ISO 27001:2022 Gap Analyse

This report outlines the current status of the ISO 27001:2022 GAP analyse and identifies relevant gaps.

It has been fully automated and generated using AI support. Please note that, while efforts have been made to ensure accuracy, AI-generated outputs may contain errors, just like human-generated reports. All findings should be validated as part of the internal review process.

1. Scope of the GAP

1.1 Applicability

This internal audit covers the Information Security Management System (ISMS) of [company-name] as defined under the scope of its ISO/IEC 27001:2022 certification, in accordance with the internal audit planning for that standard.

1.2 Participants in the Audit

The internal audit was conducted on [date-of-report], focusing on the management system in place at [company-name].

Participants:

On behalf of [company-name]

[name-1]

[name-2]

[name-3]

On behalf of Valecta

Stephan Csorba

1.3 Audit Criteria

The audit was carried out in accordance with the ISO/IEC 27001:2022 standard by Valecta.

1.4 Audit Objectives

The purpose of this GAP-analyse was to assess, on a sample basis, the functioning and effectiveness of the ISMS as implemented at [company-name] in accordance with ISO/IEC 27001:2022 requirements.

1.5 Scope of Entities Included in the Internal Audit

This internal audit included the following legal entities:

[company-name-1]

[company-name-2]

2. Executive Summary

2.1 Sampling Methodology

Please note that the audit was conducted based on a sampling approach, meaning that findings and conclusions are based on a selected sample of processes and data, not on 100% evaluation. The goal is to provide reasonable assurance rather than absolute certainty. This methodology proved effective and enabled the organization to identify targeted improvement actions.

2.2 General Impressions of the Management System

The ISMS at [company-name] demonstrates a mature and comprehensive implementation of ISO/IEC 27001:2022 controls, with well-defined policies, procedures, and evidence supporting most organizational, people, physical, and technological controls. Management commitment is evident through regular reviews, training, and incident management processes. The organization has established strong supplier management and incident response capabilities.

However, some areas require attention to fully meet the standard’s expectations and to strengthen the ISMS further.

2.2.1 Highlights

- Comprehensive Information Security Policy covering roles, responsibilities, access control, incident management, and compliance.

- Effective access control and identity management with formal user registration, de-registration, and privileged access controls.

- Robust incident management processes including detection, response, learning, and evidence collection.

- Well-documented business continuity and disaster recovery plans with defined recovery objectives.

- Strong network security, cryptography, and secure development lifecycle practices.

- Regular internal and external audits with management reviews and corrective actions.

- Thorough supplier relationship management including contracts, SLAs, and risk assessments.

- Extensive employee screening, training, and disciplinary processes.

2.2.2 Findings

- Evidence gaps exist for some controls, particularly in information classification and labelling, intellectual property rights compliance, documented operating procedures, and physical security monitoring.

- Remote working policies lack detailed security controls and guidelines.

- Supporting utilities controls (e.g., power, HVAC) are not sufficiently documented.

- Data masking policies beyond testing environments are not formally documented.

- Redundancy of information processing facilities lacks explicit documented controls.

- Protection of information systems during audit testing is not addressed.

- Equipment siting and protection controls need formal definition and documentation.

- Cabling security and environmental threat protections require documented controls.

2.2.3 Non-conformities identified:

• Lack of documented evidence for information classification and labelling controls (A.5.12, A.5.13).

• Absence of formal procedures and evidence for intellectual property rights compliance (A.5.32).

• Missing documented operating procedures covering incident management, change management, backup, and recovery (A.5.37).

• No explicit policy or procedures for protection of information systems during audit testing (A.8.34).

• Insufficient documentation of physical security monitoring such as CCTV or intrusion detection (A.7.4).

• Lack of documented controls for cabling security (A.7.12) and environmental threat protection (A.7.5).

• No formal data masking policy beyond testing environments (A.8.11).

2.2.4 Opportunities for improvement:

• Develop and provide documented evidence of information classification and labelling schemes, including asset owner responsibilities.

• Formalize and document intellectual property rights compliance procedures and maintain evidence.

• Create and maintain documented operating procedures for key ISMS processes such as incident management, change management, backup, and recovery.

• Establish and document controls for physical security monitoring, including CCTV and access logging.

• Enhance remote working policies with detailed security controls, secure access methods, endpoint security, and monitoring.

• Document controls for supporting utilities to ensure availability and security.

• Define and document equipment siting and protection measures to prevent damage and unauthorized access.

• Develop a formal data masking policy covering all relevant environments beyond testing.

• Document redundancy and failover mechanisms explicitly for critical information processing facilities.

• Implement procedures to protect information systems during audit testing activities.

• Provide explicit evidence of NDA signings and approval records for external service providers.

• Include documented emergency access procedures and compensating controls where segregation of duties is difficult.

• Provide documented cabling security controls aligned with regulations.

• Include documented clear desk and screen policies.

• Provide documented equipment maintenance procedures and records.

• Include documented approval processes for privileged utility programs.