

Updated on 16/05/2025

Sign up

## CISM© Certification Preparation Course

ALL-IN-ONE: EXAMINATION INCLUDED IN PRICE

5 days (35 hours)

### Presentation

Become an expert in risk analysis and management with our CISM© (Certified Information Security Manager) training. We'll teach you every area, so you're fully prepared for the exam.

In fact, we'll be taking a closer look at the four main concepts assessed. Firstly, governance in cybersecurity, understanding the role of governance and the [standards](#) governing information security.

Next, we look at risk management, to find out how to assess [potential threats](#) and ensure a good monitoring process. We continue with the security program, which explains the different components of cybersecurity. You'll learn how to create measures and procedures to protect your organization.

Finally, the last part deals with incident management, how to categorize them and operations following a disaster.

### Objectives

- Acquire the knowledge needed to pass the CISM© exam
- Understand IT security risk management practices
- Implement the necessary procedures in response to an incident

### Target audience

- ISD

- CISO
- Computer scientist
- Business continuity manager
- Engineer
- Auditor
- Cybersecurity Consultant

## Prerequisites

- 5 years' professional experience in information security management
- Basic knowledge of auditing standards
- Business continuity skills
- Understanding of technical English

Note: Ambient IT is not the owner of CISM®, this certification belongs to ISACA®.

## CISM® Certification Preparation Program

### Area 1 - IT security governance

- Describe the role of governance in creating value for the company
- Explain the importance of information security governance in context of overall corporate governance
- Describe the influence of corporate management, structure and culture on the effectiveness of a company's information security strategy
- Identify relevant legal, regulatory and contractual requirements that have an impact on the company
- Describe the impact of the information security strategy on risk management for the company
- Evaluate common frameworks and standards used to govern an information security strategy
- Explain why measurements are essential in the development and evaluation of the information security strategy

### Area 2 - IT security risk management

- Apply risk assessment strategies to reduce impact of information security risks
- Assess the types of threats facing the company
- Explain how security control repositories affect the analysis of vulnerabilities and control deficiencies
- Differentiate between the application of different types of risk treatment from the point of view of food safety information
- Describe the influence of risk ownership and controls on the information security program
- Describe the information security risk monitoring and reporting process

### Area 3 - Computer security program

- Describe the components and resources used to develop an information security program
- Distinguish between the common IS standards and frameworks available to build a information security
- Explain how to align IS policies, procedures and guidelines with business needs
- Describe the process of defining a roadmap for the company's safety program. information
- Describe the key measures of the information security program used to progress and report to senior management.
- Explain how to manage the SI program using controls
- Create a strategy to improve awareness and knowledge of the information security program
- Describe the process for integrating the security program with IT operations and third-party suppliers
- Communicate key information from the information security program to relevant stakeholders

## Area 4 - Incident management

- Distinguish between incident management and incident response
- Describe the requirements and procedures needed draw up an incident response plan.
- Identify techniques used to classify or categorize incidents
- Describe the types of roles and responsibilities required for an effective incident management and response team
- Distinguish between the types of incident management tools and technologies available to a company. company
- Describe the processes and methods used to investigate, assess and contain an incident
- Identify the types of communication and notification used to inform key stakeholders of incidents and tests
- Describe the processes and procedures used to eradicate and remedy incidents
- Describe the requirements and benefits of event documentation
- Explain the relationship between business impact, continuity and incident response
- Describe disaster recovery processes and results
- Explain the impact of measurements and tests when evaluating the incident response plan

## Strategies and tips for exam success Mock exam

## Companies concerned

This course is aimed at both individuals and companies, large or small, wishing to train their teams in a new advanced computer technology, or to acquire specific business knowledge or modern methods.

## Positioning on entry to training

Positioning at the start of training complies with Qualiopi quality criteria. As soon as registration is finalized, the learner receives a self-assessment questionnaire which enables us to assess his or her estimated level of proficiency in different types of technology, as well as his or her expectations and personal objectives for the training to come, within the limits imposed by the selected format. This questionnaire also enables us to anticipate any connection or security difficulties within the company (intra-company or virtual classroom) which could be problematic for the follow-up and smooth running of the training session.

## Teaching methods

Practical course: 60% Practical, 40% Theory. Training material distributed in digital format to all participants.

## Organization

The course alternates theoretical input from the trainer, supported by examples, brainstorming sessions and group work.

## Validation

At the end of the session, a multiple-choice questionnaire verifies the correct acquisition of skills.

## Sanction

A certificate will be issued to each trainee who completes the course.