iGUIDE

ISMS

Independent Reviews, Compliance and DOPs

iNFOSECBASE

Contents

A Guide to Information Security Independent Reviews, Compliance and Documented Operating Procedures (DOPs)

Introduction

ISO 27001 provides a structured framework for managing information security risks. Three critical aspects of compliance with ISO 27001:2022 include independent reviews (A.5.35), compliance with security policies (A.5.36) and documented operating procedures (A.5.37). These controls help organisations ensure their security controls remain effective, that policies are followed and processes are well-documented to maintain a consistent security posture.

This guide outlines the purpose, implementation and best practices for each of these requirements to help organisations maintain compliance and strengthen their Information Security Management System (ISMS).

Independent Reviews of Information Security

Purpose

Independent reviews of information security ensure that security policies, procedures and controls remain effective, aligned with business objectives and compliant with regulatory requirements. These reviews help organisations identify weaknesses, assess risks and implement improvements.

Implementation Steps

- **Define Review Objectives**: Establish the scope, criteria and frequency of independent security reviews.
- **Select Independent Reviewers**: Use internal auditors, external security consultants or regulatory bodies for unbiased assessments.
- **Conduct Security Assessments**: Evaluate policies, technical controls and incident response effectiveness.
- **Document Findings**: Identify gaps, non-conformities and areas for improvement.
- **Report to Management**: Share findings with senior leadership for decision-making.
- **Implement Corrective Actions**: Address identified weaknesses and track resolution progress.

Best Practices

- Schedule periodic reviews (e.g. annually or after significant security incidents).
- Use recognised security frameworks (e.g. ISO 27001, NIST etc.) as benchmarks.
- Ensure review findings result in actionable improvements.

Compliance with Policies, Rules and Standards

Purpose

Ensuring compliance with security policies and standards is essential for maintaining a strong security posture. Compliance minimises the risk of security breaches, regulatory penalties and operational disruptions.

Implementation Steps

- **Develop Security Policies**: Define clear security policies, aligned with legal and business requirements.
- **Communicate Policies**: Ensure all employees and third parties are aware of and understand security rules.
- **Monitor Compliance**: Conduct internal audits, security assessments and automated compliance checks.
- **Enforce Consequences for Non-Compliance**: Establish disciplinary actions and remedial steps for violations.
- **Conduct Training & Awareness**: Educate employees on security policies and industry best practices.

Best Practices

- Integrate compliance monitoring with security tools (e.g. SIEM, endpoint protection).
- Perform regular security audits to assess adherence to policies.
- Encourage a culture of security awareness through training programs.

Documented Operating Procedures

Purpose

Documented operating procedures ensure security-related tasks are consistently performed, reducing the risk of human error and enabling effective incident response, system maintenance and compliance verification.

Implementation Steps

- **Identify Critical Processes**: Determine which security operations require formal documentation (e.g. incident response, access control, data encryption, technical operations).
- **Create Standard Operating Procedures (SOPs)**: Develop step-by-step instructions for executing security tasks.
- **Ensure Accessibility**: Store procedures securely but ensure they are accessible to authorised personnel.
- **Review & Update Regularly**: Periodically revise documents to reflect changes in technology, threats and regulations.
- **Train Employees on Procedures**: Ensure staff understand and can follow documented procedures effectively.

Best Practices

- Use a version control system to track updates to procedures.
- Maintain a centralised document repository with access controls.
- Simulate security scenarios to validate SOP effectiveness.

Summary

By implementing independent security reviews, ensuring compliance with security policies and maintaining documented operating procedures, organisations can strengthen their ISMS, reduce security risks and demonstrate ongoing commitment to information security. Regular assessments, continuous training and well-documented processes contribute to a resilient and ISO 27001-compliant security environment.