

CISM TRAINING
EXAM PREPARATION TRAINING

CISM

WHAT IS CISM?

- Certified Information Security Manager (CISM) is a certification for information security managers awarded by ISACA (Information Systems Audit and Control Association).
- CISM means higher earning potential and career advancement.
- Recent independent studies consistently rank CISM as one of the highest paying and sought after IT certifications.
- CISM is one of the most sought-after positions in Information Technology.
- Government agencies, multinational companies, and enterprises are just some of the sectors that benefit much from hiring such professional.

BENEFIT OF CISM

- CISM Impacts Your Career and Your Organization.
- CISM understand the business. They know how to manage and adapt technology to their enterprise and industry.
- As a CISM, you will benefit in three important ways: delivering value to enterprises, ongoing education and career improvement.
- As an expert in the field, you can showcase your understanding between the connection between business goals and information security program.



WHO SHOULD ATTEND?

- Any candidate can attend training who want to learn about CISM
- Risk managers and Security professionals
- Security auditors
- Information security staff and Compliance personnel
- Information security managers, CSOs, CISOs and CIOs
- Information security assurance providers

LEARNING OBJECTIVES

- Gain knowledge of the core competencies required of a world class information security professional.
- Be thoroughly prepared for the CISM certification examination.
- Demonstrates your understanding of the relationship between an information security program and broader business goals and objectives.
- Distinguishes you as having not only information security expertise, but also knowledge and experience in the development and management of an information security program.
- Puts you in an elite peer network.
- Is considered essential to ongoing education, career progression and value delivery to enterprises.



COURSE CONTENTS

DOMAIN 1 : INFORMATION SECURITY GOVERNANCE

- Establish and maintain an information security strategy and align the strategy with corporate governance
- Establish and maintain an information security governance framework
- Establish and maintain information security policies
- Develop a business case
- Identify internal and external influences to the organization
- Obtain management commitment
- Define roles and responsibilities
- Establish, monitor, evaluate and report metrics

DOMAIN 2 : INFORMATION RISK MANAGEMENT AND COMPLIANCE

- Establish a process for information asset classification and ownership
- Identify legal, regulatory, organizational and other applicable requirements
- Ensure that risk assessments, vulnerability assessments and threat analyses are conducted periodically
- Determine appropriate risk treatment options
- Evaluate information security controls
- Identify the gap between current and desired risk levels
- Integrate information risk management into business and IT processes
- Monitor existing risk.
- Report noncompliance and other changes in information risk

DOMAIN 3: INFORMATION SECURITY PROGRAM DEVELOPMENT AND MANAGEMENT

- Establish and maintain the information security program
- Ensure alignment between the information security program and other business functions
- Identify, acquire, manage and define requirements for internal and external resources
- Establish and maintain information security architectures
- Establish, communicate and maintain organizational
  information security standards, procedures, guidelines
- Establish and maintain a program for information security awareness and training
- Integrate information security requirements into organizational processes
- Integrate information security requirements into contracts and activities of third parties
- Establish, monitor and periodically report program management and operational metrics

DOMAIN 4 : INFORMATION SECURITY INCIDENT MANAGEMENT

- Establish and maintain an organizational definition of, and severity hierarchy for, information security incidents
- Establish and maintain an incident response plan
- Develop and implement processes to ensure the timely identification of information security incidents
- Establish and maintain processes to investigate anddocument information security incidents
- Establish and maintain incident escalation and notification processes
- Organize, train and equip teams to effectively respond to information security incidents
- Test and review the incident response plan periodically
- Establish and maintain communication plans and processes
- Conduct post-incident reviews
- Establish and maintain integration among the incident response plan, disaster recovery plan and business continuity plan



CERTIFICATION

CISM Exam Information:

- Exam Duration : 4 Hours
- Exam Format : Multiple Choices
- Number of Questions : 150 Questions
- Exam Pass Mark : 450 with the scale of 200-800 points.
- Testing Centre – PSI Testing Site
- Exam Fee – ISACA Member: US $575
- ISACA Non-member: US $760

PREREQUISITE

To apply for CISM certification, the candidate must fulfil the required experience/qualification as mentioned below.

1. Five [5] years of experience in the Information Security Management Field

A) The qualified experience must include a minimum 3 years of experience in any of the three [3] job practice domains namely.

- Information Security Governance.
- Information Risk management.
- Information Security Program Development and Management.
- Information Security Incident Management.

B) A substitute up to two (2) years of Information Security Management experience with waivers, that includes,

- General information security work experience (minimum of 1 month, maximum of 2 years)
- Current CISSP in good standing (2-year waiver)
- Current CISA in good standing (2-year waiver)
- Postgraduate degree relevant to Information Security Management (2-year waiver)
- Information Systems Management experience (1-year waiver)

Skilled based certification, such as GIAC, MCSE, CompTIA Security+, CBCP, ESL IT Security Manager (1-year waiver)

Please Note: The work experience you use for certification need to be verified

WISELEARNER