compliance Enforcement
- Project Risk Analysis
- Other Actions
- Other Organizational Support
- Program Budgeting

## **Lesson 5: Implementing an Information Security Program**

- Policy Compliance
- Standards Compliance
- Training and Education
- ISACA Control Objectives
- Third-party Service Providers
- Integration into Lifecycle Processes
- Monitoring and Communication
- Documentation
- The Plan of Action

## **Lesson 6: Information Infrastructure and Architecture**

- Managing Complexity
- Objectives of Information Security Architectures
- Physical and Environmental Controls

## **Lesson 7: Information Security Program**

- Information Security Program Deployment Metrics
- Metrics
- Strategic Alignment
- Risk Management

- Value Delivery
- Resource Management
- Assurance Process Integration
- Performance Measurement
- Security Baselines
- Domain 03 Review

## **Domain 04 - Information Security Program Management**

---

### **Lesson 1: Information Security Management Overview**

- Importance of Security Management
- Outcomes of Effective Security Management
- Risk Management
- Value Delivery
- Business Process Assurance

### **Lesson 2: Organizational Roles and Responsibilities**

- Information Security Manager Responsibilities
- Risk Management Responsibilities
- Technology Competencies
- Management and Administrative Responsibilities
- Board of Directors
- Executive Management
- Security Steering Committee
- Information Technology Unit
- Business Unit Manager
- Other Business Units

### **Lesson 3: The Framework for Information Security Management**

- Technical Components
- Operational Components of Security
- Management Components of Security
- The Administration Components of Security
- Other Components

### **Lesson 4: Measuring Performance**

- Measuring Risk and Loss
- Metrics for Organizational Objectives
- Determining Compliance
- Measuring Productivity
- Other Metrics

### **Lesson 5: Challenges Facing Information Security**

- What Is the State of Security Management
- The State of Information Security Management

### **Lesson 6: Resources**

- Control Best Practices
- Control Countermeasures
- Other Control Countermeasures

### **Lesson 7: Other Management Considerations**

- Implementation of the Security Program Management
- Management Metrics and Monitoring
- Other Security Monitoring Efforts
- The Lifecycle Process
- Other Aspects of Monitoring
- What Should Be Done About Noncompliance Issues
- Domain 04 Review

## **Domain 05 - Incident Management and Response**

---

### **Lesson 1: Responding to the Incident Overview**

- Responding to the Incident Overview
- Response and Management
- Incident Response Planning
- Importance of Incident Response
- Outcomes of the IRP

### **Lesson 2: Incident Management Concepts**

- Software Engineering Institute Definitions
- Technologies of Incident Response
- Incident Management Charter

### **Lesson 3: The Incident Response Manager**

- The Objectives of Incident Management
- Monitoring and Measuring Incident Management
- Alignment
- Integration
- Other Incident Management Considerations

### **Lesson 4: What Are Good Incident Management Procedures**

- The Difficulties of Creating an Incident Management Plan

### **Lesson 5: Resources for Incident Management**

- Human Resources
- Incident Response Team Organization
- IRT Roles and Responsibilities
- IRT Roles
- IRT Skills
- BIA
- IRT Capability
- Combining the BIA with the IRT
- Creating the Incident Response Plan
- Response and Recovery Plans
- 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 6: Testing Response and Recovery Plans**

- Periodic Testing
- Analyzing Test Results
- Measuring the Test Results

### **Lesson 7: 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
- Demo - Vulnerability Scan
- Domain 05 Review
- Course Closure