

Advanced Cybersecurity and Cloud Security for IT Managers Training Course

28 December 2026 – 1 January 2027
Tokyo

AGILE LEADERS
Training Center

Advanced Cybersecurity and Cloud Security for IT Managers Training Course

Ref: 745_264831 **Date:** 28 December 2026 – 1 January 2027 **Location:** Tokyo **Fees:** 10000 Euro

Overview

Advanced Cybersecurity and Cloud Security for IT Managers Training Course is a one-week advanced course for IT, infrastructure, technical operations, and security managers who leave with a Cybersecurity and Cloud Security Management Action Plan. Participants apply the shared responsibility model, analyze asset and identity exposure, evaluate cloud configuration risk, review security architecture, prioritize controls through NIST CSF 2.0 and CSA CCM v4.1, oversee security logging and detection, coordinate cloud incident response, and align security investment priorities. Agile Leaders Training Center develops cybersecurity and cloud security management.

Who Should Attend

- Technology leaders responsible for cybersecurity and cloud-security decisions
- Infrastructure teams responsible for cloud services and control ownership
- Security functions responsible for monitoring and incident oversight
- Operations leaders responsible for service resilience and supplier coordination
- Managers responsible for security investment and performance reporting

The course assumes participants govern technology services or security decisions and leaves out hands-on cloud engineering, certification exam preparation, introductory awareness, and AI cybersecurity tools.

Departments and Industries

The course supports departments and industries where managers must connect technical security evidence with cloud-service decisions and operational accountability.

- Information technology and cloud operations
- Cybersecurity and infrastructure management
- Financial services and telecommunications
- Healthcare and professional-service organizations
- Industrial, logistics, and digital-service operations

Learning Objectives

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

- Apply NIST CSF 2.0 outcomes to management decisions
- Analyze shared responsibility across cloud service relationships
- Evaluate identity, configuration, and data exposure evidence
- Prioritize cloud controls using CSA CCM v4.1
- Assess monitoring, detection, and incident coordination arrangements
- Build a Cybersecurity and Cloud Security Management Action Plan

Course Agenda

Day 1: Cybersecurity Risk and Cloud Responsibility

- NIST CSF 2.0 Governance Outcome Map
- Cybersecurity Risk Decision Register
- Cloud Shared Responsibility Matrix
- Cloud Service and Data Dependency Map
- Security Ownership and Accountability Chart

Day 2: Exposure and Architecture Review

- Asset and Identity Exposure Register
- Privileged Access Review Checklist
- Cloud Configuration Risk Assessment
- Data Protection Flow Map
- Security Architecture Decision Record

Day 3: Control Selection and Supplier Assurance

- CSA CCM v4.1 Control Mapping
- Control Coverage and Evidence Matrix
- Cloud Change and Configuration Review
- Third-Party Security Assurance Questionnaire
- Control Gap Prioritization Grid

Day 4: Detection, Incidents, and Performance

- Security Logging Coverage Map
- Detection Oversight and Escalation Dashboard
- Cloud Incident Coordination Playbook
- Business Continuity Dependency Review
- Cybersecurity Performance Indicator Set

Day 5: Security Management Decision Practice

- Exercise: Map Shared Responsibility and Ownership
- Exercise: Review Identity and Configuration Exposure
- Exercise: Prioritize Cloud Control Gaps
- Exercise: Coordinate Detection and Incident Decisions
- Capstone: Cybersecurity and Cloud Security Management Action Plan

Practical Exercises

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

- Suggested activity: map security responsibilities across an organization and its cloud suppliers.
- Suggested activity: review identity, configuration, and data-flow evidence for management decisions.
- Suggested activity: compare cloud control gaps and prioritize remediation using risk and dependency criteria.
- Suggested activity: coordinate a cloud incident scenario and revise security performance indicators.

FAQs

Who suits advanced cybersecurity and cloud security management training, and what does it assume?

IT, infrastructure, technical operations, and security managers suit the training; it assumes they govern technology services, control ownership, risk decisions, or incident coordination.

How does cybersecurity and cloud security management differ from cloud engineering training?

Cybersecurity and cloud security management concentrates on risk, responsibility, control evidence, oversight, incidents, metrics, and investment decisions rather than platform deployment or hands-on configuration.

How should IT managers apply the cloud shared responsibility model?

IT managers should map each security responsibility to the organization, cloud provider, or supplier, verify evidence, assign accountable owners, and identify gaps at service boundaries.

How can IT managers prioritize cloud security controls?

IT managers can prioritize cloud security controls by comparing exposure, business dependency, control coverage, evidence strength, supplier responsibility, and the operational impact of untreated gaps.

AGILE LEADERS
Training Center

What belongs in a Cybersecurity and Cloud Security Management Action Plan?

A Cybersecurity and Cloud Security Management Action Plan includes risks, service dependencies, responsibility assignments, exposure findings, control gaps, monitoring priorities, incident decisions, suppliers, performance indicators, investments, owners, and target actions.

Conclusion

Participants take back a Cybersecurity and Cloud Security Management Action Plan supported by responsibility maps, exposure registers, architecture records, control mappings, detection dashboards, and incident playbooks. It changes fragmented technical evidence into prioritized management decisions with accountable owners. The plan gives technology leaders a repeatable basis for oversight, escalation, investment, and improvement.