Certified Information Security Manager (CISM) Training Course

The Certified Information Security Manager (CISM) course equips professionals with skills to manage enterprise-level security management responsibilities and aligns IT security with business goals.

SEC-302

Course Outcomes

Professional, practical, & hands-on live instructor-led training

Advance your skills and graduate as a certified professional, with the skills, experience, and job-search know how to get your career moving.

Start Today

Potential Career Tracks

Information Security Manager · Security Director

IT Security Consultant · Risk Management Analyst

Compliance and Risk Manager

Information Security Officer

Taught by Industry Veterans &
World Class Instructors

Introduction to Certified Information Security Manager (CISM)

Course Overview

Intellectual Point's Certified Information Security Manager (CISM) Training Course is meticulously crafted to equip information security managers with the skills necessary to design, implement, and manage an information security program. The course is aligned with global security practices and prepares you for the CISM certification exam, ensuring that you acquire both theoretical knowledge and practical expertise. It covers essential topics such as information risk management, governance, incident management, and program development to foster a deeper understanding of information security within an organization. By the course's conclusion, you'll not only be ready to sit for the exam but also adept at applying information security principles to real-world scenarios.

Throughout the training, you will explore key domains of information security management such as information risk management, security governance, information security program development, and incident management. The course includes immersive scenarios and case studies, equipping you with the ability to respond effectively to security incidents and manage risks. By the end, you will be able to apply this knowledge to enhance security practices within your organization, ensuring robust information protection strategies.

Obtainable Skills

Risk Management Strategies · Information Security Governance · Incident Response Planning

Security Program Development · Threat Management · Audit and Compliance

Data Protection Techniques · Policy Development · Incident Management

Course Insights

Audience Profile

This CISM Training Course is targeted towards mid-career professionals aspiring to step into managerial roles in information security. Ideal for information security officers, IT managers, and security consultants, this course is designed for those with experience in managing security programs and a keen interest in enhancing their strategic capabilities. It suits individuals looking to gain recognition in the information security field and those preparing for the CISM certification to advance their career towards leadership roles in security management.

Course Outcomes

By the end of this course, participants will:

1. Master the concepts of information security governance and effectively align it with business goals.
2. Develop and manage information security programs that bolster organizational resilience.
3. Analyze risk and employ risk management techniques to secure organizational assets.
4. Respond to and manage security incidents to minimize impact and facilitate recovery.
5. Pass the CISM certification exam with confidence, enhancing your professional growth.

Module by Module Learning *Outline*

6 Modules

Module 1: Information Security Governance

Learning Objectives:

- Understand the role of security governance within an organization.
- Align information security strategies with business objectives.

Topics Covered

Principles of Security Governance:

- Definition and importance of security governance.
- Alignment of security objectives with business goals.

Strategic Security Planning:

- Developing security plans and policies.
- Establishing a governance framework.

Module 2: Risk Management

Learning Objectives:

- Identify and assess information security risks.
- Implement risk management strategies to protect organizational assets.

Topics Covered

Risk Assessment Methodologies:

- Methods for identifying and evaluating risks.
- Tools and techniques for risk assessment.

Risk Mitigation Strategies:

- Developing risk treatment plans.
- Implementing and monitoring risk controls.

Module 3: Information Security Program Development

Learning Objectives:

- Design and implement effective security programs.
- Enhance organizational resilience through security measures.

Topics Covered

Security Program Design:

- Key components of a security program.
- Structuring a security program framework.

Implementation and Management:

- Rolling out security measures and initiatives.
- Monitoring and improving program effectiveness.

Module 4: Incident Management

Learning Objectives:

- Develop incident response plans and procedures.
- Effectively manage and mitigate security incidents.

Topics Covered

Incident Response Planning:

- Components of an incident response plan.
- Establishing roles and responsibilities.

Incident Handling Techniques:

- Strategies for detecting and responding to incidents.
- Post-incident analysis and reporting.

Module 5: Exam Preparation and Practical Application

Learning Objectives:

- Review key concepts and prepare for the CISM exam.
- Apply learned skills to practical security scenarios.

Topics Covered

CISM Exam Strategies:

- Exam format and question types.
- Tips for effective exam preparation and study techniques.

Practical Scenarios and Case Studies:

- Applying security management skills to real-world scenarios.
- Analyzing case studies for hands-on learning.