iGUIDE

ISMS

Information Security Technical Operating Procedures

INFOSECBASE

Contents

A Guide to Information Security Technical Operating Procedures

Introduction

ISO 27001:2022 emphasises the importance of secure technical operating procedures to ensure the confidentiality, integrity and availability of information systems. Organisations must implement structured controls to manage system capacity, configuration, redundancy and security across their IT environments.

This guide outlines key requirements and best practices for implementing technical operating procedures under ISO 27001:2022, covering aspects such as capacity management, configuration management, secure system architecture, network segregation, application security and more.

What Are Technical Operating Procedures in ISO 27001:2022?

In the context of ISO 27001:2022, Technical Operating Procedures (TOPs) are detailed, structured documents that describe the specific technical actions or processes used to manage and protect information within the organisation's Information Security Management System (ISMS). These procedures outline how various technical controls and systems are operated, monitored and maintained to ensure the confidentiality, integrity and availability of information.

ISO 27001:2022 focuses on establishing, implementing, maintaining and continually improving an ISMS. The standard itself does not provide specific procedures but rather sets out the framework for organisations to design and implement such procedures to manage information security risks.

Key Technical Operating Controls in ISO 27001:2022

Capacity Management

Objective

Ensure that IT resources can handle current and future demands without performance degradation.

Key Requirements

- Monitor and analyse system performance to anticipate capacity needs.
- Implement proactive resource scaling to prevent bottlenecks.
- Maintain capacity plans to align IT resources with business objectives.

Best Practices

- Use automated monitoring tools to track CPU, memory, disk and network usage.
- Implement alerts for abnormal system loads and resource exhaustion.
- Regularly review and update capacity plans to match business growth.

Configuration Management

Objective

Ensure IT systems are securely configured and maintained to prevent vulnerabilities.

Key Requirements

- Define a baseline configuration for all IT assets.
- Document and track all system configurations.
- Apply change control procedures before modifying configurations.

Best Practices

- Use configuration management tools for automation.
- Regularly audit configurations for compliance with security policies.
- Restrict administrative privileges to authorised personnel only.

Redundancy of Information Processing Facilities

Objective

Prevent service disruptions by ensuring critical systems have failover and backup mechanisms.

Key Requirements

- Implement redundant infrastructure for critical IT systems.
- Ensure backups and failover systems are tested periodically.
- Maintain disaster recovery (DR) and business continuity (BC) plans.

Best Practices

- Use geographically separate data centres for redundancy.
- Perform regular DR drills to validate failover procedures.
- Implement high-availability (HA) clustering for critical applications.

Clock Synchronisation

Objective

Ensure that all system clocks are accurately synchronised to maintain data integrity and auditability.

Key Requirements

- Use Network Time Protocol (NTP) servers to sync system clocks.
- Ensure consistent timestamps across logs, applications and databases.
- Monitor clock drift to prevent discrepancies.

Best Practices

- Use multiple NTP sources for redundancy.
- Regularly verify time synchronisation across systems.
- Enforce clock synchronisation policies for all networked devices.

Use of Privileged Utility Programs

Objective

Prevent unauthorised access and misuse of powerful administrative tools.

Key Requirements

- Restrict access to privileged utilities (e.g. command-line tools, debugging software).
- Implement multi-factor authentication (MFA) for privileged access.
- Log and monitor all usage of administrative tools.

Best Practices

- Use Privileged Access Management (PAM) solutions to enforce least privilege.
- Regularly review privileged access logs for anomalies.
- Disable or remove unnecessary privileged utilities.

Installation of Software on Operational Systems

Objective

Prevent unauthorised and unverified software installations that could introduce security risks.

Key Requirements

- Implement an approval process for software installations.
- Restrict installation rights to authorised personnel only.
- Regularly update and patch all installed software.

Best Practices

- Use application whitelisting to prevent unauthorised software.
- Conduct security assessments before deploying new software.
- Implement endpoint security tools to monitor software installations.

Segregation of Networks

Objective

Protect sensitive data by separating network environments based on security needs.

Key Requirements

- Implement logical and physical segmentation for internal and external networks.
- Use firewalls and VLANs to restrict access between network zones.
- Monitor network traffic to detect unauthorised access attempts.

Best Practices

- Enforce zero-trust network architecture principles.
- Use dedicated networks for sensitive systems (e.g. financial, medical data).
- Regularly test network segmentation to ensure effectiveness.

Application Security Requirements

Objective

Ensure applications are securely designed and developed to prevent vulnerabilities.

Key Requirements

- Apply secure coding practices throughout the Software Development Lifecycle (SDLC).
- Conduct regular security testing (e.g. penetration testing, vulnerability testing, code reviews).
- Implement input validation to prevent injection attacks.

Best Practices

- Use automated static and dynamic application security testing (SAST/DAST) tools.
- Regularly train developers on secure coding techniques.
- Follow industry standards (e.g. OWASP Top 10) for application security.

Secure System Architecture and Engineering Principles

Objective

Design and maintain resilient IT architectures to support security and business needs.

Key Requirements

- Follow a layered security approach (defence in depth).
- Apply least privilege principles in system design.
- Use encryption for data protection.

Best Practices

- Implement zero-trust architecture (ZTA).
- Conduct regular security assessments on system architecture.
- Use micro segmentation to enhance security boundaries.

Outsourced Development

Objective

Ensure security requirements are enforced when using third-party developers.

Key Requirements

- Define security requirements in contracts with vendors.
- Perform security audits on outsourced code.
- Restrict external access to internal development environments.

Best Practices

- Use code repositories with access control for external developers.
- Ensure secure data transfer methods between internal and external teams.

- Conduct penetration tests on third party-developed software.

Separation of Development, Test and Production Environments

Objective

Reduce security risks by segregating IT environments.

Key Requirements

- Ensure strict separation between development, testing and production systems.
- Restrict access between environments based on role-based access control (RBAC).

Best Practices

- Use separate infrastructure and credentials for each environment.
- Monitor data movement between environments to prevent leaks.

Test Information

Objective

Prevent the use of sensitive production data in test environments.

Key Requirements

- Anonymise or mask production data before using it for testing.
- Restrict access to test environments.

Best Practices

- Use synthetic data instead of real customer data for testing.
- Regularly audit test environments for security compliance.

Protection of Information Systems During Audit Testing

Objective

Ensure audits do not introduce security risks or operational disruptions.

Key Requirements

- Define controlled testing procedures to protect live systems.
- Monitor audit activities to detect anomalies.

Best Practices

- Use isolated testing environments for security assessments.
- Ensure minimal system impact during penetration tests and audits.

Summary

ISO 27001:2022 technical operating procedures play a crucial role in ensuring the security, availability and integrity of IT systems. Organisations must implement structured controls covering capacity management, configuration management, redundancy, network segregation, secure authentication and application security to mitigate risks effectively. Key security measures include restricting privileged access, ensuring secure software installation, implementing network segmentation and enforcing secure system architecture principles.

Additionally, outsourced development, separation of IT environments and secure audit testing must be carefully managed to prevent vulnerabilities. By adopting these best practices, organisations can enhance cybersecurity, protect sensitive information and comply with ISO 27001:2022 requirements, ensuring a resilient and well-secured IT infrastructure.