ISO 27001 Compliance Audit

Executive Summary

Confidential - For Internal Use Only

Executive Summary - ISO 27001 Compliance Audit

Table of Contents

1. Introduction

This report provides an executive-level overview of the ISO 27001 compliance audit conducted for [Company Name] on [Date]. The audit focused on evaluating the effectiveness of the Information Security Management System (ISMS), identifying control gaps, and recommending corrective measures in alignment with ISO 27001 requirements.

2. Audit Scope

The audit scope covered information security policies, access control, incident response, risk management, supplier relationships, and business continuity planning. The evaluation was based on ISO 27001:2013 clauses and Annex A controls.

3. Key Findings

1. Access control policies are partially documented but lack enforcement monitoring.
2. Incident response procedures exist but have not been tested in the last 12 months.
3. Supplier risk assessments are performed ad hoc without formal criteria.
4. Data backup encryption is implemented, but disaster recovery tests are incomplete.

4. Risk Assessment

Each finding has been evaluated using a qualitative risk assessment, prioritizing based on likelihood and impact. High-risk areas include incident response readiness and supplier risk management, requiring immediate corrective actions.

5. Corrective Action Plan

- Implement automated monitoring for access control enforcement.
- Conduct a full incident response simulation within 90 days.
- Develop a standardized supplier risk assessment framework.
- Complete disaster recovery testing and document lessons learned.