ISACA CISM®, Certified Information Security Manager® incl QAE

Duration: 4 Days **Course Code: CISM** **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) :** 6 month access
Please note :
"The exam is not included with the course. However, the exam voucher can be purchased separately when attending the associated training"
The exam voucher is available only to GK course attendees and cannot be purchased as a standalone product
Updated 9/2026

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:**
- **Domain 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.
- Identify the relevant legal, regulatory, and contractual requirements that impact the enterprise.
- Describe the influence of enterprise leadership, structure, and culture on the effectiveness of an information security strategy.
- Describe the effects of the information security strategy on enterprise risk management.
- Explain the relationship between enterprise architecture (EA) and effective enterprise governance.
- Evaluate the common frameworks and standards used to govern an information security strategy.
- Explain how to align information security policies, procedures, and guidelines with the needs of the enterprise.
- Describe the process of defining an information security program road map.
- Outline key information security program metrics used to track and report progress to senior management.
- Explain how to manage the information security 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 security program information to relevant stakeholders.
- **Domain 4 - Incident Management**
- Distinguish between incident management and incident response.

- Explain why metrics are critical in developing and evaluating the information security strategy.
- **Domain 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 the 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.
- **Domain 3 - Information Security Program**
- Describe the goals and objectives of an information security architecture.
- Outline the components and resources used to build an information security program.
- Distinguish between common information security standards and frameworks available for building an information security program.
- Outline the requirements and procedures necessary to develop an incident response plan.
- 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.
- 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.

Prerequisites:

No formal prerequisites. Basic information security knowledge is recommended.

Testing and Certification

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 6 months after the training.

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 .

NB: The exam voucher for the official CISM exam is not included in the course price. However, the exam voucher can be purchased when attending the associated training.

The exam voucher is available only to Global Knowledge course attendees and cannot be purchased as a standalone product.

Follow-on-Courses:

- CISSP Certification Preparation
- CISA, Certified Information Systems Auditor

Content:

Domain 1 - Information Security Governance

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

Domain 2 - Information Security Risk Management

- Emerging Risk and Threat Landscape
- Vulnerability and Control Deficiency Analysis
- Risk Assessment and Analysis
- Risk Treatment/Risk Response Options
- Risk and Control Ownership
- Risk Monitoring and Reporting

Domain 3 - Information Security Program

- Information Security Architecture
- Information Security Program Resources
- Information Security Industry Standards and Frameworks
- Information Security Policies, Standards, Procedures, and Guidelines
- Information Asset Identification and Classification
- Information Security Control Design and Selection
- Information Security Program Metrics Development
- Information Security Control Implementation and Integrations
- Information Security Control Testing and Evaluation
- Information Security Awareness and Training
- Management of External Services
- Information Security Program Metrics, Communications, and Reporting

Domain 4 - Incident Management

- Incident Response Plan
- Business Impact Analysis (BIA)
- Business Continuity Plan (BCP)
- Disaster Recovery Plan (DRP)
- Incident Classification/Categorization
- Incident Management Training, Testing, and Evaluation
- Incident Management Tools and Techniques
- Incident Investigation and Evaluation
- Incident Containment Methods
- Incident Response Communications
- Incident Eradication and Recovery
- Post-incident Review Practices

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com/en-eg/

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo