ISO 27001 GAP ASSESSMENT

INTERNAL AUDIT PLAN

ISO27001 – LEAD AUDITOR

GAP ASSESSMENT

FOR

CloudTech Solutions

Prepared as part of ISO 27001 Lead Auditor Certification Project Portfolio

SUBMITTED BY

Arji Bhandhavi

Rohith Mangaiahgari

EMAIL ID's: arjibhandhavi.ac@gmail.com | sairohithmr@gmail.com

DATE: 07/05/2025

INTRODUCTION

This Internal Audit Plan outlines the framework and schedule for conducting the internal ISMS audit for CloudTech Solutions as part of our ISO/IEC 27001:2022 compliance efforts. The audit is intended to verify that controls identified during the ISO 27001 gap assessment have been implemented effectively and are operating as intended.

OBJECTIVE

The primary objective of this internal audit is to evaluate the effectiveness of implemented ISMS controls, identify nonconformities, and ensure continuous improvement of the information security posture at CloudTech Solutions. The audit also ensures compliance with ISO/IEC 27001:2022 requirements.

SCOPE OF THE AUDIT

The audit covers:

- Organizational departments and functions that manage, process, or protect information assets
- Key areas such as HR, IT, Network Infrastructure, Application Development, and Data Storage
- All ISMS-related activities, policies, and procedures within the defined scope of CloudTech Solutions' ISMS

AUDIT CRITERIA

The internal audit will be conducted against the following criteria:

- ISO/IEC 27001:2022 Standard
- CloudTech Solutions' internal ISMS policies, procedures, and documented information
- Risk treatment plan and previous audit findings (if applicable)
- Legal, regulatory, and contractual obligations relevant to ISMS

AUDIT SCHEDULE

Date	**Area / Function Audited**	**Location**
2025-05-10	Information Security Management	Remote
2025-05-11	HR & Access Control	Remote
2025-05-12	IT Infrastructure & Networking	Remote
2025-05-13	Application Development & Hosting	Remote

AUDIT METHODOLOGY

The internal audit will follow a structured and risk-based approach, involving:

- Review of ISMS documentation and records
- Interviews with key stakeholders and process owners
- Sampling and verification of implemented controls
- Observations of operational practices
- Review of previous audit reports and corrective actions

CONFIDENTIALITY & ETHICS

All information collected during the audit will be treated as confidential and used exclusively for audit purposes. Auditors will uphold integrity, objectivity, and professionalism throughout the audit process.

EXPECTED OUTCOMES

- Confirmation of compliance with ISO/IEC 27001:2022 requirements
- Identification of nonconformities (if any) and opportunities for improvement
- Recommendations to strengthen ISMS effectiveness
- A formal Internal Audit Report to be generated post-audit

****** END ******