Internal Audit Summary Report – ISMS

Audit Type: Internal self-assessment

Audit Period: 15–17 May 2026

Scope: ISMS documentation and controls

Standard: ISO/IEC 27001:2022

Methodology

The internal audit was conducted through a structured review of documented ISMS artefacts and selected operational practices. The audit methodology consisted of document review and walkthrough sessions to verify alignment with ISO/IEC 27001:2022 requirements and organizational risk management objectives.

Summary of Results

- Conformities identified: 4
- Nonconformities identified: 1
- Opportunities for Improvement (OFIs): 2

Key Findings

- Vendor risk assessment process is not formally documented (Finding ID: F-02).
- Risk Treatment Plan (RTP) requires defined management approval and sign-off fields to ensure accountability (Finding ID: F-01).
- Incident response drills have not yet been conducted or documented, limiting preparedness testing (Finding ID: F-03).

Conclusion

Based on the results of the internal audit, the Information Security Management System (ISMS) is assessed as partially conformant with the requirements of ISO/IEC 27001:2022. While core ISMS processes and documentation are in place, identified nonconformities and opportunities for improvement indicate the need for further strengthening of vendor risk management, formal approval mechanisms for risk treatment, and practical testing of incident response capabilities. Corrective and preventive actions have been defined and are being tracked through the Corrective Action Plan (CAPA) register to support continual improvement of the ISMS.

Prepared by: Self (Portfolio Internal Review)

Date: 17-May-2026