interface

We teach. You do.

ITIL

CISM: Certified Information Security Manager

$2,395.00

- 3 Days

Upcoming Dates

Course Description

ISACA’s Certified Information Security Manager® (CISM®) certification indicates expertise in information security governance, program development and management, incident management and risk management. If you are a mid-career IT professional aspiring to senior management roles in IT security and control, CISM can get you the visibility you need.

While there are many certifications focused on the information security practitioner, CISM® provides a unique opportunity to demonstrate qualified security skills ***and*** effective business acumen. This course helps students to build or improve an overarching governance program and then support that with effective information security management practices. Experienced instructors bring real-world examples of balancing business needs with security management.

This course will help you successfully join those CISM® colleagues who have demonstrated understanding of effective business management *and* the knowledge to manage cybersecurity risks to information & technology.

Course Outline

Domain 1—Information Security Governance

In this domain, students will learn to work with organizational leaders to establish priority, budget, and expectations for information security and privacy. Those details help establish and maintain an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives.

Topics include:

- Information security strategy in alignment with organizational goals and objectives
- Establishing an information security governance framework to guide activities
- Integrating security governance into corporate governance to support enterprise goals
- Effective management of information security policies
- Gaining and maintaining enterprise leaders through business cases and ongoing business communication
- Ways to establish, monitor, evaluate and report key information security metrics to provide management with accurate and meaningful information regarding the effectiveness of the information security strategy

Domain 2—Information Risk Management

In this domain, students will learn about information security risk in a business context. Risk often gets described in purely technical terms; this course focuses on cost-effective risk management practices to ensure that technical and business security aspects are well aligned.

Topics include:

- Information asset classification to ensure proportional risk management
- Ways to ensure risk assessments, vulnerability assessments and threat analyses are conducted consistently and in appropriate ways
- Appropriate risk treatment/response options to manage risk to acceptable levels based on organizational risk appetite
- Planning and applying security controls for information and technology to effectively manage risk to an acceptable level
- Integration of information risk management into business and IT processes
- Monitoring organizational risk conditions for internal and external factors (e.g., key risk indicators [KRIs], threat landscape, geopolitical, regulatory change)
- Adjusting to evolving risk conditions so that risk scenarios are managed appropriately
- Ongoing reporting and risk communication with senior management about the effects of uncertainty on organizational goals and objectives

Domain 3—Information Security Program Development and Management

Students will learn specific approaches and models for building and maintaining an information security program that achieves the security management strategy. The instructor will share collaborative methods to identify and protect the organization's assets while aligning to information security strategy and business goals.

Topics include:

- Establish and/or maintain the information security program in alignment with the information security strategy
- Identify, acquire and manage requirements for internal and external resources to execute the information security program
- Establish and maintain information security processes and resources (including people and technologies) to execute an effective information security program
- Establish, promote and maintain a program for information security awareness and training to foster an effective security culture
- Integrate information security requirements into organizational processes (e.g., change control, mergers and acquisitions, system development, business continuity)
- Establish, monitor and analyze program management and operational metrics to evaluate the effectiveness and efficiency of the information security program

Domain 4— Information Security Incident Management

In this domain, students will apply the structure, strategy, and teams from previous domains to support a focus on detecting, responding to and recovering from information security incidents to minimize business impact.

Topics include:

- Establish and maintain an organizational definition of information security incidents to classify and categorize incidents (including legal, regulatory and other requirements)
- Establish and maintain an incident response plan to ensure an effective and timely response to information security incidents
- Develop and implement processes to ensure the timely identification and investigation of information security incidents that could impact the business
- Establish and maintain processes to investigate and document information security incidents in order to determine the cause and respond appropriately
- Apply team-building skills, communications methods, and relationships from earlier domains to establish and maintain incident notification and escalation processes
- Organize, train and equip incident response teams to respond to information security incidents in an effective and timely manner
- Test, review and improve the incident response plan periodically to ensure an effective response to information security incidents and to improve response capabilities
- Establish and maintain communication plans and processes to manage communication with internal and external entities
- Conduct post-incident reviews to determine root causes, develop corrective actions, reassess risk, evaluate response effectiveness and take appropriate remedial actions
- Establish and maintain integration among the incident response plan, business continuity plan and disaster recovery plan

Audience

Prerequisites

Although none is required for the course, obtaining ISACA's CISM certification requires a minimum of 5 years of professional information security management work experience for certification. Full details regarding CISM requirements (including methods to waive up to 2 years' experience) is available from the ISACA site.

What You Will Learn