ISO 27001 GAP ASSESSMENT

GAP ASSESSMENT REPORT

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: 03/05/2025

Executive Summary

This Gap Assessment Report presents a detailed review of CloudTech Solutions' current information security management posture in alignment with the ISO/IEC 27001:2022 standard. The objective is to identify areas of compliance, partial implementation, and non-conformance, and provide a remediation plan to achieve full compliance with the ISO 27001 framework.

CloudTech Solutions, a global IT services provider specializing in cloud infrastructure and cybersecurity solutions, must meet high information security expectations due to its sensitive clientele, including healthcare and financial institutions. This report serves as a roadmap for closing identified compliance gaps and enhancing the overall effectiveness of the organization’s Information Security Management System (ISMS).

Methodology

2.1 Data Collection

- **Primary Sources**: Simulated interviews with IT staff, review of existing policies, mock assessments of technical systems.
- **Secondary Sources**: ISO 27001:2022 standard, NIST CSF, industry frameworks, and prior internal documentation.

2.2 Gap Analysis Approach

- Used a custom-built **Gap Assessment Checklist** to evaluate clauses 4–10 and Annex A controls.
- Each control was marked as:

- **Compliant** – fully implemented
- **Partially Compliant** – implemented but lacks maturity or consistency
- **Non-Compliant** – not implemented or missing entirely

- Evidence was documented for each clause, along with risk implications and actionable recommendations.

Summary of Findings

Category	**Status Summary**
Clauses 4–10 (Core ISMS)	Partially Compliant
Annex A Controls (Selected)	Mixed (Compliant to Non-Compliant)
Risk Management Framework	In Development
Policy Documentation	Needs Consolidation
Incident Response Mechanisms	Incomplete
Supplier Security Controls	Lacking Formal Oversight

Key Risks Identified:

- Incomplete risk treatment documentation
- Lack of documented supplier agreements
- Weakness in incident detection and response planning

Detailed Gap Analysis

Clause / Control	Current Status	Evidence	Recommendation
Clause 4: Context of the Organization	Partially Compliant	Mission/vision identified, but no documented internal/external issues	Document a Context Analysis and maintain regularly
Clause 5: Leadership	Partially Compliant	No formal InfoSec roles defined	Assign and communicate roles (CISO, ISMS lead)
Clause 6: Planning	Non-Compliant	No formal risk assessment process found	Define a Risk Treatment Methodology
Clause 7: Support	Partially Compliant	Some policies exist, training limited	Establish awareness program and documentation control
Clause 8: Operation	Partially Compliant	Controls implemented but undocumented	Maintain operating procedures and incident logs
Clause 9: Performance Evaluation	Non-Compliant	No audits or review meetings held	Schedule annual ISMS internal audits and reviews
Clause 10: Improvement	Non-Compliant	No corrective actions documented	Create a CAPA (Corrective and Preventive Action) process
Annex A.5: InfoSec Policies	Compliant	Acceptable Use Policy exists	Review annually and assign ownership
Annex A.6: Org of InfoSec	Partially Compliant	Roles unclear, no reporting structure	Create an InfoSec governance structure
Annex A.12: Ops Security	Partially Compliant	No secure backup policy	Develop backup and recovery procedures

Recommendations and Roadmap

Priority	Action Item	Timeline	Owner
High	Conduct a full risk assessment	Month 1	ISMS Lead
High	Develop and document ISMS policies	Month 1–2	Compliance Team
Medium	Establish regular awareness training	Month 2	HR + Security
Medium	Create supplier evaluation policy	Month 3	Procurement
Low	Define improvement KPIs and audit metrics	Month 4	CISO

Compliance Score:

Estimated Readiness: 58% (Based on weighted checklist scoring)

Target Compliance: 100% by 6 months with active remediation

Conclusion

This Gap Assessment is a foundational step in CloudTech Solutions' journey toward ISO 27001 certification. Addressing the highlighted issues will not only align the organization with global security standards but also build stakeholder trust, protect client data, and ensure regulatory compliance.

Continuous review, internal audits, and management commitment will be key to success. Future initiatives should include a formal certification plan, third-party audit preparation, and integration of security into business strategy.