CERTIFIED INFORMATION SECURITY MANAGER

CISM

Duration: 4 days; Instructor-led

OVERVIEW

Designed for IT professionals with technical expertise and experience in IS/IT security and control looking to transition from team player to manager. CISM can add credibility and confidence to interactions with internal and external stakeholders, peers, and regulators.

This certification indicates expertise in information security governance, program development and management, incident management and risk management.

Content in this course is:

- Aligned with the CISM job practice.
- Adapted from the CISM Review Manual 16th Edition.
- Reviewed by subject matter experts that hold the CISM certification.

The course features an enhanced facilitator guide, additional participant resources, knowledge check questions from the CISM Questions, Answers and Explanations (QAE) database along with scenario-based activities and enrichment materials (articles, podcasts and whitepapers) selected from the ISACA website to provide learners with an opportunity to go deeper into specific areas related to the course content.

OBJECTIVES

After completing this course, participants should be able to:

- Explain the relationship between executive leadership, enterprise governance and
- information security governance.
- Outline the components used to build an information security strategy.
- Explain how the risk assessment process influences the information security strategy.
- Articulate the process and requirements used to develop an effective information risk
- response strategy.
- Describe the components of an effective information security program.
- Explain the process to build and maintain an enterprise information security program.
- Outline techniques used to assess the enterprise's ability and readiness to manage an
- information security incident.

PREREQUISITES

To earn the CISM credential you need five years of information security work experience, with a minimum of three years of information security management work experience in three or more of the job practice analysis areas.

AUDIENCE

The CISM certification is perfect for experienced information security managers and everyone who works in IT Governance. You will learn about four domains in information security. These domains are about compliance, risk management and security governance

COURSE CONTENTS

Module 1: Information Security Governance

Session Topics:

- Enterprise Governance Overview
- Organizational Culture, Structures, Roles and Responsibilities
- Legal, Regulatory and Contractual Requirements
- Information Security Strategy
- Information Governance Frameworks and Standards
- Strategic Planning

Learning Objectives:

- Describe the role of governance in creating value for the enterprise.
- Explain the importance of information security governance in the context of overall enterprise governance.
- Describe the influence of enterprise leadership, structure and culture on the effectiveness of an information security strategy.
- Identify the relevant legal, regulatory and contractual requirements that impact the enterprise
- Describe the effects of the information security strategy on enterprise risk management.
- Evaluate the common frameworks and standards used to govern an information security strategy
- Explain why metrics are critical in developing and evaluating the information security strategy

Resources:

- Information Security Program Governance Objectives and Outcomes
- Common Roles in the Enterprise
- Example RACI Chart

Module 2: Information Security Risk Management

Session Topics:

- Risk and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Assessment, Evaluation and Analysis

- Information Risk Response
- Risk Monitoring, Reporting and Communication

Learning Objectives:
- Apply risk assessment strategies to reduce the impact of information security risk.
- Assess the types of threats faced by the enterprise.
- Explain how security control baselines affect vulnerability and control deficiency analysis
- Differentiate between application of risk treatment types from an information security perspective
- Describe the influence of risk and control ownership on the information security program.
- Outline the process of monitoring and reporting information security risk.

Resources:
- Vulnerabilities and Threats
- Operational Risk Categories
- Risk Register Example
- Risk Report Example
- Risk Scenario Technique Main Issues
- Typical Risk Management Documentation
- Risk Communication Plan

Module 3: Information Security Program Development and Management

Session Topics:
- IS Program Development and Resources
- IS Standards and Frameworks
- Defining an IS Program Road Map
- IS Program Metrics
- IS Program Management
- IS Awareness and Training
- Integrating the Security Program with IT Operations
- Program Communications, Reporting and Performance Management

Learning Objectives:
- Outline the components and resources used to build an information security program.
- Distinguish between common IS standards and frameworks available to build an information security program.
- Explain how to align IS policies, procedures and guidelines with the needs of the enterprise
- Describe the process of defining an IS program road map.
- Outline key IS program metrics used to track and report progress to senior management.
- Explain how to manage the IS program using controls.
- Create a strategy to enhance awareness and knowledge of the information security program
- Describe the process of integrating the security program with IT operations and third-party providers.
- Communicate key IS program information to relevant stakeholders.

Resources:
- Information Security Program Governance Objectives and Outcomes
- Alternate Enterprise Architecture Frameworks
- Policies, Standards, Procedures and Guidelines
- Security Program Components Checklist
- Information Security Framework Components
- Technical Control Components and Architecture
- Contract Points
- Information Security Liaison Responsibilities
- Types of Security Issues
- Measuring Information Security Program Performance
- Information Security Program Management Evaluation Questions

Module 4: Information Security Incident Management

Session Topics:
- Incident Management and Incident Response Overview
- Incident Management and Response Plans
- Incident Classification/Categorization
- Incident Management Operations, Tools and Technologies
- Incident Investigation, Evaluation, Containment and Communication
- Incident Eradication, Recovery and Review
- Business Impact and Continuity
- Disaster Recovery Planning
- Training, Testing and Evaluation
- Learning Objectives:
- Distinguish between incident management and incident response
- Outline the requirements and procedures necessary to develop an incident response plan
- Identify techniques used to classify or categorize incidents.
- Outline the types of roles and responsibilities required for an effective incident management and response team
- Distinguish between the types of incident management tools and technologies available to an enterprise.
- Describe the processes and methods used to investigate, evaluate and contain an incident
- Identify the types of communications and notifications used to inform key stakeholders of incidents and tests.
- Outline the processes and procedures used to eradicate and recover from incidents.
- Describe the requirements and benefits of documenting events.
- Explain the relationship between business impact, continuity and incident response.
- Describe the processes and outcomes related to disaster recovery.
- Explain the impact of metrics and testing when evaluating the incident response plan.

Resources:
- Incident Management Action Plan Phases
- Developing an Incident Response Plan
- SEU-CMU Action Plan Phases
- Types of Insurance and Coverage
- Types of Recovery Sites
- Legal Aspects of Forensic Evidence