Certified Information Security Manager (CISM)

Duration 4 Days

The ISACA® Certified Information Security Manager® is the fastest growing and arguably the most prestigious qualification available for Information Security managers today. CISM® properly recognizes that security is first and foremost a management rather than a technical issue. CISM defines the core competencies and international standards of performance that information security managers are expected to master.

The course provides an intense environment in which participants can acquire, thoroughly and properly, the skills and knowledge expected of a world-class information

LEARNING OUTCOMES

This course has been independently commissioned with two objectives:

- To provide an environment in which security professionals can acquire, thoroughly and properly, the skills and knowledge expected of a world class information security manager. Whether or not you intend to sit for the CISM exam, this course is a powerful way to equip yourself with the knowledge of the five core competencies that define the successful information security manager.
- To maximize your prospects at the CISM exam if you choose to sit it.

COURSE CONTENTS

This 5-day course is structured to follow the CISM review manual and examination flow. A full day is provided for each of the core competencies and associated task and knowledge statements, thereby ensuring a detailed and thorough coverage of all areas that will be tested. The fundamental thrust of examination is on understanding the concepts, not on memorizing facts. As a result, the course will be presented in an interactive manner to ensure the underlying concepts are understood and examination questions can be analyzed properly to achieve the correct answer.

WHO NEEDS TO ATTEND

The CISM designation is for Information Security professionals who have 3-5 years of front-line experience with the security of information. This credential is geared towards Information Security managers and those who have information security management responsibilities.

EXAM FORMAT

The CISM exam is currently held three times per year in June, September and December. Comprehensive information is available in the CISM Exam Bulletin of Information which can be downloaded from www.isaca.org

You must register for the exam directly with ISACA. You can register online at www.isaca.org/examreg

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th
Call us today 0-2634-7993-4
177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th

PREREQUISITES

Qualifying for CISM requires a combination of four "e's": experience, ethics, education and examination. Specifically, the requirements are:

- Successful completion of the CISM exam
- Adherence to a code of professional conduct
- Commitment to continuing professional education
- Submission of verified evidence of a minimum of 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 areas. Waivers for general information security work experience are available, if certain education or certification requirements are met

The CISM certification program recognizes the achievement of the CISSP credential as a baseline representation that an individual has gained general information security skill and knowledge, just as it does with individuals who have earned a CISA. As such, CISSPs receive a two-year general information security experience waiver. However, CISSPs will not be eligible to earn a CISM unless they have the required experience and can demonstrate proficiency and practical knowledge in the role of an information security manager.

Holders of other, more specialized credentials, such as the SANS Global Information Assurance Certification (GIAC), Microsoft Security Systems Engineer (MCSE), CompTIA Security + Credential and the Disaster Recovery Institute Certified Business Continuity Professional (CBCP) also can receive a one-year general information security experience waiver.

COURSE OUTLINE

1. Information Security Governance and Strategy

Introduction:

- Definition
- Objective
- Tasks
- Overview

Topics:

- Effective Information Security Governance
- Key Information Security Concepts and Issues
- The IS Manager
- Scope and Charter of Information Security Governance
- IS Governance Metrics
- Developing an IS Strategy – Common Pitfalls
- IS Strategy Objectives
- Determining Current State of Security
- Strategy Resources
- Strategy Constraints
- Action Plan Immediate Goals
- Action Plan Intermediate Goals

Practice Questions; Review of Practice Questions;

- Reference Materials and Glossary

2. Risk Management

Introduction:

- Definition
- Objective
- Tasks
- Overview

Topics:

- Effective Information Security Risk Management
- Integration into Life Cycle Processes
- Implementing Risk Management
- Risk Identification and Analysis Methods
- Mitigation Strategies and Prioritization
- Reporting Changes to Management

Practice Questions; Review of Practice Questions;

- Reference Materials and Glossary

3. Information Security Programme Management

Introduction:

- Definition
- Objective
- Tasks
- Overview

Topics:

- Planning
- Security Baselines
- Business Processes
- Infrastructure
- Malicious Code (Malware)
- Life Cycles
- Impact on End Users
- Accountability
- Security Metrics
- Managing Internal and External Resources

Practice Questions; Review of Practice Questions;

- Reference Materials and Glossary

4. Information Security Management

Introduction:

- Definition
- Objective
- Tasks
- Overview

Topics:

- Implementing Effective Information Security Management
- Security Controls and Policies
- Standards and Procedures
- Trading Partners and Service Providers
- Security Metrics and Monitoring
- The Change Management Process
- Vulnerability Assessments
- Due Diligence
- Resolution of Non-Compliance Issues
- Culture, Behavior and Security Awareness

Practice Questions; Review of Practice Questions;

- Reference Materials and Glossary

5. Response Management

Introduction:

- Definition
- Objective
- Tasks
- verview

Topics:

- Performing a Business Impact Analysis
- Developing Response and Recovery Plans
- Incident Response Processes
- Executing Response and Recovery Plans
- Documenting Events
- Post Event Reviews

Practice Questions; Review of Practice Questions;

- Reference Materials and Glossary

NETWORK TRAINING CENTER CO.,LTD. (NTC) | www.trainingcenter.co.th

Call us today 0-2634-7993-4

177/1 BUI Bldg., 14th Fl., Unit 1, 3 & 4, Surawongse Rd., Suriyawongse, Bangrak, Bangkok, THAILAND | Email: sales@trainingcenter.co.th