Audit Report - Information Security Policy

ISO 27001:2022 Internal Audit

Audit ID: 122

Framework: ISO 27001:2022

Policy: Information Security Policy

Auditor: Radha Sharma

Reviewer: admin.grc

Due Date: 27/09/2025

Progress: 30% (Completed)

Audit Type: Internal

Status: Completed

Executive Summary

This internal audit assessed the organization's Information Security Policy compliance against ISO 27001:2022 requirements. The audit covered policy framework, governance structure, risk management processes, and implementation effectiveness across all business units.

Overall Assessment: **Satisfactory** with minor improvements required

Compliance Score: 85%

Audit Period: August 1-20, 2025

Report Date: August 24, 2025

Audit Scope and Objectives

Scope

- Information Security Policy framework (A.5.1)
- Information security roles and responsibilities (A.5.2)
- Segregation of duties (A.5.3)
- Management responsibilities (A.5.4)
- Information security in project management (A.5.5)

Objectives

- Evaluate policy completeness and currency
- Assess implementation effectiveness
- Verify compliance with ISO 27001:2022 requirements
- Identify improvement opportunities

Key Findings Summary

Finding Level	Count	Percentage
Critical	0	0%
Major	2	15%
Minor	6	45%
Observations	5	40%

Detailed Findings

Major Findings

M-001: Policy Review and Update Process

Control: A.5.1 - Policies for information security

Finding: Information Security Policy has not been reviewed for 14 months, exceeding the 12-month review requirement.

Risk: Outdated policy may not address current threats and organizational changes.

Recommendation: Implement automated policy review reminders and establish quarterly review cycles for critical policies.

Management Response: *Agreed. Policy review scheduled for September 15, 2025.*

Target Date: September 30, 2025

M-002: Incomplete Role Definition

Control: A.5.2 - Information security roles and responsibilities

Finding: Security roles for 3 new departments established in 2025 are not clearly defined in the policy.

Risk: Unclear responsibilities may lead to security gaps and accountability issues.

Recommendation: Update policy to include specific security roles for all organizational units.

Management Response: *Role definitions being drafted with HR and department heads.*

Target Date: October 15, 2025

Minor Findings

Minor-001: Document Version Control

Control: A.5.1 - Policies for information security

Finding: Some policy documents lack proper version control numbering.

Recommendation: Implement standardized version control system.

Minor-002: Training Records

Control: A.5.2 - Information security roles and responsibilities

Finding: Training completion records not maintained for all staff with security responsibilities.

Recommendation: Establish centralized training record system.

Minor-003: Policy Accessibility

Control: A.5.1 - Policies for information security

Finding: Policy documents not easily accessible to all employees through corporate intranet.

Recommendation: Improve policy portal navigation and search functionality.

Positive Observations

1. **Strong Executive Support**: Clear commitment from senior management to information security
2. **Comprehensive Policy Coverage**: All required ISO 27001:2022 policy areas addressed
3. **Regular Communication**: Effective security awareness communication program
4. **Incident Response Integration**: Well-integrated incident response procedures
5. **Third-Party Management**: Strong vendor security requirements

Compliance Assessment

ISO 27001:2022 Control Assessment

Control	Requirement	Implementation	Compliance	Comments
A.5.1	Information security policies	Implemented	80%	Needs regular review process
A.5.2	Information security roles	Implemented	75%	Role definitions incomplete
A.5.3	Segregation of duties	Implemented	90%	Well documented and implemented
A.5.4	Management responsibilities	Implemented	85%	Clear accountability structure
A.5.5	Project management	Implemented	95%	Excellent integration

Risk Assessment

Identified Risks

1. **Policy Currency Risk**: Medium - Outdated policies may not address current threats
2. **Role Clarity Risk**: Medium - Unclear responsibilities in new departments
3. **Training Gap Risk**: Low - Some staff lacking current security training
4. **Access Risk**: Low - Policy accessibility issues for some employees

Risk Mitigation

- Implement automated policy review system
- Conduct role definition workshops
- Deploy learning management system
- Enhance intranet policy portal

Recommendations

Immediate Actions (0-30 days)

1. Schedule and complete overdue policy review
2. Implement automated review reminders
3. Begin role definition workshops for new departments

Short-term Actions (30-90 days)

1. Complete role definitions for all departments
2. Deploy centralized training tracking system
3. Enhance policy portal functionality
4. Conduct policy awareness campaign

Long-term Actions (90+ days)

1. Establish continuous policy improvement process
2. Implement advanced training analytics
3. Develop policy effectiveness metrics
4. Create policy compliance dashboard

Management Action Plan

Action Item	Owner	Target Date	Status
Policy review completion	Legal/Compliance	Sept 30, 2025	In Progress
Role definition update	HR/Security	Oct 15, 2025	Planned
Training system deployment	HR/IT	Nov 30, 2025	Planned
Portal enhancement	IT	Dec 15, 2025	Planned

Conclusion

The Information Security Policy audit reveals a fundamentally sound policy framework with strong management support and comprehensive coverage. The identified findings are manageable and primarily relate to process improvements rather than fundamental policy gaps.

The organization demonstrates strong commitment to information security through clear governance structures and integrated security processes. Implementation of the recommended improvements will enhance policy effectiveness and ensure continued compliance with ISO 27001:2022 requirements.

Next Steps

1. **30-day Follow-up**: Review progress on immediate actions
2. **Quarterly Review**: Monitor implementation of short-term actions
3. **Annual Assessment**: Comprehensive policy framework evaluation
4. **Continuous Monitoring**: Track policy compliance metrics

Auditor: Radha Sharma, Senior Internal Auditor

Review: admin.grc, Audit Manager

Distribution: Executive Team, Department Heads, Compliance Committee

Next Audit: February 2026