Audit Report - Organization of Information Security Policy

ISO 27001:2022 Internal Audit

Audit ID: 125

Framework: ISO 27001:2022

Policy: Organization of Information Security Policy

Auditor: Priya Gupta

Reviewer: admin.grc

Due Date: 27/09/2025

Progress: 60% (Completed)

Audit Type: Internal

Status: Completed

Executive Summary

This internal audit evaluated the organization's Information Security governance structure and organizational controls in accordance with ISO 27001:2022 requirements. The assessment covered organizational roles, responsibilities, project management security, and third-party relationship management.

Overall Assessment: **Excellent** with minor refinements recommended

Compliance Score: 91%

Audit Period: August 12-28, 2025

Report Date: August 24, 2025

Audit Scope and Objectives

Scope

- Information security roles and responsibilities (A.5.2)
- Segregation of duties (A.5.3)
- Management responsibilities (A.5.4)
- Contact with authorities (A.5.5)
- Contact with special interest groups (A.5.6)
- Information security in project management (A.5.7)
- Mobile device policy (A.6.7)
- Teleworking (A.6.8)

Objectives

- Assess organizational security governance structure
- Evaluate role definitions and segregation of duties
- Review project security integration
- Validate third-party security coordination

Key Findings Summary

Finding Level	Count	Percentage
Critical	0	0%
Major	1	10%
Minor	4	40%
Observations	5	50%

Detailed Findings

Major Findings

M-001: Project Security Integration Gaps

Control: A.5.7 - Information security in project management

Finding: 3 out of 12 active projects lack documented security requirements or security reviews. Project management methodology does not mandate security checkpoints.

Risk: Projects may introduce security vulnerabilities or bypass security controls.

Recommendation: Integrate security reviews into standard project methodology and establish mandatory security gates.

Management Response: *Project methodology update approved. Security gates being defined with PMO.*

Target Date: October 15, 2025

Minor Findings

Minor-001: Authority Contact Update

Control: A.5.5 - Contact with authorities

Finding: Contact information for 2 regulatory authorities not updated in the past 18 months.

Recommendation: Establish quarterly contact verification process.

Target Date: September 30, 2025

Minor-002: Interest Group Participation

Control: A.5.6 - Contact with special interest groups

Finding: Limited participation in industry security forums and threat intelligence sharing groups.

Recommendation: Increase engagement with relevant security communities.

Target Date: November 30, 2025

Minor-003: Mobile Device Policy Clarity

Control: A.6.7 - Mobile device policy

Finding: BYOD policy lacks specific security requirements for different device types.

Recommendation: Enhance policy with device-specific security standards.

Target Date: October 31, 2025

Minor-004: Telework Security Guidelines

Control: A.6.8 - Teleworking

Finding: Remote work security guidelines need updates for hybrid work environment.

Recommendation: Update teleworking policy for current work arrangements.

Target Date: September 15, 2025

Organizational Structure Analysis

Information Security Governance

Executive Level

- **Chief Information Security Officer (CISO)**: Dedicated role with direct CEO reporting
- **Security Committee**: Monthly meetings with executive participation
- **Board Oversight**: Quarterly security updates to board of directors

Operational Level

- **Security Team**: 8 dedicated security professionals
- **Security Champions**: 15 departmental representatives
- **Incident Response Team**: Cross-functional 12-member team

Roles and Responsibilities Matrix

Role	Security Policy	Risk Management	Incident Response	Compliance	Training
CISO	Owner	Owner	Leader	Owner	Sponsor
Security Manager	Co-owner	Manager	Manager	Manager	Owner

IT Manager	Implementer	Contributor	Member	Contributor	Participant
Department Heads	Enforcer	Contributor	Coordinator	Enforcer	Champion
All Employees	Compliant	Reporter	Reporter	Compliant	Participant

Segregation of Duties Assessment

Financial Systems

- **Approval Authority**: Well-segregated across multiple approvers
- **System Access**: Appropriate role-based separation
- **Audit Trail**: Comprehensive logging and monitoring

IT Operations

- **Development vs. Production**: Clear separation maintained
- **Administrative Access**: Properly segregated and monitored
- **Change Management**: Multi-level approval process

Security Operations

- **Policy Development**: Separated from implementation
- **Monitoring**: Independent from system administration
- **Investigation**: Separate from normal operations

Project Security Integration Analysis

Current State

- **Total Active Projects**: 12
- **Projects with Security Reviews**: 9 (75%)
- **Security Requirements Documented**: 9 (75%)
- **Security Testing Completed**: 7 (58%)

Project Categories

Project Type	Count	Security Review Status	Risk Level
Infrastructure	4	4 completed	Medium
Application Development	5	3 completed	High
Business Process	2	2 completed	Low
Compliance	1	1 completed	Low

Security Integration Gaps

1. **Application Projects**: 2 projects missing security reviews
2. **Testing Phase**: 5 projects lack comprehensive security testing
3. **Documentation**: 3 projects missing security architecture documentation

Risk Assessment

Organizational Risks

1. **Project Security**: Medium - Some projects may introduce vulnerabilities
2. **Contact Management**: Low - Minor outdated contact information
3. **Community Engagement**: Low - Limited external security collaboration
4. **Policy Currency**: Low - Some policies need minor updates

Mitigating Factors

1. **Strong Leadership**: Excellent executive support for security
2. **Clear Structure**: Well-defined roles and responsibilities
3. **Regular Reviews**: Consistent security committee oversight
4. **Good Documentation**: Comprehensive policy framework

Compliance Assessment

ISO 27001:2022 Control Assessment

Control	Requirement	Implementation	Compliance	Comments

A.5.2	Information security roles	Implemented	95%	Excellent role definition and matrix
A.5.3	Segregation of duties	Implemented	90%	Strong segregation across functions
A.5.4	Management responsibilities	Implemented	95%	Clear management accountability
A.5.5	Contact with authorities	Implemented	85%	Contact updates needed
A.5.6	Special interest groups	Partial	75%	Limited external engagement
A.5.7	Project security	Implemented	80%	Integration gaps in methodology
A.6.7	Mobile device policy	Implemented	85%	BYOD policy needs enhancement
A.6.8	Teleworking	Implemented	90%	Minor policy updates needed

Best Practices Identified

Organizational Excellence

1. **Security Committee Effectiveness**: Monthly meetings with excellent attendance and engagement
2. **Role Clarity**: Comprehensive RACI matrix for all security activities
3. **Executive Support**: Strong C-level commitment and resource allocation
4. **Cross-functional Integration**: Security champions program working effectively
5. **Incident Response**: Well-structured team with clear escalation procedures

Innovation Areas

1. **Security Awareness Program**: Creative and engaging training approaches
2. **Metrics and Reporting**: Comprehensive security dashboards and KPIs
3. **Threat Intelligence**: Effective integration of external threat information
4. **Continuous Improvement**: Regular process optimization based on lessons learned

Recommendations

Immediate Actions (0-30 days)

1. **Contact Verification**: Update regulatory authority contact information
2. **Telework Policy**: Update remote work security guidelines
3. **Project Review**: Complete security reviews for pending projects

Short-term Actions (30-90 days)

1. **Project Methodology**: Integrate security gates into PMO processes
2. **Mobile Policy**: Enhance BYOD policy with device-specific requirements
3. **External Engagement**: Increase participation in security communities
4. **Training Updates**: Refresh security awareness training content

Long-term Actions (90+ days)

1. **Maturity Assessment**: Conduct comprehensive security maturity evaluation
2. **Automation**: Implement automated policy compliance monitoring
3. **Integration**: Enhance security tool integration and orchestration
4. **Benchmarking**: Regular comparison with industry best practices

Management Action Plan

Action Item	Owner	Target Date	Priority	Status
Project security gates	PMO/CISO	Oct 15, 2025	High	Approved
Contact verification	Security Team	Sep 30, 2025	Medium	Planned
Telework policy update	HR/Security	Sep 15, 2025	Medium	In Progress
BYOD policy enhancement	IT/Security	Oct 31, 2025	Medium	Planned
Industry engagement	CISO	Nov 30, 2025	Low	Planned

Key Performance Indicators

Current Metrics

- **Security Committee Attendance**: 95%
- **Role Training Completion**: 98%
- **Policy Acknowledgment**: 96%
- **Incident Response Time**: 15 minutes average
- **Project Security Review**: 75%

Target Improvements

- **Project Security Review**: 100%
- **External Engagement**: 4 forums minimum
- **Policy Currency**: 100% within 12 months
- **Authority Contacts**: Quarterly verification

Conclusion

The Organization of Information Security Policy audit reveals an exemplary organizational security structure with strong leadership, clear roles, and effective governance processes. The organization demonstrates mature security management with excellent executive support and well-defined accountability structures.

The single major finding regarding project security integration is easily addressable and reflects the organization's growth rather than fundamental weaknesses. The minor findings are maintenance items that further demonstrate the organization's attention to continuous improvement.

The identified best practices position the organization as a potential benchmark for security governance in the industry. The strong foundation provides excellent support for ongoing security improvements and compliance initiatives.

Follow-up Activities

1. **Monthly**: Track project security integration progress
2. **Quarterly**: Review organizational changes and role updates
3. **Semi-annually**: Assess security committee effectiveness
4. **Annually**: Comprehensive organizational security maturity assessment

Auditor: Priya Gupta, Lead Internal Auditor

Review: admin.grc, Audit Manager

Distribution: Executive Team, Security Committee, Department Heads

Next Audit: April 2026