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 [date-of-report], 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 commitment to information security with comprehensive policies and procedures aligned to ISO/IEC 27001:2022. Many controls are well documented and implemented, supported by management reviews and evidence of ongoing monitoring. However, some areas lack documented evidence or formal procedures, indicating opportunities for further strengthening the ISMS.

2.2.1 Highlights

- ✔ Comprehensive Information Security Policy covering scope, responsibilities, enforcement, and management commitment.

- ✔ Effective incident management procedures with monthly ISSC briefings and CAPA forms usage.
- ✔ Strong password and authentication policies including two-factor authentication and complexity requirements.
- ✔ Well-defined roles and responsibilities for information security across the organization.
- ✔ Documented backup and restoration policies with successful restore tests.
- ✔ Supplier relationship management with contracts, SLAs, and risk assessments in place.
- ✔ Secure disposal and handling of information storage media and equipment.
- ✔ Documented change management and secure development lifecycle policies.

2.2.2 Findings

While many controls are implemented effectively, the audit identified several areas where documented evidence or formal procedures are missing or incomplete. These gaps may impact the full assurance of compliance and effectiveness of the ISMS.

2.2.3 Non-conformities identified:

- ✖ Lack of documented evidence for Acceptable Use Policy enforcement and disciplinary actions.
- ✖ Missing formal documented procedures and evidence for Information Classification, Labelling, and Information Transfer controls.
- ✖ No documented Identity Management procedures including user registration and de-registration.
- ✖ Absence of documented NDAs or confidentiality agreements for external providers and employees.
- ✖ No documented remote working and mobile device policies or evidence of enforcement.
- ✖ Missing documented physical security perimeter controls such as card swipe, alarm systems, visitor management, and CCTV monitoring.
- ✖ Lack of documented network security controls including firewalls, segregation of networks, and remote access approvals.
- ✖ No formal documented data masking policy or procedures for test environments.
- ✖ Missing documented malware protection controls and evidence of implementation.

- ✕ No documented approval and control procedures for privileged utility programs and software installation.
- ✕ Lack of documented equipment maintenance policy covering all company equipment.
- ✕ No explicit documented procedures for contact with authorities in case of incidents.
- ✕ Missing documented procedures for cloud service approval and review.
- ✕ No documented procedures for protecting information systems during audit and penetration testing.
- ✕ Lack of documented capacity management process and formal capacity planning policy.
- ✕ Missing documented network service security and web filtering controls.
- ✕ No explicit documented cryptography usage and testing evidence.
- ✕ No documented access controls for source code repositories.
- ✕ Missing documented off-premises asset security policies.

2.2.4 Opportunities for improvement:

- Develop and document formal Acceptable Use Policies with enforcement evidence.
- Establish and maintain documented procedures for Information Classification, Labelling, and Information Transfer with supporting evidence.
- Implement formal Identity Management processes including user registration and de-registration documentation.
- Provide documented NDAs and confidentiality agreements for all external providers and employees.
- Document and enforce remote working and mobile device policies.
- Enhance physical security controls by documenting perimeter security, visitor management, and implementing CCTV or continuous monitoring.
- Document and implement comprehensive network security controls including firewalls, segregation, remote access, and web filtering.
- Develop and implement a formal data masking policy for test and development environments.
- Document malware protection controls and provide evidence of their implementation.

- Establish approval and control procedures for privileged utility programs and software installation.
- Create a formal equipment maintenance policy covering all IT and physical equipment with schedules and responsibilities.
- Document procedures for contact with authorities in case of incidents such as data leakage or disasters.
- Formalize cloud service approval and periodic review procedures with evidence.
- Develop explicit procedures to protect information systems during audit and penetration testing.
- Implement a formal capacity management process including monitoring, forecasting, and resource planning.
- Document security controls for network services and implement web filtering technologies.
- Document cryptography usage policies and evidence of regular testing.
- Provide documented access controls for source code repositories.
- Document off-premises asset security policies including encryption and handling.