€TRAINING

Certified Information Security Manager CISM

Certified Information Security Manager CISM

Introduction:

This program is designed to prepare participants for the certification exam only.

This training program offers participants comprehensive knowledge and practical skills essential for managing, designing, and assessing information security systems within organizations. It empowers them to enhance organizational resilience, protect critical assets, and effectively manage cybersecurity threats.

Program Objectives:

At the end of this program, participants will be able to:

- Understand the principles of information security governance and risk management.
- Develop skills in designing and implementing information security systems.
- Learn techniques for assessing and managing cybersecurity risks.
- Gain insights into industry standards and regulations for information security.
- Enhance capabilities in leading and managing information security initiatives within organizations.
- Prepare for successful completion for the Certification Exam.

Targeted Audience:

- Information Security Managers.
- IT Auditors.
- Risk Managers.
- Compliance Officers.
- Security Consultants.
- IT Managers.

Program Outline:

Unit 1:

Information Security Governance:

- Overview of information security governance principles.
- Roles and responsibilities of information security managers.
- Establishing and maintaining an information security management framework.
- Developing and implementing information security policies and procedures.
- Case studies on effective information security governance practices.

Unit 2:

Risk Management and Compliance:

- Principles of risk management in information security.
- Identifying and assessing information security risks.
- Developing risk mitigation strategies and controls.
- Ensuring compliance with regulatory requirements and industry standards.
- Exercises on conducting risk assessments and compliance audits.

Unit 3:

Information Security Program Development and Management:

- Steps for designing and implementing information security programs.
- Developing security architectures and frameworks.
- Managing security operations and incident response.
- Steps for implementing security controls and technologies.
- Case studies on successful information security program management.

Unit 4:

Information Security Incident Management:

- Understanding the incident management process.
- Detecting, analyzing, and responding to security incidents.
- Developing incident response plans and procedures.
- Conducting post-incident reviews and lessons learned.

- Real-world examples of effective incident management practices.

Unit 5:

Industry Standards and Best Practices

- Overview of relevant industry standards ISO 27001, NIST.
- Understanding regulatory requirements for information security.
- Implementing best practices for information security management.
- Documenting and reporting information security activities.
- Prepare for the Certification Exam.

Note: This program is designed to prepare participants for the certification exam only.