ISO 27001:2022 Gap Analyse

1. Scope of the GAP

1.1 Applicability

This internal audit covers the Information Security Management System (ISMS) of **consultancy** 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 **2025-07-09**, focusing on the management system in place at **consultancy**.

Participants:

- On behalf of consultancy
  - zeeshan
- 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 **consultancy** 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:

- consultancy

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 consultancy demonstrates a strong foundation with comprehensive policies and procedures aligned to ISO 27001:2022 requirements. Many controls are well documented and supported by evidence from management review meetings and policy documents. However, some areas lack explicit documented evidence or formalized procedures, indicating opportunities for further strengthening the ISMS.

2.2.1 Highlights

- ✔ Information Security Policy is well defined and communicated.
- ✔ Incident management and response procedures are established and documented.

- ✔ Access control and identity management policies are implemented with supporting evidence.
- ✔ Supplier relationships and contracts include information security requirements and are actively managed.
- ✔ Business Continuity and Disaster Recovery Plans are in place and tested.
- ✔ Security awareness training is conducted with full completion rates.
- ✔ Logging, monitoring, and patch management processes are documented and operational.

2.2.2 Findings

While many controls are effectively implemented, the audit identified several areas where documentation or evidence is incomplete or missing. Some policies exist but lack direct supporting evidence of implementation. Additionally, a few controls require formalization or enhancement to meet best practice standards fully.

2.2.3 Non-conformities identified:

- ✘ No documented evidence of acceptable use policies and enforcement.
- ✘ Lack of documented information classification and labelling procedures with supporting evidence.
- ✘ No explicit documented process for monitoring and managing cloud services security.
- ✘ Missing documented remote working policy covering security controls and user responsibilities.
- ✘ No documented controls or evidence for data masking and anonymization in testing environments.
- ✘ Absence of documented policies for protection of information systems during audit testing.
- ✘ No explicit documented policies for cabling security, network services security, and privileged utility program approvals.
- ✘ Lack of documented controls for physical security monitoring such as CCTV or intrusion detection.
- ✘ Missing documented controls for supporting utilities (power, HVAC, water) to ensure availability and protection.
- ✘ No explicit documented terms and conditions of employment embedding information security responsibilities.

- ✘ No documented evidence of screening and background verification processes.
- ✘ No documented evidence of subscriptions or contacts with special interest groups for security news.
- ✘ No documented evidence of secure development lifecycle (SDLC) policies and application security requirements implementation.
- ✘ No explicit documented secure systems architecture and engineering principles.
- ✘ No explicit documented policies or evidence for web filtering or URL filtering.
- ✘ No explicit documented cryptography controls evidence despite policy statements.
- ✘ No documented evidence of capacity management processes.
- ✘ No explicit documented policies for security of network services.
- ✘ No explicit documented policies or evidence for source code access controls and segregation.
- ✘ No explicit documented policies or evidence for secure coding practices and code reviews.
- ✘ No explicit documented policies or evidence for separation of development, test, and production environments with data masking.
- ✘ No explicit documented policies or evidence for equipment siting and protection against environmental risks.
- ✘ No explicit documented policies or evidence for off-premises asset security and mobile device protection.
- ✘ No explicit documented contact details or procedures for engaging with local authorities in incident response plans.

2.2.4 Opportunities for improvement:

> - Develop and document a comprehensive acceptable use policy with enforcement evidence.
> - Formalize and provide evidence for information classification and labelling procedures.
> - Establish documented cloud services security controls and approval processes with supporting evidence.
> - Create a detailed remote working policy addressing security controls, secure access, and user responsibilities.
> - Implement data masking and anonymization policies for testing and development environments.

- Develop policies and procedures to protect information systems during audit testing.
- Document and implement physical security monitoring controls such as CCTV and intrusion detection.
- Document controls for supporting utilities to ensure availability and protection of information processing facilities.
- Include explicit clauses on information security responsibilities in employment contracts and terms.
- Document and provide evidence of screening and background verification processes.
- Maintain and document subscriptions or contacts with special interest groups and external security information sources.
- Document and provide evidence of secure development lifecycle and application security requirements.
- Develop and document secure systems architecture and engineering principles.
- Implement and document web filtering and URL filtering controls.
- Provide documented evidence of cryptography controls in use.
- Document and provide evidence of capacity management processes.
- Develop and document policies for security of network services including service hardening and monitoring.
- Document and provide evidence of source code access controls and segregation of duties.
- Document and provide evidence of secure coding practices and code reviews.
- Document and provide evidence of separation of development, test, and production environments with data masking.
- Develop and document equipment siting and protection controls addressing environmental and physical risks.
- Document and provide evidence of off-premises asset security and mobile device protection.
- Document and provide contact details and procedures for local authorities in incident response plans.
- Define and document formal procedures and schedules for monitoring, reviewing, and managing changes in supplier services.

- Establish and document a formal process for capturing lessons learned from incidents and integrating improvements into ISMS.
- Include explicit documentation of management responsibilities and enforcement processes.
- Provide explicit documentation or examples of compensating controls where segregation of duties is not possible.
- Provide more detailed evidence of user registration, privileged access management, and session controls.
- Provide more explicit evidence of timely de-registration and controls on shared or anonymous IDs.
- Provide more explicit evidence of formal authorization and revocation processes for access rights.
- Provide more explicit evidence of formal threat intelligence acquisition and dissemination processes.
- Provide explicit evidence of periodic inventory updates including physical location and assigned users.
- Provide explicit evidence of logging all access and restrictions on sensitive data in logs.
- Document and provide evidence of privileged utility program controls and approval processes.