ISO 27001:2022 Gap Analyse

1. Scope of the GAP

1.1 Applicability

This internal audit covers the Information Security Management System (ISMS) of **topcity** 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 **2025-07-14**, focusing on the management system in place at **topcity**.

Participants:

- On behalf of topcity:
  - zeeshan
  - ali
- On behalf of supporting company alpha:
  - jj
  - kk
- 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 **topcity** in accordance with ISO/IEC 27001:2022 requirements.

1.5 Scope of Entities Included in the Internal Audit

- topcity
- alpha (supporting entity)

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 topcity demonstrates a comprehensive set of documented policies and procedures aligned with ISO/IEC 27001:2022 requirements. Most organizational, people, physical, and technological controls are defined and implemented with clear responsibilities and processes. However, evidence of implementation is often incomplete or missing, and some areas require further formalization and documentation.

2.2.1 Highlights

- Policies and procedures are well documented across organizational, people, physical, and technological controls.
- Access control and identity management policies are defined with formal user registration, de-registration, and multi-factor authentication.
- Incident management procedures cover detection, reporting, analysis, and response.
- Secure development lifecycle and application security requirements are established.
- Network security and cryptography controls are in place with firewall rules, encryption, and monitoring.
- Physical security measures include controlled access, locked server racks, and visitor escorting.
- Information classification and labeling schemes are defined and applied.
- Supplier relationships are governed by contracts and SLAs with security clauses.
- Information security roles and responsibilities are clearly assigned.
- Awareness and training efforts are initiated with welcome letters and password guidance.

2.2.2 Findings

- Many controls have documented policies but lack explicit or sufficient evidence of implementation.
- Some critical areas such as information security during disruptions, ICT readiness for business continuity, and remote working policies are not fully developed or documented.
- Physical security monitoring (e.g., CCTV) and equipment maintenance procedures require formalization.
- Data leakage prevention lacks explicit technical controls or tools.
- Capacity management processes are not clearly documented.
- Secure systems architecture and engineering principles are not formally documented beyond Unix hardening.
- Protection of information systems during audit testing is not explicitly addressed.
- Incident reporting procedures and disciplinary enforcement could be more explicitly linked to evidence.
- Some password policy enforcement details need clarification, such as special character requirements and account unlock timing.

2.2.3 Non-conformities identified:

- Information security during disruption (A.5.29): No explicit documented controls or procedures specifically addressing information security during disruptions such as disaster recovery or incident-induced outages.
- ICT readiness for business continuity (A.5.30): Lack of explicit ICT readiness measures such as redundancy, failover, or recovery time objectives documented.

- Remote working (A.6.7): No comprehensive remote working policy covering secure home environment, user responsibilities, or remote access controls beyond device and network access.
- Physical security monitoring (A.7.4): No explicit mention of CCTV or continuous monitoring systems.
- Supporting utilities (A.7.11): No comprehensive policy on power, cooling, or other utilities for critical facilities.
- Equipment maintenance (A.7.13): No detailed documented procedures or responsibilities for equipment maintenance.
- Data leakage prevention (A.8.12): No explicit technical controls or tools for data leakage prevention described.
- Redundancy of information processing facilities (A.8.14): No detailed redundancy strategies or infrastructure redundancy controls described.
- Secure systems architecture and engineering principles (A.8.27): No formal documented principles beyond Unix hardening.
- Protection of information systems during audit testing (A.8.34): No explicit documented procedures or controls for protecting systems during audit testing.
- Capacity management (A.8.6): No formal capacity management process or tools documented.

2.2.4 Opportunities for improvement:

- Develop and document specific information security controls and procedures for business continuity and disruption scenarios, including roles, communication, and recovery priorities.
- Enhance ICT readiness by defining infrastructure resilience, redundancy, failover mechanisms, and recovery time objectives.
- Create a comprehensive remote working policy addressing secure remote environments, user responsibilities, secure connections, and monitoring.
- Implement physical security monitoring measures such as CCTV or intrusion detection systems and document their management.
- Establish documented procedures for supporting utilities management to ensure availability and protection of information assets.
- Formalize equipment maintenance procedures covering all IT assets with schedules, responsibilities, and verification.
- Introduce and document technical data leakage prevention controls, including DLP tools, monitoring, and enforcement mechanisms.
- Define and document redundancy strategies for critical information processing facilities to ensure availability and resilience.
- Develop formal secure systems architecture and engineering principles covering all platforms and system types.
- Document controls and procedures to protect information systems during audit testing to prevent disruption or data compromise.
- Establish formal capacity management processes including monitoring, forecasting, and resource planning.
- Improve evidence collection and documentation for enforcement of password policies, disciplinary processes, and incident reporting channels.
- Strengthen ongoing information security awareness, education, and training programs with formalized schedules and content.