



ISO 27001:2022 Gap Analyse

1. Scope of the GAP

1.1 Applicability

This internal audit covers the Information Security Management System (ISMS) of **Vlectra** 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 **Vlectra**.

Participants:

- On behalf of Vlectra
- [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 **Vlectra** 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:

- Vlectra

2. Executive Summary



2.1 Sampling Methodology

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 Vlectra demonstrates a strong commitment to information security with comprehensive policies and procedures aligned to ISO/IEC 27001:2022. Most controls are well implemented with documented evidence and active management review processes. However, some gaps remain in documentation completeness and formalization of certain controls.

2.2.1 Highlights

-  Comprehensive Information Security Policy covering scope, objectives, roles, responsibilities, and management review.
-  Effective access control and identity management with centralized password management and multi-factor authentication.

- ✓ Strong incident management processes including reporting, response, and learning with CAPA forms and regular ISSC briefings.
- ✓ Well-defined supplier relationship management with contracts, SLAs, risk assessments, and NDAs.
- ✓ Regular security awareness training with 100% completion and ongoing communication.
- ✓ Business Continuity and Disaster Recovery plans with tested recovery procedures and crisis management.
- ✓ Secure development lifecycle with documented SDLC, code reviews, and annual PEN-tests.

2.2.2 Findings

- Several controls lack direct documented evidence despite policy statements, including information classification, labelling, information transfer controls, and IT asset inventory.
- Physical security controls such as perimeter security, monitoring (CCTV), and equipment maintenance are not fully documented or evidenced.
- Some technological controls like data masking, data leakage prevention, redundancy of processing facilities, and protection during audit testing require formal documentation and implementation.
- Remote working policy is partially covered but lacks a comprehensive documented policy addressing all aspects of secure remote access and device management.
- Contact with authorities and special interest groups is managed informally; formalized contacts and participation could be improved.

2.2.3 Non-conformities identified

- ✗ No documented information classification scheme and periodic review evidence.
- ✗ Lack of documented labelling guidelines and evidence of labelling per classification.
- ✗ Missing documented controls for information transfer including approval and protection measures.
- ✗ No documented IT asset inventory or evidence of periodic physical asset checks.
- ✗ Physical security perimeter and monitoring controls lack documented evidence and formal procedures.
- ✗ No formal documented equipment maintenance policy covering all IT and physical equipment.

- ✗ No formal documented remote working policy covering secure access, user responsibilities, and monitoring.
- ✗ No documented procedures for protection of information systems during audit and penetration testing.
- ✗ Lack of documented data masking and data leakage prevention technical controls.
- ✗ No explicit documented redundancy mechanisms for information processing facilities.
- ✗ Intellectual property rights compliance procedures not documented.
- ✗ Documented operating procedures including incident management, change management, backup, and recovery are missing.

2.2.4 Opportunities for improvement

- Develop and document a comprehensive information classification and labelling scheme with periodic reviews.
- Formalize and document controls for information transfer including approval processes and protection measures.
- Establish and maintain a documented IT asset inventory with regular physical verification.
- Enhance physical security controls by documenting perimeter security, monitoring (CCTV), and equipment maintenance policies.
- Create a detailed remote working policy addressing secure access, device management, user responsibilities, and monitoring.
- Document procedures to protect information systems during audit and penetration testing to prevent disruption or data exposure.
- Implement and document technical data masking and data leakage prevention controls.
- Document and implement redundancy controls for critical information processing facilities to ensure availability.
- Maintain documented procedures for intellectual property rights compliance and software licensing.
- Document and maintain comprehensive operating procedures covering incident management, change management, backup, and recovery.
- Formalize contact points with authorities and participation in special interest groups or industry forums.

- Include explicit references or attachments of key policy documents in management review or ISMS repositories for clarity and audit readiness.