Internal Audit Report for ISO 27001 Compliance Readiness

Prepared for: INFO-7374 Solutions

Team Members:

- **Adish Shah – 002872219**
- **Ashok Kumar Reddy Naguri – 002817769**
- **Krisha Lakhani – 002334794**
- **Devansh Thard – 002687975**

---

1. Introduction

INFO-7374 Solutions is a mid-tier cybersecurity organization that delivers cloud security services tailored to financial institutions. As part of its efforts to strengthen information security and meet regulatory requirements, the company is working towards obtaining ISO 27001:2013 certification for its Information Security Management System (ISMS). This internal audit serves to evaluate INFO-7374's current ISMS implementation, pinpoint areas of non-compliance, and recommend corrective measures prior to the official certification audit.

---

2. Audit Scope and Objectives

2.1 Scope of the Audit

The audit encompasses INFO-7374 Solutions' ISMS processes, systems, and infrastructure, particularly those supporting:

- Cloud-based security services for financial sector clients
- Internal information technology systems
- Data storage and customer transaction platforms
- Authentication mechanisms and access management controls
- Regulatory compliance operations and third-party integrations

2.2 Audit Objectives

- Verify the ISMS framework is aligned with ISO 27001:2013 standards
- Identify and document areas of non-conformance
- Provide actionable recommendations to address any compliance gaps
- Support the organization in achieving ISO 27001 certification readiness

---

3. Audit Methodology

The audit was conducted using a combination of methods to thoroughly evaluate the ISMS:

- Document Analysis: Review of key ISMS documentation, including policies, risk assessments, Statements of Applicability (SoA), incident response plans, and access control procedures
- Stakeholder Interviews: Discussions with system owners, security managers, HR representatives, and other relevant personnel
- Onsite Inspections: Physical security assessments, focusing on access control measures and environmental security
- Data Sampling: Examination of access logs, incident records, and encryption configurations
- Control Testing: Verification of technical controls such as password complexity requirements and user access validation procedures

---

4. ISMS Framework Overview

4.1 Scope of INFO-7374’s ISMS

The organization’s ISMS framework includes:

- Security solutions offered to financial institutions
- Core IT infrastructure and data centers
- Control over employee and third-party access to information assets
- Storage and management of customer financial transactions
- Compliance mechanisms for meeting industry regulations

4.2 Key Information Assets Protected by the ISMS

1. Customer financial transaction data
2. User authentication credentials, including multi-factor authentication (MFA) details
3. Regulatory and compliance reports
4. Cloud security platform and infrastructure components
5. Systems used for employee access management and control

4.3 Major Security Risks Identified

1. Inadequate access controls, increasing the risk of unauthorized system access
2. Data breaches due to the storage of unencrypted customer data
3. Potential regulatory violations arising from incomplete audit documentation and records

---

5. Audit Planning and Documentation Review

5.1 Essential Documents for ISO 27001 Certification Audit

INFO-7374 Solutions must ensure the following documents are prepared and maintained:

1. Information Security Management System (ISMS) Policy
2. Comprehensive Risk Assessment Report
3. Statement of Applicability (SoA)
4. Access Control Policy and Procedures
5. Documented Incident Response Plan

5.2 Sample Audit Checklist

Audit Area	Key Question
ISMS Documentation	Is there an approved ISMS policy?
Risk Management	Have formal risk assessments been completed and documented?
Access Control	Are user access controls in place and documented?

Audit Area	Key Question
Data Security	Is customer data encrypted during transmission and storage?
Incident Handling	Is there a documented and tested incident response plan?

5.3 Audit Goals and Anticipated Outcomes

- Ensure the organization’s security controls meet ISO 27001 requirements
- Detect non-conformities and areas requiring improvement
- Recommend corrective actions to address compliance gaps
- Prepare the organization for the ISO 27001 certification process

6. Internal Audit Findings

6.1 Summary of Non-Conformities

Issue Identified	Category	Explanation
Shared administrative credentials	Major	Shared passwords undermine access control and accountability, increasing the risk of unauthorized access
Absence of documented risk assessments	Major	While risk assessments have been conducted, a lack of formal documentation impedes risk management and auditability
No formalized incident response plan (IRP)	Major	Without a documented IRP, the organization cannot effectively detect, respond to, or recover from security incidents
Lack of encryption for stored customer data	Major	Customer data stored in plaintext increases exposure to data breaches and regulatory non-compliance risks
Insufficient staff awareness of ISMS policies	Minor	Lack of employee training on ISMS policies raises the potential for human error and security incidents

6.2 Applicable ISO 27001 Clauses and Controls

Issue	Relevant Clause / Annex A Control
Shared administrative credentials	Clause 9.4 / Annex A.9.2 (User Access Management)
Absence of documented risk assessments	Clause 6.1.2 / Annex A.8.2 (Information Classification)
No incident response plan	Clause 6.1.3 / Annex A.16.1 (Information Security Incident Management)
Lack of encryption for customer data	Clause 10.1 / Annex A.10.1 (Cryptographic Controls)
Insufficient ISMS awareness training	Clause 7.2 / Annex A.7.2 (Information Security Awareness)

---

7. Corrective and Preventive Action Plan

Non-Conformity	Corrective Actions	Preventive Actions	Responsible Party	Timeline
Shared admin credentials	Eliminate shared accounts, implement Role-Based Access Control (RBAC) and Multi-Factor Authentication (MFA)	Conduct quarterly user access reviews	IT Security Lead	30 Days
Lack of documented risk assessments	Perform and record comprehensive risk assessments; maintain a formal risk register	Conduct annual risk reviews and updates	Risk Manager	45 Days
No incident response plan	Develop, approve, and distribute an Incident Response Plan (IRP)	Test the IRP annually and conduct tabletop exercises	Incident Response Manager	60 Days

Non-Conformity	Corrective Actions	Preventive Actions	Responsible Party	Timeline
No encryption of customer data	Enable AES-256 encryption for all data at rest; implement secure encryption key management practices	Conduct semi-annual encryption audits	Data Protection Officer	30 Days
Lack of ISMS policy training	Launch mandatory ISMS awareness training for all staff	Include security awareness in onboarding and conduct annual refresher sessions	HR & ISMS Manager	30 Days

---

8. Recommendations for Compliance Enhancement

Short-Term (0 to 3 Months)

- Discontinue use of shared administrative accounts; implement RBAC and MFA
- Encrypt all sensitive customer data both in transit and at rest
- Complete and formalize the organization's risk assessment processes and maintain an enterprise risk register

Medium-Term (3 to 6 Months)

- Develop and deploy an Incident Response Plan (IRP); conduct regular testing and drills
- Establish a continuous security awareness training program, including phishing simulations and threat awareness modules

Long-Term (6 to 12 Months)

- Implement a Security Information and Event Management (SIEM) system for real-time monitoring and threat detection
- Automate compliance management through a Governance, Risk, and Compliance (GRC) platform to streamline policy enforcement and audits

---

9. Conclusion

This internal audit has identified significant areas where INFO-7374 Solutions must take corrective action to align its ISMS with ISO 27001:2013 standards. The proposed corrective and preventive actions are essential for mitigating information security risks and ensuring the organization’s readiness for ISO 27001 certification. Timely implementation of these measures will enhance the company’s security posture, improve regulatory compliance, and build trust with stakeholders.