

CISM – Certified Information Security Manager («CS1»)

The intent of this training as well as certification is to provide a common body of knowledge for information security management. The CISM focuses on information risk management as the basis of information security.

Duration: 4 days

Price: 5'000.–

Course documents: Digital Courseware

Content

This training includes material on broader issues such as how to govern information security as well as on practical issues such as developing and managing an information security program and managing incidents.

We consider at Digicomp this training to be a real alternative to ISO 27001 Lead Auditor, specifically because it goes beyond auditing and focuses on the "best practices" management of IS.

1. Information Security Governance
 - Develop information security strategy to align with business strategy and direction
 - Establish reporting and communication channels regarding information security governance activities
2. Risk Management Process
 - Develop a systematic, analytical, and continuous risk management process
 - Understand and implement risk identification, analysis, and mitigation activities from the CISM training course
 - Define and prioritize risk mitigation strategies
 - Appropriately report changes in risk to the correct levels of management on a periodic and event-driven basis
3. Information Security Governance
 - Create and maintain plans for implementing a carefully designed information security governance framework
 - Develop information security baselines from organizational needs, as well as international standards
 - Ensure security is effectively incorporated into the organizations established change management processes at CISM training course
 - Effectively integrate information security policies, guidelines, procedures, and accountability into the organization's culture
4. Managing risks
 - Manage security risk from contracts; transfer risk with contracts
 - Understand information security compliance issues resulting from Sarbanes-Oxley
5. Strategic alignment
 - Properly align IT strategic planning with organizational strategic planning
 - Control risk within software development or acquisition projects
6. Financial Aspects
 - How to position information security management within the organization
 - Control IT security risk relating to IT funding
7. Organizational and enterprise culture issues
 - Manage risk associated with social engineering, physical infrastructure threats, malicious code, and software vulnerabilities at CISM course
8. Business Continuity Planning and Resilience
 - Integrating Information Security into Business Continuity, Disaster Recovery, and Incident Response

- Organize, train, and properly equip response teams

Key Learnings

To prepare you to the official exam provided by the ISACA.

Methodology & didactics

Starting in July, the course will be held in two blocks of two days each. In the week following the first two days, time is set aside for independent reflection and deepening of what has been learned. This phase serves as a solid basis to work on the contents of the last two sessions in a targeted way.

Target audience

Security Managers, IT Systems Managers, quality Managers, Project Managers

Requirements

Knowing the area of IT Gouvernance, see the course :

- [CISA – Certified Information Systems Auditor \(«CAM»\)](#)

Certification

The examination fee varies between USD 345.00 and USD 575.00, depending on the time of registration with ICASA, not included in the course fee. The CISA exam is only available through ISACA and is schedule three times per year (June, September & December). For more information, please visit the [ISACA website](#).

Any questions?

We are happy to advise you on +41 44 447 21 21 or info@digicomp.ch. You can find detailed information about dates on www.digicomp.ch/courses-security/information-security-data-protection/course-cism-certified-information-security-manager