Certified Information Security Manager (CISM)

GOVERNANCE TRAINING

COURSE OVERVIEW

The ISACA Certified Information Security Manager (CISM) certification is one of the most important and prestigious InfoSec qualifications in the world today. CISM defines the core competencies and international standards of performance that information security managers are expected to master. It provides executive management with the assurance that those who have earned their CISM have the experience and knowledge to offer effective security management and advice.

The management-focused CISM is the globally accepted standard for individuals who design, build and manage enterprise information security programs. CISM is the leading credential for information security managers. The recent quarterly IT Skills and Certifications Pay Index (ITSCPI) from Foote Partners ranked CISM among the most sought-after and highest-paying IT certifications. CISM defines the core competencies and international standards of performance that information security managers are expected to master. It provides executive management with the assurance that those who have earned their CISM have the experience and knowledge to offer effective security management and advice.

COURSE SUMMARY

Certificate:

Certified Information Security Manager (CISM)

Course Format:

Classroom, Virtual or Self-Paced

Course Duration:

Classroom: 4 days
Virtual: 5 days (2x2-hours a day)

EXAM FORMAT

- 150 questions per paper
- Objective Examination
- 4 Hours duration
- Pass Mark – 450 or Higher
- Closed Book

TARGET AUDIENCE

ISACA's Certified Information Security Manager (CISM) certification is for those with technical expertise and experience in IS/IT security and control and wants to make the move from team player to manager. CISM can add credibility and confidence to your interactions with internal and external stakeholders, peers and regulators.

LEARNING OBJECTIVES

This program provides a dynamic learning experience where you'll learn:

- Information Security Governance – Affirms the expertise to establish and/or maintain an information security governance framework (and supporting processes) to ensure that the information security strategy is aligned with organizational goals and objectives. Domain 1 confirms your ability to develop and oversee an information security governance framework to guide activities that support the information security strategy.
- Managing Information Risk – proficiency in this key realm denotes advanced ability to manage information risk to an acceptable level, in accordance with organizational risk appetite, while facilitating the attainment of organizational goals and objectives. Domain 2 demonstrates expertise in classifying information assets to ensure measures taken to protect those assets are proportional to their business value
- Developing and Managing an Information Security Program – establishes ability to develop and maintain an information security program that identifies, manages and protects the organization's assets while aligning with business goals. Domain 3 attests to ability to ensure the information security program adds value while supporting operational objectives of other business functions (human resources, accounting, procurement, IT, etc.)