

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 the organization demonstrates a strong commitment to information security, with comprehensive policies and procedures aligned to ISO/IEC 27001:2022 requirements. Most controls are well implemented, supported by documented evidence and regular management reviews. The organization maintains effective incident management, access control, supplier management, and physical security measures. Training and awareness programs are robust, and continuous improvement processes are in place.

However, some areas require enhancement to fully meet the standard's expectations and strengthen the ISMS.

2.2.1 Highlights

Strong Information Security Policy framework with director approval and annual reviews.

Comprehensive access control and identity management with formal user registration and de-registration.

Effective incident management including detection, response, and learning processes supported by CAPA documentation.

Robust supplier relationship management with contracts, SLAs, and security requirements.

Well-defined physical security controls including access restrictions and secure disposal of assets.

Documented backup and business continuity plans with recovery objectives and resource planning.

Secure software development lifecycle with code reviews, testing, and secure coding practices.

Regular internal and external audits with management oversight and corrective actions.

2.2.2 Findings

Some documented policies and procedures lack explicit evidence or formal documentation, particularly in:

Information classification and labelling schemes – no direct evidence of classification activities or labelling guidelines.

Intellectual property rights compliance – absence of documented procedures and evidence.

Documented operating procedures – no explicit evidence covering incident management, change management, backup, and recovery.

Physical security monitoring – lack of documented CCTV or intrusion detection systems.

Equipment maintenance – no documented maintenance procedures or records.

Data masking – no formal policy beyond testing environments.

Protection of information systems during audit testing – no documented controls or procedures.

Supporting utilities – lack of detailed controls for power, HVAC, and other critical infrastructure.

Cabling security – no documented controls found.

Remote working – remote access policies exist but lack comprehensive security controls and guidelines.

Redundancy of information processing facilities – implied but not explicitly documented.

Contact with authorities – procedures exist but explicit documented contact lists or procedures are recommended.

Segregation of duties – compensating controls such as monitoring or audit trails should be documented where segregation is difficult.

2.2.3 Non-conformities identified:

Information classification and labelling (A.5.12, A.5.13): Lack of documented classification scheme and labelling guidelines.

Intellectual property rights (A.5.32): No documented procedures or evidence of compliance.