CISM®, Certified Information Security Manager® incl QAE

Duration: 4 Days   **Course Code: CISM**   **Version: 2023**   **Delivery Method: Virtual Learning**

Overview:

The CISM (Certified Information Security Manager) course is a globally recognized certification program designed for professionals in the field of information security management. It is offered by ISACA (Information Systems Audit and Control Association), a leading international professional association for IT governance, risk management, and cybersecurity.
The CISM certification focuses on the management and governance of information security within an organization. It provides a framework and best practices for developing, implementing, and managing an effective information security program.

Continuing Professional Education (CPE): 31
Practice questions (QAE = Questions, Answers and Explanations) : 12 month access

Please note : The exam is not included with the course but can be purchased seperately.

Virtual Learning

This interactive training can be taken from any location, your office or home and is delivered by a trainer. This training does not have any delegates in the class with the instructor, since all delegates are virtually connected. Virtual delegates do not travel to this course, Global Knowledge will send you all the information needed before the start of the course and you can test the logins.

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.
Experienced information security managers and those who have information security management responsibilities, including IT consultants, auditors, managers, security policy writers, privacy officers, information security officers, network administrators, security device administrators, and security engineers.

Objectives:

- **Learning Objectives:**

- **Module 1: Information Security Governance**

- Describe the role of governance in creating value for the enterprise.

- Explain the importance of information security governance in the context of overall enterprise governance.

- Describe the influence of enterprise leadership, structure and culture on the effectiveness of an information security strategy.

- Identify the relevant legal, regulatory and contractual requirements that impact the enterprise.

- Describe the effects of the information security strategy on enterprise risk management.

- Evaluate the common frameworks and standards used to govern an information security strategy.

- Explain why metrics are critical in developing and evaluating the information security strategy.

- Information Risk Management and Compliance

- Distinguish between common IS standards and frameworks available to build an information security program.

- Explain how to align IS policies, procedures and guidelines with the needs of the enterprise.

- Describe the process of defining an IS program road map.

- Outline key IS program metrics used to track and report progress to senior management.

- Explain how to manage the IS program using controls.

- Create a strategy to enhance awareness and knowledge of the information security program.

- Describe the process of integrating the security program with IT operations and third-party providers.

- Communicate key IS program information to relevant stakeholders.

- **Module 4: Information Security Incident Management**

- Distinguish between incident management and incident response

- Outline the requirements and procedures necessary to develop an

- Information Security Program Development and Management

- Information Security Incident Management

- **Module 2: Information Security Risk Management**

- Apply risk assessment strategies to reduce the impact of information security risk.

- Assess the types of threats faced by the enterprise.

- Explain how security control baselines affect vulnerability and control deficiency analysis.

- Differentiate between application of risk treatment types from an information security perspective.

- Describe the influence of risk and control ownership on the information security program.

- Outline the process of monitoring and reporting information security risk.

- **Module 3: Information Security Program Development and Management**

- Outline the components and resources used to build an information security program.

- incident response plan.

- Identify techniques used to classify or categorize incidents.

- Outline 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 an enterprise.

- Describe the processes and methods used to investigate, evaluate and contain an incident.

- Identify the types of communications and notifications used to inform key stakeholders of incidents and tests.

- Outline the processes and procedures used to eradicate and recover from incidents.

- Describe the requirements and benefits of documenting events.

- Explain the relationship between business impact, continuity and incident response.

- Describe the processes and outcomes related to disaster recovery.

- Explain the impact of metrics and testing when evaluating the incident response plan.

Prerequisites:

Attendees should meet the following prerequisities:

- None required.

Testing and Certification

To become officially CISM certified, you need to meet the requirements below:

- Pass the official CISM exam
- Have at least 5 years of relevant work experience in at least two CISM domains (or 4 years of experience supplemented by an HBO+ education).
The CISM exam is focused on the four domains defined by ISACA. The actual exam takes 4 hours and consists of 150 English-language multiple choice questions. For more information on certification, please visit: https://www.isaca.org/credentialing/cism

Practice questions (QAE = Questions, Answers and Explanations) are available online via a voucher. The voucher is part of the course material. It allows you to practice during the training and is available up to 12 months after the training

---

Follow-on-Courses:
- CISAU - Certified Information Systems Auditor (CISA)
- CISSP - Official (ISC)2 Certified Information Systems Security Professional Training (CISSP) - Including Exam

---

Content:

Domain 1: Information Security Governance

- Enterprise Governance Overview
- Organizational Culture, Structures, Roles and Responsibilities
- Legal, Regulatory and Contractual Requirements
- Information Security Strategy
- Information Governance Frameworks and Standards
- Strategic Planning

Domain 2: Information Risk Management

- Risk and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Assessment, Evaluation and Analysis
- Information Risk Response
- Risk Monitoring, Reporting and Communication

Domain 3: Information Security Program Development ; Management

- IS Program Development and Resources
- IS Standards and Frameworks
- Defining an IS Program Road Map
- IS Program Metrics
- IS Program Management
- IS Awareness and Training
- Integrating the Security Program with IT Operations
- Program Communications, Reporting and Performance Management

Domain 4: Information Security Incident Management

- Incident Management and Incident Response Overview
- Incident Management and Response Plans
- Incident Classification/Categorization
- Incident Management Operations, Tools and Technologies
- Incident Investigation, Evaluation, Containment and Communication
- Incident Eradication, Recovery and Review
- Business Impact and Continuity
- Disaster Recovery Planning
- Training, Testing and Evaluation

Further Information:

For More information, or to book your course, please call us on Head Office 01189 123456 / Northern Office 0113 242 5931

info@globalknowledge.co.uk

www.globalknowledge.com/en-gb/

Global Knowledge, Mulberry Business Park, Fishponds Road, Wokingham Berkshire RG41 2GY UK