



Certified Information Security Manager (CISM)

Module 1: Introduction

- Instructor Introduction
- Course Introduction
- Exam Overview

Module 2: Information Security Governance

- Module Overview
- InfoSec Strategic Context Part 1
- InfoSec Strategic Context Part 2
- GRC Strategy and Assurance
- Roles and Responsibilities
- GMA Tasks Knowledge and Metrics
- IS Strategy Overview
- Strategy Implementation
- Strategy Development Support
- Architecture and Controls
- Considerations and Action Plan
- InfoSec Prog Objectives and Wrap-Up

Module 3: Information Security Risk Management

- Module Overview
- Risk Identification Task and Knowledge
- Risk Management Strategy
- Additional Considerations
- Risk Analysis and Treatment Tasks & Knowledge
- Leveraging Frameworks
- Assessment Tools and Analysis
- Risk Scenario Development
- Additional Risk Factors
- Asset Classification and Risk Management
- Risk Monitoring and Communication
- Information Risk Management Summary

Module 4: InfoSec Prog Development and Management

- Module Overview
- Alignment and Resource Management - Task and Knowledge
- Key Relationships

Standards Awareness and Training - Tasks and Knowledge
Awareness and Training
Building Security into Process and Practices - Tasks and Knowledge
Additional Technology Infrastructure Concerns
Security monitoring and reporting Overview Tasks and Knowledge
Metrics and Monitoring
Summary

Module 5: Information Security Incident Management

Module Overview
Planning and Integration Overview Task and Knowledge
Incident Response Concepts and Process
Forensics and Recovery
Readiness and Assessment - Overview Tasks and Knowledge
Identification and Response Overview Tasks and Knowledge
Incident Processes

Module 6: Exam Prep

Case Study - Security On a Shoestring Budget
Case Study - APT In Action
Summary
Exam Prep