Internal Audit Report

Organization	Technet	Revision	1.0
Auditor	Vaishnavi Deshpande	Audit Date	10-06-2025

Scope	Entire ISMS covering IT systems, development, support and policy implementation
Reference Standard	ISO /IEC 27001:2022

Table of Contents

---

1. Audit Objectives

- Evaluate compliance with ISO 27001 controls and policies.
- Identify gaps in ISMS implementation.
- Assess the effectiveness of risk treatment and control application.1

2. Audit Summary Table

Audit Area	Clause / Control	Findings	Compliant (Y/N)	Remarks
ISMS Context & Scope	4.1 - 4.3	Scope defined, Context analysis yet to be completed	Partial	Annual review recommended
Leadership & Policy	5.1 - 5.3	Policy approved, communicated via email	Yes	Awareness could be improved
Risk Management	6.1.2 - 6.1.3	RA and RTP documented, SoA filled.	Yes	Periodic review recommended
Support & Resources	7.2 - 7.4	Awareness session held, dev team not trained. Centralized document control in progress.	Partial	Conduct developer specific training and centralize policy storage.
Operational Controls	A 5.17 , A5.18	Role based access control implemented on critical systems.	Yes	Password policy reviewed
	A 8.11	Laptops partially encrypted	No	Complete rollout and verify
	A 6.4	Phishing simulations conducted, spam filtering established	Yes	Conduct simulation quarterly.
Incident Management	A 5.24	Process documented, no recent incidents	Yes	Simulate test incident annually
Business Continuity	A 5.30 - A 5.33	BCP Documented	Yes	Annual review recommended
Monitoring & Measurement	9.1 - 9.2	Metrics tracked monthly. Management reviews evidence present.	Yes	Establish a monthly review of the performance metrics.
Internal Audit	9.2	This report is the first internal audit	Yes	Establish audit cycle (biannual)

Management review	9.3	Held in April 2025	Yes	Establish review quartely
Continual Improvement	10.1 - 10.2	CAPA Tracker exists but no tracking of closure dates.	Partial	Finalize closure dates

3. Nonconformities / Observations

Finding Type	Clause / Control	Description	Recommended action
Nonconformity	4.2	Context analysis yet to be completed	Schedule and document context analysis
Observation	7.2 - 7.4	Developer training not yet conducted	Schedule targeted security training
Nonconformity	A 8.11	Device encryption not enforced for all endpoints	Implement full disk encryption and track
Nonconformity	10.1 - 10.2	CAPA Tracker exists but no tracking of closure dates.	Finalize and track closure dates

4. Conclusion

The ISMS implementation is progressing well with a strong foundation in scope, risk and policy areas. However, there are **gaps in encryption, training and documentation** that needs to be addressed to move toward full compliance. A follow up internal audit is recommended in **December 2025.**

Sign Off

Auditor: Vaishnavi Deshpande

Date: 10 June 2025