ISO 27001:2022 Gap Analyse

1. Scope of the GAP

1.1 Applicability

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

Participants:

- On behalf of Zeeshan
  - Shaharyar
  - Hasaan
- 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 Zeeshan 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:

- Zeeshan

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 Zeeshan demonstrates a strong alignment with ISO/IEC 27001:2022 requirements, with comprehensive policies and procedures established across organizational, people, physical, and technological controls. Management commitment is evident through regular reviews, defined roles and responsibilities, and documented evidence of policy implementation. However, some areas require further documentation and formalization to fully close identified gaps.

2.2.1 Highlights

- ✔ Well-defined Information Security Policy covering scope, enforcement, roles, and management commitment.

- ✔ Effective access control and identity management processes with documented user registration and periodic reviews.
- ✔ Comprehensive incident management procedures including response, assessment, and learning from incidents.
- ✔ Strong backup and disaster recovery planning with successful restore tests documented.
- ✔ Regular internal and external audits with management reviews and security awareness training.
- ✔ Supplier relationships managed with contracts, SLAs, and risk assessments.
- ✔ Physical security controls including access restrictions, key management, and secure disposal of equipment.
- ✔ Network security maintained with firewalls, encryption, logging, and monitoring.

2.2.2 Findings

While the ISMS is largely compliant, several controls lack explicit documented procedures or evidence, which may impact audit confidence. Some policies are implied or partially documented but require formalization. The following areas were noted:

- Information labelling procedures are not explicitly documented or evidenced.
- Intellectual property rights compliance procedures are missing.
- Integration of information security in project management and SDLC lacks explicit documentation.
- Data masking and data leakage prevention controls are not established.
- Controls for privileged utility programs and access to source code need formal documentation.
- Physical security monitoring such as CCTV or intrusion detection is not documented.
- Supporting utilities controls (e.g., HVAC, fire suppression) require development and documentation.
- Remote working policy is implied but not formally documented.
- Equipment siting and off-premises asset security controls need formalization.
- Protection of information systems during audit testing is not explicitly addressed.

2.2.3 Non-conformities identified:

- ✘ Lack of documented procedures for information labelling and handling.
- ✘ No formal intellectual property rights compliance procedures.
- ✘ Missing documented integration of information security in project management and SDLC.
- ✘ Absence of data masking and data leakage prevention policies.
- ✘ No documented controls for privileged utility programs and source code access.
- ✘ Physical security monitoring (e.g., CCTV) not implemented or documented.
- ✘ Supporting utilities controls are not comprehensively documented.
- ✘ Formal remote working policy is missing.
- ✘ Equipment siting and off-premises asset security controls are insufficiently documented.
- ✘ No explicit procedures protecting information systems during audit testing.

2.2.4 Opportunities for improvement:

- Develop and document formal procedures for information labelling and handling aligned with classification schemes.
- Create and implement intellectual property rights compliance policies and maintain related inventories.
- Document integration of information security requirements within project management and SDLC processes.
- Establish data masking and data leakage prevention controls to protect sensitive information.
- Formalize controls and approval processes for privileged utility programs and secure source code access.
- Implement physical security monitoring such as CCTV or intrusion detection systems and document these controls.
- Develop comprehensive controls for supporting utilities to ensure availability and protection of IT infrastructure.
- Formally document a remote working policy covering security controls, user responsibilities, and technical safeguards.
- Enhance equipment siting and off-premises asset security controls with documented procedures.
- Develop procedures to protect information systems during audit testing to prevent disruption or unauthorized access.