Certified Lead Cloud Security Manager Training Course - ISO/IEC 27017 & 27018

15 – 19 March 2027
Tbilisi

AGILE LEADERS
Training Center

AGILE LEADERS
Training Center

Certified Lead Cloud Security Manager Training Course - ISO/IEC 27017 & 27018

Ref: 103600297_98923 **Date:** 15 – 19 March 2027 **Location:** Tbilisi **Fees:** 5700 Euro

Course Overview

The Certified Lead Cloud Security Manager Training Course - ISO/IEC 27017 & 27018 is designed to equip professionals with the essential tools, methodologies, and frameworks required to manage and enhance cloud security programs in line with recognized international standards. This comprehensive training covers the full lifecycle of cloud security program implementation, from risk assessment and control selection to incident management, awareness training, and documentation best practices.

Cloud environments present unique challenges, including data privacy risks, evolving compliance requirements, and the complexity of hybrid and multi-cloud models. Participants will gain deep insight into cloud security risk management, cloud security policies and procedures development, and the application of cloud-specific controls ISO 27017 to secure cloud infrastructure and services.

Additionally, the course highlights the importance of cloud data protection ISO 27018 to safeguard personally identifiable information PII, ensuring privacy in cloud computing is embedded into every stage of cloud adoption. Through interactive sessions, case studies, hands-on exercises, and collaborative group work, participants will leave with practical strategies to embed cloud security best practices into their organization's cloud ecosystem.

Target Audience

- Cloud security managers
- Information security officers
- IT infrastructure and operations managers
- Cloud architects and engineers
- Risk management professionals
- Compliance officers and legal teams
- Data protection and privacy officers
- Cloud security consultants and advisors

AGILE LEADERS
Training Center

Targeted Organizational Departments

- IT and cybersecurity departments
- Risk and compliance teams
- Cloud governance and strategy units
- Legal and data privacy functions
- Internal audit teams
- Cloud infrastructure and DevOps teams
- Managed service providers MSPs

Targeted Industries

- Financial services banks, insurance, fintech
- Healthcare and pharmaceuticals
- Telecommunications
- Retail and e-commerce
- Government agencies and public sector
- Technology, software development, and SaaS companies
- Manufacturing and logistics with cloud-based operations
- Energy and utilities leveraging cloud solutions

Course Offerings

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

- Develop and implement a cloud security program tailored to organizational needs
- Apply cloud security best practices aligned with ISO/IEC 27017 training and ISO/IEC 27018 certification principles
- Assess, identify, and mitigate cloud-specific risks through structured cloud security risk management approaches
- Develop comprehensive cloud security policies and procedures covering operational, technical, and governance aspects
- Design and implement cloud-specific controls ISO 27017 across IaaS, PaaS, and SaaS environments
- Establish and enhance cloud security documentation practices to support audits, reporting, and internal governance
- Create and deliver effective cloud security awareness training for all organizational levels
- Respond to and manage cloud security incidents through structured cloud security incident response training
- Support secure cloud migration training processes to ensure security is embedded into cloud adoption projects
- Ensure ongoing compliance with applicable cloud compliance and regulations in their industry

AGILE LEADERS
Training Center

Training Methodology

This training is highly practical, blending expert instruction with real-world case studies, interactive group work, collaborative problem-solving, and guided exercises tailored to the participants' industries and cloud environments.

Each session integrates live discussions, risk assessment exercises, hands-on development of cloud security policies and procedures, and team-based simulations for cloud security incident management. Special focus is placed on privacy in cloud computing and cloud data protection ISO 27018 to ensure participants understand how to embed privacy controls into cloud processes and documentation.

Role-play scenarios will challenge participants to apply cloud-specific controls ISO 27017 to evolving hybrid and public cloud environments, reinforcing practical skills needed to address emerging threats and regulatory expectations. Reflection sessions at the end of each day allow participants to consolidate learning and exchange insights with peers.

Course Toolbox

- Comprehensive digital course workbook with guidelines, templates, and checklists
- Example cloud security policies and procedures aligned to ISO/IEC 27017 and ISO/IEC 27018
- Practical cloud risk assessment training templates
- Sample cloud security documentation practices and audit checklists
- Cloud security awareness training slide decks and communication materials
- Cloud security incident response training scenarios and response checklists
- Case studies illustrating real-world cloud security best practices
- Tools are not provided directly, but practical insights, frameworks, and real-world examples of tools are covered extensively

Course Agenda

Day 1: Foundations of Cloud Security and Governance

- Topic 1: Introduction to cloud security best practices and their role in cloud security program implementation, with a focus on aligning with ISO/IEC 27017 training and ISO/IEC 27018 certification.
- Topic 2: Defining cloud security policies and procedures that address cloud-specific risks, data protection, and cloud compliance and regulations across different service models.
- Topic 3: Establishing cloud security roles and responsibilities within IT, cybersecurity, and governance teams to ensure effective cloud security awareness training.
- Topic 4: Developing cloud security documentation practices that support ongoing risk management, incident response, and audits.
- Topic 5: Overview of hybrid cloud security training approaches for organizations using multi-cloud and hybrid environments.
- Reflection & Review: Group discussion on how participants' organizations currently manage cloud security programs and initial steps to enhance them using cloud-specific controls ISO 27017.

AGILE LEADERS
Training Center

Day 2: Cloud Security Risk Management and Control Design

- Topic 1: Introduction to cloud security risk management and cloud risk assessment training techniques, emphasizing identification of cloud-specific vulnerabilities.
- Topic 2: Applying cloud security best practices to develop cloud security policies and procedures that mitigate identified risks and support secure cloud migration training.
- Topic 3: Selection and implementation of cloud-specific controls ISO 27017 across public cloud, private cloud, and community cloud security certification environments.
- Topic 4: Mapping cloud security documentation practices to risk management processes for improved traceability and accountability.
- Topic 5: Privacy in cloud computing and the role of cloud data protection ISO 27018 in protecting personally identifiable information PII.
- Reflection & Review: Participants share examples of cloud risk scenarios from their organizations and collaboratively identify appropriate cloud-specific controls ISO 27017.

Day 3: Security Awareness, Data Protection, and Incident Management

- Topic 1: Designing and delivering effective cloud security awareness training programs for technical teams, management, and non-technical staff.
- Topic 2: Integrating privacy in cloud computing principles into cloud security program implementation, with emphasis on cloud data protection ISO 27018.
- Topic 3: Developing and documenting cloud security incident response training programs to improve organizational readiness for cloud security incidents.
- Topic 4: Practical simulation of cloud security incident management processes, covering detection, containment, investigation, and recovery.
- Topic 5: Cloud security documentation practices for capturing incident logs, lessons learned, and incident reporting aligned with cloud compliance and regulations.
- Reflection & Review: Participants review the day's incident response scenarios, comparing approaches across different industries and cloud architectures.

Day 4: Secure Cloud Operations and Continuous Improvement

- Topic 1: Cloud security testing and monitoring processes to identify vulnerabilities, assess compliance, and ensure continuous alignment with cloud security best practices.
- Topic 2: Developing secure cloud migration training processes that embed security requirements into cloud migration projects and hybrid cloud security training initiatives.
- Topic 3: Enhancing cloud security documentation practices to align with industry requirements, internal governance, and regulatory reporting.
- Topic 4: Exploring cloud security consulting services approaches to advise business units and third-party service providers on cloud security program implementation.
- Topic 5: Establishing continuous improvement processes for maintaining cloud security best practices and evolving them to meet emerging threats and regulatory changes.
- Reflection & Review: Group brainstorming session on future trends in cloud security risk management, cloud compliance and regulations, and cloud-specific controls ISO 27017.

AGILE LEADERS
Training Center

Day 5: Real-World Application and Advanced Topics

- Topic 1: Case study workshop: Applying cloud security policies and procedures, cloud risk assessment training techniques, and cloud-specific controls ISO 27017 to a complex hybrid cloud environment.
- Topic 2: Developing tailored cloud security awareness training and incident response training programs for different organizational levels and third parties.
- Topic 3: Implementing cloud security consulting services frameworks to assess, design, and enhance cloud security program implementation across industries.
- Topic 4: Applying cloud security best practices to community cloud security certification, public cloud security certification, and hybrid cloud security training scenarios.
- Topic 5: Advanced cloud security documentation practices for creating audit-ready reports, executive summaries, and regulatory compliance packages.
- Reflection & Review: Participants develop individual action plans for enhancing their organization's cloud security program, using insights from the entire training.

FAQ

What specific qualifications or prerequisites are needed for participants before enrolling in the course?

There are no mandatory prerequisites, but a foundational understanding of cloud computing, information security management, and risk management principles will enhance participants' learning experience. The course is ideal for individuals involved in cloud security manager certification tracks, cloud security consulting services, or those responsible for cloud governance, risk, and compliance.

How long is each day's session, and is there a total number of hours required for the entire course?

Each day's session typically runs 4 to 5 hours, incorporating instructional segments, case studies, group work, and interactive discussions. Across five days, participants will complete approximately 20 to 25 hours of structured learning.

How do ISO/IEC 27017 and ISO/IEC 27018 apply to hybrid cloud security and privacy protection?

ISO/IEC 27017 provides guidelines for applying cloud-specific controls ISO 27017 to secure hybrid cloud environments, ensuring both service providers and customers understand their responsibilities. ISO/IEC 27018 enhances this by introducing privacy-specific controls focused on safeguarding personally identifiable information PII, which is particularly crucial when handling sensitive data in public and hybrid clouds.

AGILE LEADERS
Training Center

How This Course is Different from Other Certified Lead Cloud Security Manager Courses

This training stands out for its highly practical, hands-on focus. Rather than just theoretical instruction, participants actively develop cloud security policies and procedures, assess cloud-specific risks, build cloud security documentation practices, and manage simulated cloud security incidents. By integrating cloud risk assessment training, secure cloud migration training, and real-world case studies, the course ensures participants leave with practical tools they can apply immediately.