Internal Audit Checklist – ISO/IEC 27001:2022

This Internal Audit Checklist is designed to support the evaluation of the Information Security Management System (ISMS) in accordance with ISO/IEC 27001:2022. It helps verify whether required controls, processes, and documentation are properly implemented, maintained, and aligned with organizational objectives and regulatory requirements.

Audit Checklist Items:

- ISMS scope is formally defined, documented, approved by management, and communicated to relevant stakeholders.
- A comprehensive risk assessment has been conducted, including identification of assets, threats, vulnerabilities, and risk evaluation criteria.
- Risk treatment plan has been developed and implemented, with responsibilities assigned and progress tracked.
- Statement of Applicability (SoA) has been prepared, approved, and includes justification for inclusion or exclusion of Annex A controls.
- Information security policies are documented, approved, version-controlled, and communicated to employees and relevant third parties.
- Access controls are implemented using role-based access control (RBAC), authentication mechanisms, and periodic access reviews.
- An incident response process is defined, including reporting, investigation, escalation, and lessons learned procedures.
- Vendor and third-party risk management processes are implemented, including due diligence, contractual security clauses, and periodic reviews.
- A business continuity plan (BCP) and disaster recovery plan (DRP) are established, tested periodically, and aligned with business impact analysis.
- Management review meetings are conducted at planned intervals to assess ISMS performance, risks, audit results, and improvement actions.