Cybersecurity Audit Report - ISO 27001 for Alpro N.V.

Audit Date: September 12, 2021
Auditor: Rachid Amar
Company Audited: Alpro N.V. (Belgium)
Reference Standard: ISO/IEC 27001:2013 - Information Security Management System (ISMS)

Summary

1. Introduction

This audit was conducted in accordance with the requirements of the ISO/IEC 27001:2013 standard, with the aim of assessing the conformity of Alpro’s Information Security Management System (ISMS). This report provides details on the activities performed, the controls audited, and the conclusions drawn to ensure that risks related to information security within the company are effectively managed.

2. Scope of the Audit

The audit covered the following areas:

- **Headquarters**: Located in Ghent, Belgium.
- **IT Systems**: Physical and digital IT infrastructure, ERP systems (SAP), corporate networks, and servers.
- **Personnel Involved**: IT department, human resources, operations, and information management.
- **Processes**: Access control, sensitive data protection, incident management, business continuity, and product development security.

3. Audit Objectives

- Determine if Alpro’s ISMS complies with the ISO 27001 standard.
- Assess the effectiveness of the controls implemented to protect information assets.
- Identify areas for improvement and residual risks that may affect information security.
- Verify the correct implementation of established security policies and procedures.

---

4. Audit Methodology

The audit was conducted in three main phases:

1. **Planning and Document Review** A review of the company’s policies, procedures, and controls related to information security was conducted. This included:
    - Information Security Policy
    - Risk assessments
    - Risk treatment plans
    - Access control procedures
    - Incident management manual
2. **Fieldwork and Interviews** Interviews were conducted with key information security personnel, including:
    - Chief Information Security Officer (CISO)
    - Head of IT department
    - Representatives from operations and human resources
3. **Control Testing** In-situ technical and operational control checks were carried out, including vulnerability testing and log review, along with the simulation of incident scenarios.

---

5. Evaluation of Implemented Controls

In accordance with the ISO 27001 standard, the security controls defined in **Annex A** were reviewed. Below is a detailed analysis of the controls evaluated:

5.1. A.5 - Information Security Policies

Control: The organization must establish an information security policy that is approved by management and effectively communicated throughout the organization.

- **Observations**: The information security policy is up to date and has been formally approved by Alpro’s management. However, it was noted that communication of the policy to some employees was insufficient, as some were unaware of its existence during interviews.
- **Recommendations**: Strengthen internal communication campaigns on the security policy, including training sessions for employees at various levels.

5.2. A.6 - Organization of Information Security

Control: Establish a clear organizational structure with well-defined responsibilities for security management.

- **Observations**: The company has appointed a team responsible for the ISMS, with a CISO in charge. Responsibilities are clearly defined and documented. However, no formal security committee has been established to review policies and update emerging risks regularly.
- **Recommendations**: Formalize the creation of a security committee that includes representatives from IT, HR, legal, and operations to ensure periodic reviews and continuous risk management.

5.3. A.7 - Human Resource Security

Control: Controls should be implemented before, during, and after employment to manage employee security risks.

- **Observations**: Background checks are performed for new employees in critical roles. However, it was noted that not all employees receive regular security awareness training.
- **Recommendations**: Implement a mandatory training program for all employees with periodic refreshers and compliance assessments.

5.4. A.9 - Access Control

Control: Policies and procedures should be in place to control access to information and IT systems.

- **Observations**: Alpro has implemented role-based access control (RBAC) with two-factor authentication (2FA) for critical systems. However, in the ERP systems, some employees were found to have more privileges than required for their daily tasks.
- **Recommendations**: Conduct a thorough review of access permissions and adjust them according to the principle of least privilege.

5.5. A.12 - Operations Security

Control: Ensure that security operations are managed securely, including protection against malware and vulnerability management.

- **Observations**: The company has up-to-date antivirus and firewall solutions. However, it was found that not all security updates are applied automatically, leaving some systems vulnerable.
- **Recommendations**: Implement an automated process for managing patches and critical updates, prioritizing systems exposed to the internet.

5.6. A.14 - System Development Security

Control: Security controls should be integrated into software development processes.

- **Observations**: Alpro outsources part of its software development. While external vendors comply with required security standards, no regular security reviews of developed software are conducted.
- **Recommendations**: Establish a protocol for regular security reviews and testing of externally developed code.

6. Risk Management

Risk management is a core component of ISO 27001. During the audit, the process for identifying, analyzing, and treating risks at Alpro was assessed.

- **Observations**: Alpro conducts annual risk assessments, but not all residual risks are clearly documented. Additionally, not all risks are reviewed on a regular basis.
- **Recommendations**: Implement a quarterly risk review process and ensure that residual risks are clearly documented. Also, include incident simulations to prepare the organization for potential attacks.

---

7. Security Incident Review

Alpro has reported several minor incidents related to phishing attempts. No significant breaches have occurred in the last 12 months. However, it was observed that the response times to incidents need improvement.

- **Recommendations**: Improve incident response capabilities through regular drills and specialized training for the incident response team.

---

8. Overall Conclusion

Overall, Alpro has implemented an Information Security Management System that aligns with the ISO/IEC 27001 standard. Adequate policies and procedures are in place in most areas, though improvements were identified in access management, internal communication of policies, and risk management.

---

9. Recommended Corrective Actions

1. Strengthen internal communication and employee training on the security policy.
2. Formalize the creation of a security committee.
3. Review and adjust employee access permissions according to the least privilege principle.
4. Implement an automated process for security updates.
5. Establish regular security reviews for externally developed software.

Auditor: Rachid Amar
Date: September 12, 2021