

ISO/IEC 27017 - Certified Lead Implementer



www.gaqm.org

ISO/IEC 27017 - Certified Lead Implementer — Certification Overview

ISO/IEC 27017:2015 is an international standard providing guidelines for information security controls specifically for cloud services. The Cloud Security Implementer certification equips professionals with the knowledge and skills to implement and manage cloud-specific security controls effectively. This standard extends ISO/IEC 27002 by offering additional guidance for both cloud service providers (CSPs) and cloud service customers (CSCs), ensuring the confidentiality, integrity, and availability of data hosted in cloud environments. Certified implementers learn how to assess cloud risks, design security frameworks, and adopt best practices that align with organizational objectives.

The certification focuses on practical implementation skills, enabling participants to establish secure cloud infrastructures, develop cloud security policies, and maintain compliance with relevant regulations. It emphasizes risk assessment and mitigation, access management, encryption, incident response, and secure service agreements. Professionals also learn how to integrate cloud security measures with existing organizational information security management systems (ISMS), thereby providing a seamless approach to protecting data in multi-tenant cloud environments.

By attaining the ISO/IEC 27017 - Certified Lead Implementer certification, individuals demonstrate their capability to safeguard cloud services against emerging threats and vulnerabilities. They gain the confidence to implement robust security controls, ensuring stakeholders and customers can trust the organization's cloud infrastructure. This certification is increasingly recognized by organizations adopting cloud technologies, helping certified professionals advance their careers in cybersecurity, IT governance, and cloud service management.

Target Audience

- IT security professionals and cloud engineers responsible for managing cloud environments
- Information security managers seeking to extend ISMS to cloud-based services
- Cloud service providers (CSPs) aiming to implement internationally recognized security controls
- Compliance and risk management officers overseeing cloud service agreements
- Consultants and auditors who provide guidance on cloud security implementation
- Professionals involved in governance, risk, and compliance (GRC) within cloud infrastructure

What Modules are covered?

Module 1 - Introduction to Cloud Security and ISO/IEC 27017

- Overview of ISO/IEC 27017 and its relation to ISO/IEC 27002 & ISO/IEC 27001
- Key concepts of cloud computing: SaaS, PaaS, IaaS, public, private, hybrid clouds
- Cloud security challenges and risks
- Benefits of adopting ISO/IEC 27017 for cloud environments
- Roles and responsibilities of cloud service providers (CSPs) and customers (CSCs)

Module 2 - Cloud Risk Assessment and Management

- Identifying cloud-specific threats and vulnerabilities
- Risk assessment methodologies for cloud services
- Determining risk levels and prioritization
- Risk mitigation strategies in cloud environments
- Integration of cloud risk management with existing ISMS

Module 3 - Implementing Cloud Security Controls

- Guidance on controls for cloud service providers and customers
- Identity and access management (IAM) in cloud services
- Data classification, handling, and protection in the cloud
- Encryption, key management, and secure communication protocols
- Monitoring, logging, and auditing cloud activities

Module 4 - Cloud Service Agreements and Compliance

- Understanding Service Level Agreements (SLAs) and cloud contracts
- Security obligations for CSPs and customers
- Compliance requirements (e.g., GDPR, regional regulations)
- Implementing audit-ready documentation and policies
- Vendor and third-party risk management in cloud services

Module 5 - Incident Management and Business Continuity

- Incident detection, response, and reporting in cloud environments
- Managing data breaches and security incidents
- Business continuity planning for cloud services
- Disaster recovery strategies in multi-cloud or hybrid environments
- Lessons learned and continual improvement of cloud security controls

Module 6 - Integration and Continuous Improvement

- Integrating ISO/IEC 27017 controls with ISO/IEC 27001 ISMS
- Continuous monitoring and performance evaluation of cloud security
- Key performance indicators (KPIs) and metrics for cloud security
- Training, awareness, and competence for cloud teams
- Maintaining compliance and implementing continual improvement processes