CISM®

You will acquire the requisite skills to design, deploy, and manage security architecture for your organization with this CISM® training, which prepares you for the **CISM certification examination of ISACA**. The CISM course is aligned with ISACA best practices. Today, enterprises and government agencies increasingly expect their IT professionals to hold a CISM certification.

Program Duration

36 Hours

Learning Format

Live, Online and Interactive

Course Curriculum

Certified Information Security Manager (CISM®)

Lesson 01: Information Security Governance

1.01 Course Introduction
1.02 Information Security Governance: Overview
1.03 Effective Information Security Governance
1.04 Information Security Concepts and Technologies
1.05 Technologies
1.06 Scope and Charter of Information Security Governance
1.07 Information Security Governance Metrics
1.08 Information Security Strategy: Overview
1.09 Creating Information Security Strategy
1.10 Overview of Information Security Governance
1.11 Roles and Responsibilities in Information Security
1.12 Governance of Third-Party Relationships
1.13 Obtaining Senior Management Commitment
1.14 The Feasibility Study and the Business Case
1.15 Information Security Governance Metrics
1.16 Information Security Strategy Overview
1.17 COBIT
1.18 ISO Standards

Lesson 02: Information Security Risk Management

2.01 Information Risk Management and Compliance
2.02 Good Information Security Risk Management
2.03 Risk Assessment
2.04 Controls Countermeasures
2.05 Recovery Time Objective
2.06 Risk Monitoring and Communication
2.07 Risk Management: Overview
2.08 Good Information Security Risk Management
2.09 Information Security Risk Management Concepts
2.10 Implementing Risk Management

2.11 Testing Response and Recovery Plans
2.12 Risk Assessment
2.13 Controls Countermeasures
2.14 Recovery Time Objectives
2.15 Risk Monitoring and Communication

Lesson 03: Information Security Program

3.01 Development of Information Security Program
3.02 Information Security Program Objectives
3.03 Information Security Program Development Concepts
3.04 Scope and Charter of Information Security Program Development
3.05 Information Security Framework Components
3.06 Implementing an Information Security Program
3.07 Information Infrastructure and Architecture
3.08 Information Security Program
3.09 Security Program Services and Operational Activities
3.10 Overview of Information Security Programme Management
3.11 Program Objectives for Information Security
3.12 Components of an Information Security Framework
3.13 Creating a Road Map for an Information Security Programme
3.14 Policy, Standards, and Procedures
3.15 Budget for Security
3.16 Administration and Management of Security Programmes
3.17 Privacy Regulations
3.18 Architecture of Information Security
3.19 Implementation of Architecture
3.20 Cloud Computing
3.21 Countermeasures and Controls
3.22 Metrics and Monitoring for Security Programmes
3.23 Security Education and Training

Lesson 04: Incident Management

4.01 Incident Management: Overview
4.02 Incident Response: Procedures
4.03 Incident Management: Organization
4.04 Incident Management: Resources
4.05 Incident Management: Objectives
4.06 Incident Management: Metrics and Indicators
4.07 Current State of Incident Response Capability
4.08 Developing an Incident Response Plan
4.09 Information Security Incident Management
4.10 Incident Response Procedures
4.11 Incident Management: Organization
4.12 Incident Management: Resources
4.13 Incident Management: Objectives
4.14 Incident Management: Metrics and Indicators
4.15 Current State of Incident Response Capability
4.16 Develop an Incident Response Plan
4.17 BCP DRP
4.18 Testing Response and Recovery Plans
4.19 Executing the Plan

Lesson 05: CISM Case Studies

5.01 Air Traffic Control
5.02 CISM solution
5.03 IT Security Governance
5.04 Program Office Unique Framework
5.05 Is Critical Incident Stress Debriefing Effective?
5.06 Critical Incident Stress Debriefing
5.07 Information Security Risks Assessment
5.08 Impact Controls
5.09 Custom Incident Management Software
5.10 Incident Management Process
5.11 Information Security Program Development and Management
5.12 Developing Cyber Risk Management Strategy
5.13 Good Practices for Managing Information Risk
5.14 Managing Information Security Risk
5.15 Information Risk Management Communication
5.16 Stages of Information Security and Risk Management
5.17 Incident Risk: Management Functions
5.18 Information Risk: Management Introduction
5.19 Information Security: Incident Management
5.20 Process
5.21 How It Works?
5.22 Best Practices
5.23 Information Security Incident Management: Objectives
5.24 Responsibilities and Procedures
5.25 CISM Course Summary

7+ Skills Covered

Information Security Governance
Information Security Risk Management
Information Security Program
Incident Management
Design Security Architecture
Knowledge of ISACA Domains
Enterprise IT Frameworks