CISM® : Préparation à la certification Certified Information Security Manager®

Duration: 4 Days **Course Code: CISM** **Delivery Method: Classe à distance**

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
Updated 4/2026

Classe à Distance - site Client

Cette formation peut être suivie à distance en synchrone depuis n'importe quel site pourvu d'une connexion internet (2 Mb/s en symétrique recommandés). Le programme (théorie et pratique) suit le même déroulé pédagogique qu'en présentiel. La solution technologique adoptée permet aux apprenants à distance de suivre les présentations faites au tableau, de voir et d'entendre l'instructeur et les participants en temps réel, mais également d'échanger avec eux.

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.

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

The exam voucher for the official CISM exam will no longer be included in the course price from January 2023. You can order this exam as a separate product with it.

Follow-on-Courses:

- CISSP Certification Preparation
- CISA, Certified Information Systems Auditor

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:

• Compétence du formateur : Les experts qui animent la formation sont des spécialistes des matières abordées et ont au minimum cinq ans d'expérience d'animation. Nos équipes ont validé à la fois leurs connaissances techniques (certifications le cas échéant) ainsi que leur compétence pédagogique.
• Suivi d'exécution : Une feuille d'émargement par demi-journée de présence est signée par tous les participants et le formateur.
• En fin de formation, le participant est invité à s'auto-évaluer sur l'atteinte des objectifs énoncés, et à répondre à un questionnaire de satisfaction qui sera ensuite étudié par nos équipes pédagogiques en vue de maintenir et d'améliorer la qualité de nos prestations.

Délais d'inscription :

• Vous pouvez vous inscrire sur l'une de nos sessions planifiées en inter-entreprises jusqu'à 5 jours ouvrés avant le début de la formation sous réserve de disponibilité de places et de labs le cas échéant.
• Votre place sera confirmée à la réception d'un devis ou """"booking form""""" signé. Vous recevrez ensuite la convocation et les modalités d'accès en présentiel ou distanciel.
• Attention, si cette formation est éligible au Compte Personnel de Formation, vous devrez respecter un délai minimum et non négociable fixé à 11 jours ouvrés avant le début de la session pour vous inscrire via moncompteformation.gouv.fr.

Accueil des bénéficiaires :

• En cas de handicap : plus d'info sur globalknowledge.fr/handicap
• Le Règlement intérieur est disponible sur globalknowledge.fr/reglement