

{\rtf1\ansi\deff0  
{\fonttbl{\f0\fswiss\fcharset0 Arial;}}  
{\colortbl ;\red0\green128\blue0;\red255\green0\blue0;}  
\viewkind4\uc1\pard\sa200\sl276\slmult1\f0\fs24\b ISO 27001:2022 Gap Analyse\par  
This report outlines the current status of the ISO 27001:2022 GAP analyse and identifies relevant gaps.\par  
It has been fully automated and generated using AI support. Please note that, while efforts have been made to ensure accuracy, AI-generated outputs may contain errors, just like human-generated reports. All findings should be validated as part of the internal review process.\par  
  
\b0 1. Scope of the GAP\par  
1.1 Applicability\par  
This internal audit covers the Information Security Management System (ISMS) of \b [company-name] \b0 as defined under the scope of its ISO/IEC 27001:2022 certification, in accordance with the internal audit planning for that standard.\par  
  
1.2 Participants in the Audit\par  
The internal audit was conducted on \b [date-of-report] \b0 , focusing on the management system in place at \b [company-name] \b0 .\par  
Participants:\par  
On behalf of \b [company-name]\b0 \par  
[name-1]\par  
[name-2]\par  
[name-3]\par  
On behalf of Valecta\par  
Stephan Csorba\par  
  
1.3 Audit Criteria\par  
The audit was carried out in accordance with the ISO/IEC 27001:2022 standard by Valecta.\par  
  
1.4 Audit Objectives\par  
The purpose of this GAP-analyse was to assess, on a sample basis, the functioning and effectiveness of the ISMS as implemented at \b [company-name] \b0 in accordance with ISO/IEC 27001:2022 requirements.\par  
  
1.5 Scope of Entities Included in the Internal Audit\par  
This internal audit included the following legal entities:\par  
[company-name-1]\par  
[company-name-2]\par  
  
\b 2. Executive Summary\par  
\b0 2.1 Sampling Methodology\par  
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.\par  
  
2.2 General Impressions of the Management System\par  
The ISMS at \b [company-name] \b0 demonstrates a mature and comprehensive implementation of ISO/IEC 27001:2022 controls, with well-defined policies, procedures, and evidence supporting most organizational, people, physical, and technological controls. Management commitment is evident through regular reviews, training, and incident management processes. The organization has established strong supplier management, access control, incident response, and business continuity planning.\par  
However, some areas require enhancement to fully meet the standard’s expectations and to strengthen the ISMS effectiveness.\par  
  
2.2.1 Highlights\par  
- Information Security Policy is approved by management and reviewed annually.\par  
- Clear definition of roles and responsibilities across the organization.\par  
- Effective access control and identity management with documented user registration and de-registration.\par  
- Comprehensive incident management including detection, response, learning, and evidence collection.\par  
- Strong supplier relationship management with contracts, SLAs, and risk assessments.\par  
- Robust backup, logging, network security, and cryptography controls implemented.\par  
- Documented secure development lifecycle and change management processes.\par  
- Regular security awareness training with 100% completion rate.\par  
- Business Continuity Plan covers incident management, recovery, and crisis communication.\par  
  
2.2.2 Findings\par  
- Some documented evidence is missing or incomplete for certain controls, particularly in information classification, labelling, and intellectual property rights compliance.\par  
- Remote working policies lack detailed security controls and formal documentation.\par  
- Physical security monitoring (e.g., CCTV, intrusion detection) is not explicitly documented.\par  
- Controls for supporting utilities (power, HVAC) and environmental threat protections are insufficiently detailed.\par  
- Data masking policies beyond testing environments are not formally documented.\par  
- Procedures for protection of information systems during audit testing are absent.\par  
- Equipment siting and protection controls need formal definition and documentation.\par  
- Cabling security controls lack explicit evidence and documentation.\par  
- Some evidence recommendations suggest inclusion of explicit approval records, documented procedures, and formal role matrices.\par  
  
2.2.3 Non-conformities identified:\par  
{\cf2  
- Lack of documented information classification scheme and evidence of asset owner classification activities (A.5.12).\par  
- Absence of documented labelling guidelines and evidence of application (A.5.13).\par  
- No explicit documented procedures ensuring compliance with intellectual property rights and software licensing (A.5.32).\par  
- Missing documented operating procedures covering incident management, change management, backup, recovery, and other operational controls (A.5.37).\par  
- No formal data masking policy covering all relevant environments beyond testing (A.8.11).\par  
- Lack of documented controls or procedures to protect information systems during audit testing (A.8.34).\par  
- No explicit documented cabling security controls per regulations (A.7.12).\par  
- No detailed physical and environmental threat protection controls (A.7.5).\par  
- Missing documented equipment maintenance procedures and records (A.7.13).\par  
}\cf0  
  
2.2.4 Opportunities for improvement:\par  
- Develop and document a formal information classification and labelling scheme with evidence of implementation.\par  
- Establish and maintain documented procedures for intellectual property rights compliance.\par  
- Create and maintain documented operating procedures for key ISMS operational activities.\par  
- Formalize and document comprehensive remote working and mobile device security policies.\par  
- Implement physical security monitoring controls such as CCTV, access logs, and intrusion detection systems.\par  
- Define and document controls for supporting utilities and environmental safeguards.\par  
- Develop and document a formal data masking policy applicable beyond testing environments.\par  
- Establish procedures to protect information systems during audit testing activities.\par  
- Provide documented cabling security controls aligned with applicable regulations.\par  
- Define and document equipment siting and protection measures.\par  
- Maintain documented equipment maintenance schedules and records.\par  
- Enhance evidence collection by including explicit approval records, formal role and responsibility matrices, and documented review outcomes.\par  
  
\par  
}