



CISMP Information Security Management Principles Training Course

26 – 30 April 2027
Milan

CISMP Information Security Management Principles Training Course

Ref: 749_157082 **Date:** 26 – 30 April 2027 **Location:** Milan **Fees:** 7000 Euro

Overview

CISMP Information Security Management Principles Training Course is a five-day foundation course for security coordinators, IT managers, risk and compliance functions, operations staff, and auditors who leave with an Information Security Management Principles Workbook. Participants apply information security concepts, governance, risk assessment, policy, asset management, access control, operations security, incident management, business continuity, legal responsibilities, and improvement methods. Agile Leaders Training Center develops CISMP information security management principles.

Who Should Attend

- Information-security functions responsible for policies, controls, and management reporting
- IT-management functions responsible for services, assets, and security decisions
- Risk and compliance functions responsible for assessment and control evidence
- Security-operations functions responsible for access, monitoring, and incident handling
- Audit and assurance functions responsible for evaluating security-management practices

The course assumes participants have basic working IT knowledge and awareness of security controls and leaves out penetration testing, forensic acquisition, product configuration, and claims that attendance awards certification.

Departments and Industries

The course supports departments and industries that need consistent information-security decisions and control practices.

- Information security and IT management
- Risk, compliance, and internal audit
- Financial services and telecommunications
- Healthcare and digital-service organizations
- Industrial, logistics, and professional-service operations

Learning Objectives

By the end of this course, participants will be able to:



- Apply information-security concepts to business and technical contexts
- Build governance, policy, asset, and responsibility artifacts
- Evaluate risks and select proportionate control treatments
- Analyze access, operations, and technical-control requirements
- Build incident-management and business-continuity arrangements
- Evaluate legal, compliance, assurance, and improvement evidence

Course Agenda

Day 1: Security Principles and Governance

- Confidentiality, Integrity, and Availability Decision Matrix
- Threat, Vulnerability, Impact, and Risk Model
- Information Security Governance Responsibility Map
- Security Policy Hierarchy and Ownership Register
- Ethics, Assurance, and Accountability Checklist

Day 2: Risk, Assets, and Control Selection

- Information Asset Inventory and Valuation Sheet
- Risk Appetite and Tolerance Criteria
- Threat and Vulnerability Assessment Worksheet
- Risk Treatment and Control Selection Matrix
- Residual Risk Acceptance Record

Day 3: Access and Operations Security

- Identity, Authentication, Authorization, and Accounting Model
- Access-Control Role and Privilege Matrix
- Security Operations Responsibility Calendar
- Vulnerability, Patch, and Change Control Workflow
- Supplier and Cloud Security Review Checklist

Day 4: Incidents, Continuity, and Compliance

- Security Incident Classification and Escalation Matrix
- Incident Response Roles and Communication Plan
- Business Impact and Service Dependency Map
- Business Continuity and Recovery Strategy Sheet
- Legal, Compliance, and Audit Evidence Register

Day 5: Information Security Management Practice

- Exercise: Classify Assets and Assess Security Risks
- Exercise: Select Controls and Draft Policy Requirements
- Exercise: Analyze Access and Operations Evidence
- Exercise: Coordinate Incident and Continuity Decisions
- Capstone: Information Security Management Principles Workbook

Practical Exercises

The course uses suggested activities drawn from financial services, healthcare, telecommunications, industrial operations, logistics, and digital services.

- Suggested activity: classify information assets, assess threats and vulnerabilities, and document treatment decisions.
- Suggested activity: map responsibilities, draft policy requirements, and compare control options.
- Suggested activity: evaluate access records, operations evidence, and supplier-security findings.
- Suggested activity: coordinate an incident scenario with continuity, communication, and improvement actions.

FAQs

Who suits CISM information security management principles training, and what does it assume?

Security, IT, risk, compliance, operations, and audit functions suit the training; it assumes basic working IT knowledge and awareness of security-control activities.

How does CISM information security management training differ from technical cybersecurity training?

CISM information security management training focuses on governance, risk, policies, controls, incidents, continuity, legal responsibilities, and assurance rather than penetration testing, product configuration, or forensic investigation.

How do information security management principles support control selection?

Information security management principles support control selection by connecting assets, threats, vulnerabilities, impacts, risk appetite, treatment choices, ownership, evidence, and residual-risk decisions.

How should information security governance responsibilities be documented?

Information security governance responsibilities should be documented through accountable owners, delegated decision rights, policy responsibilities, escalation paths, reporting needs, and review arrangements.



What belongs in an Information Security Management Principles Workbook?

An Information Security Management Principles Workbook includes governance maps, policy structures, asset records, risk assessments, control decisions, access models, operations workflows, incident arrangements, continuity dependencies, compliance evidence, and improvement actions.

Conclusion

Participants take back an Information Security Management Principles Workbook supported by governance maps, risk matrices, control records, access models, incident plans, continuity artifacts, and evidence registers. It changes disconnected security activities into traceable management decisions. The workbook provides a repeatable basis for control ownership, assurance, response coordination, and improvement.