iGUIDE

ISMS

Information Security
Use of Cloud Services

INFOSECBASE

Contents

A Guide to Information Security Use of Cloud Services

Introduction

Cloud computing provides scalability and cost savings but introduces security challenges. ISO 27001control A.5.23 offers a structured approach to securing cloud environments. This guide outlines essential security controls to help organisations manage risks effectively.

Key Controls for Cloud Security

Security Policies

- Define and update cloud security policies.
- Address data protection, access management and compliance.
- Ensure alignment with regulatory requirements and industry standards.
- Communicate policies effectively to all stakeholders.

Risk Management

- Identify risks like data breaches, service outages and unauthorised access.
- Conduct regular risk assessments and document findings.
- Implement encryption, MFA, network segmentation and access controls.
- Establish incident response plans specific to cloud-based threats.

Asset and Access Control

- Maintain an inventory of cloud assets and classify data based on sensitivity.
- Use RBAC (Role-Based Access Control) and enforce the principle of least privilege.
- Implement MFA for accessing sensitive cloud resources.
- Regularly review and update access permissions to prevent unauthorised access.

Cryptography & Operations Security

- Encrypt sensitive data both in transit and at rest using industry standards.
- Implement robust key management policies and restrict key access.
- Monitor cloud activities through logging and security event management.
- Apply security patches promptly and automate updates where possible.

Third-Party & Compliance Management

- Assess cloud providers against compliance frameworks (e.g. GDPR, HIPAA, SOC 2).
- Define security responsibilities in contractual agreements with providers.
- Regularly audit third-party security measures and verify compliance.
- Ensure data processing agreements address confidentiality and data protection requirements.

Business Continuity aND Monitoring

- Develop and test disaster recovery plans to minimise downtime.
- Establish redundancy and backup mechanisms for critical cloud-based services.
- Conduct regular security audits and penetration tests to identify vulnerabilities.
- Use security monitoring tools to detect and respond to threats in real time.

Implementation Steps

- **Define Scope**: Identify which cloud services and assets fall under the ISMS.
- **Conduct a Risk Assessment**: Analyse security risks and vulnerabilities.
- **Develop Security Controls**: Implement necessary technical and procedural safeguards.
- **Train Personnel**: Provide cloud security awareness training.
- **Monitor & Audit**: Continuously review security measures for effectiveness.
- **Improve & Adapt**: Update security strategies based on new threats and compliance requirements.

Summary

ISO 27001:2022 A.5.23 provides a framework for securing cloud services. Key measures include establishing security policies, managing risks, controlling access, encrypting data, ensuring compliance and maintaining business continuity. By following these guidelines, organisations can strengthen their cloud security posture and reduce potential threats.