

# ISO 27001:2022 Gap Assessment & Implementation Roadmap

Information Security Management System Readiness Evaluation

**Prepared By:** Mustafa Alobaidy  
Cybersecurity Governance, Risk & Compliance  
Specialist

**Assessment Date:** March 5, 2026  
**Document Version:** 1.0

## 1. Executive Summary

**Purpose:** This gap assessment report evaluates the organization's current information security posture against the requirements of ISO/IEC 27001:2022, the international standard for Information Security Management Systems (ISMS). The assessment identifies gaps between current security controls and ISO 27001 Annex A requirements, providing a strategic roadmap for achieving certification readiness.

**Scope:** The assessment examined 10 critical security control domains from ISO 27001 Annex A, focusing on technical and organizational controls essential for establishing a comprehensive ISMS. The evaluation was conducted through documentation review, stakeholder interviews, technical configuration analysis, and security control testing.

**Overall Findings:** The organization demonstrates a **52% compliance level** with assessed ISO 27001 controls. While foundational security practices exist, significant gaps were identified in formal documentation, security monitoring, incident response capabilities, and vendor risk management. With focused remediation efforts over a 12-month period, the organization can achieve certification readiness.

### Key Findings

- **Critical Gaps:** 2 controls require immediate attention (Incident Response, Logging & Monitoring)
- **High Priority:** 4 controls need significant improvement within 3-6 months

- **Medium Priority:** 3 controls require moderate enhancements
- **Low Priority:** 1 control needs minor refinement
- **Estimated Timeline to Certification:** 12-14 months with dedicated resources

## 2. Assessment Methodology

The gap assessment was conducted using a comprehensive evaluation framework aligned with ISO 27001:2022 Annex A control objectives. The methodology incorporated the following activities:

- **Documentation Review:** Analysis of existing security policies, procedures, standards, and guidelines to determine alignment with ISO 27001 requirements
- **Technical Assessment:** Examination of security configurations, system hardening, access controls, and monitoring capabilities through hands-on technical evaluation
- **Stakeholder Interviews:** Structured discussions with IT leadership, security personnel, system administrators, and business unit managers to understand current practices
- **Control Testing:** Validation of control effectiveness through sampling, testing, and evidence collection
- **Gap Analysis:** Comparison of current state against ISO 27001 requirements, identifying specific deficiencies and remediation needs
- **Risk Evaluation:** Assessment of risk exposure resulting from identified gaps, categorized as Critical, High, Medium, or Low

Each control was evaluated using a maturity scale: **Non-existent (0%)**, **Initial/Ad-hoc (25%)**, **Developing (50%)**, **Defined (75%)**, and **Optimized (100%)**.

## 3. Gap Assessment Table

The following table presents detailed findings for each assessed ISO 27001 Annex A control, including current implementation status, identified gaps, associated risks, and recommended remediation actions.

CONTROL REFERENCE	CONTROL DOMAIN	CURRENT STATE	IDENTIFIED GAP	RISK LEVEL	RECOMMENDED REMEDIATION
A.5.15	Access Control	Basic authentication exists; no formal access review process; privileged access not segregated	Lack of role-based access control (RBAC), no periodic access reviews, insufficient privileged account management	HIGH	Implement RBAC framework, establish quarterly access reviews, deploy privileged access management (PAM) solution, enforce least privilege principle
A.5.9	Asset Management	Partial asset inventory maintained in spreadsheets; incomplete for cloud assets and mobile devices	No centralized asset register, incomplete asset classification, missing asset ownership assignment	MEDIUM	Deploy automated asset discovery tool, create comprehensive asset register with classification schema, assign asset owners, establish update procedures
A.5.24	Incident Response	No formal incident response plan; reactive approach to security events; unclear escalation procedures	Missing incident response policy and procedures, no designated incident response team, no incident classification framework	CRITICAL	Develop comprehensive incident response plan, establish IR team with defined roles, implement incident management system, conduct tabletop exercises

CONTROL REFERENCE	CONTROL DOMAIN	CURRENT STATE	IDENTIFIED GAP	RISK LEVEL	RECOMMENDED REMEDIATION
A.8.15	Logging and Monitoring	Basic logging enabled on some systems; no centralized log management; limited security monitoring	No SIEM solution, inconsistent logging across infrastructure, no log retention policy, lack of security event correlation	CRITICAL	Deploy SIEM platform, implement comprehensive logging across all systems, establish 12-month log retention, configure security alerting and correlation rules
A.5.19	Vendor Risk Management	Informal vendor selection process; minimal security requirements in contracts; no ongoing vendor assessments	No third-party risk assessment program, missing security requirements in vendor agreements, lack of vendor security monitoring	HIGH	Develop vendor risk assessment framework, create security requirements template for contracts, implement annual vendor security reviews, classify vendors by risk
A.6.3	Security Awareness Training	Ad-hoc security communications; no formal training program; onboarding includes basic security overview	No structured security awareness program, missing role-specific training, no training effectiveness measurement	HIGH	Launch annual security awareness training program, implement phishing simulation campaigns, develop role-based training modules, track completion and

CONTROL REFERENCE	CONTROL DOMAIN	CURRENT STATE	IDENTIFIED GAP	RISK LEVEL	RECOMMENDED REMEDIATION
					effectiveness metrics
A.8.13	Backup and Recovery	Regular backups performed for critical systems; some backup testing conducted; no formal backup policy	Incomplete backup coverage, inconsistent testing schedule, lack of documented recovery procedures, no off-site backup verification	MEDIUM	Establish comprehensive backup policy, extend coverage to all critical systems and data, implement quarterly recovery testing, document recovery time objectives (RTOs)
A.8.24	Encryption Controls	HTTPS enabled for public-facing applications; some database encryption; inconsistent encryption for data at rest	No enterprise encryption policy, missing encryption for sensitive data at rest, insufficient key management, no encryption for backups	HIGH	Develop encryption policy and standards, implement full-disk encryption for endpoints, encrypt sensitive databases and file shares, deploy centralized key management system
A.8.8	Vulnerability Management	Periodic vulnerability scanning; patch management follows vendor schedules; no formal vulnerability	Inconsistent scanning frequency, no vulnerability prioritization framework, delayed patching for	MEDIUM	Implement continuous vulnerability scanning, establish vulnerability remediation SLAs based on

CONTROL REFERENCE	CONTROL DOMAIN	CURRENT STATE	IDENTIFIED GAP	RISK LEVEL	RECOMMENDED REMEDIATION
		management process	non-critical systems, missing vulnerability acceptance process		severity, create formal exception process, integrate with change management
A.8.32	Change Management	Change approval process exists for production systems; limited documentation; emergency changes not well-controlled	Informal change documentation, inconsistent testing requirements, no change advisory board, weak rollback procedures	LOW	Formalize change management policy, establish Change Advisory Board (CAB), implement change request system with approval workflows, define emergency change procedures

#### 4. Priority Remediation Plan

The following phased approach outlines the recommended implementation timeline to address identified gaps and achieve ISO 27001 certification readiness. The plan prioritizes critical and high-risk controls while establishing foundational ISMS components.

## Phase 1: Foundation & Critical Controls (0–3 Months)

- **Establish ISMS Framework:** Develop and approve Information Security Policy, define ISMS scope, appoint Information Security Manager and ISMS implementation team
- **Incident Response (Critical):** Develop incident response plan and procedures, establish incident response team with 24/7 contact roster, implement incident ticketing system, conduct initial tabletop exercise
- **Logging & Monitoring (Critical):** Deploy SIEM solution (e.g., Splunk, ELK Stack, or Microsoft Sentinel), implement centralized logging for all critical systems, establish log retention policy and procedures
- **Risk Assessment:** Conduct comprehensive information security risk assessment, develop risk treatment plan, establish risk acceptance criteria and approval process
- **Documentation:** Begin development of mandatory ISMS documentation including Statement of Applicability (SoA), risk assessment methodology, and core security procedures

## Phase 2: Control Implementation & Process Development (3–6 Months)

- **Access Control (High):** Design and implement RBAC model, deploy privileged access management solution, establish quarterly access review process, implement multi-factor authentication (MFA)
- **Vendor Risk Management (High):** Develop third-party risk assessment framework and questionnaires, update master services agreement template with security requirements, conduct initial vendor risk assessments for critical suppliers
- **Security Awareness Training (High):** Launch organization-wide security awareness training program, develop training content and delivery platform, implement quarterly phishing simulation campaigns, establish training completion tracking
- **Encryption Controls (High):** Develop encryption policy and standards, implement full-disk encryption for all endpoints, encrypt sensitive databases, deploy key management system
- **Asset Management (Medium):** Deploy automated asset discovery solution, create comprehensive asset register with classification, assign asset owners and custodians
- **Internal Audit:** Conduct first internal ISMS audit to identify remaining gaps and assess control effectiveness

Phase 3: Optimization & Certification Readiness (6–12 Months)

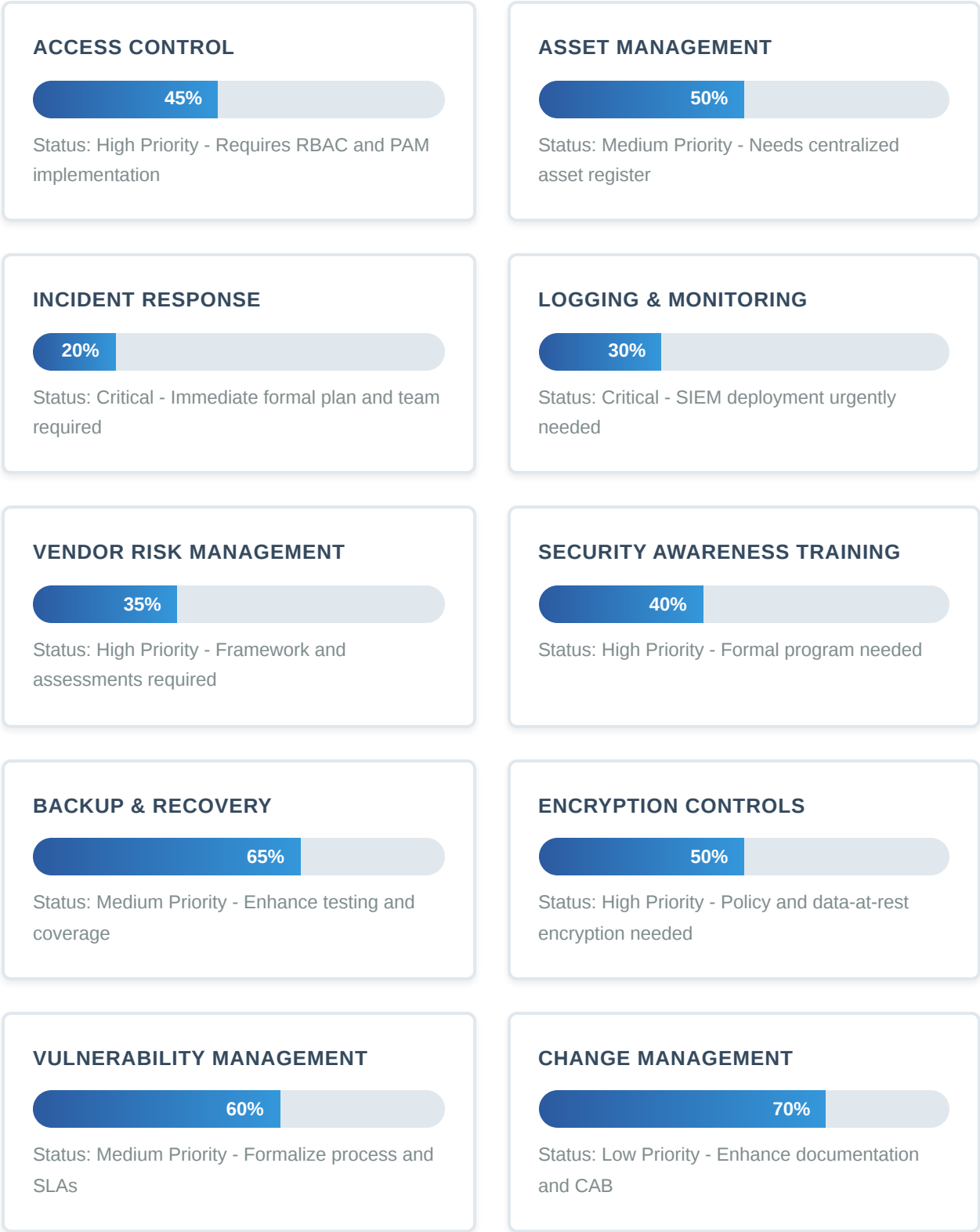
- **Backup & Recovery (Medium):** Formalize backup and recovery policy, extend backup coverage to all critical assets, implement quarterly disaster recovery testing with documented results
- **Vulnerability Management (Medium):** Implement continuous vulnerability scanning across all assets, establish vulnerability remediation SLAs (Critical: 7 days, High: 30 days, Medium: 60 days), integrate with patch management
- **Change Management (Low):** Enhance change management procedures with formal documentation requirements, establish Change Advisory Board with regular meetings, implement automated change tracking system
- **Monitoring & Metrics:** Deploy security dashboards and KPIs, configure automated SIEM correlation rules and alerting, establish security metrics reporting to management
- **Management Review:** Conduct formal management review of ISMS performance, review and update risk assessment, demonstrate continual improvement
- **Pre-Certification Audit:** Engage external consultant for pre-assessment gap analysis (Stage 0 audit), remediate findings, conduct second internal audit
- **Certification Audit:** Schedule and prepare for formal ISO 27001 certification audit (Stage 1 and Stage 2)

5. ISO 27001 Readiness Scorecard

The following scorecard provides a maturity assessment across the evaluated security control domains, indicating current compliance levels and readiness for certification.







Recommendations & Next Steps

To achieve ISO 27001 certification readiness within the projected 12-14 month timeline, the following immediate actions are recommended:

- **Executive Sponsorship:** Secure visible executive support and budget allocation for ISMS implementation, designating a senior management representative
- **Resource Allocation:** Assign dedicated resources to the ISMS implementation team, including Information Security Manager, security analysts, and project coordinator
- **Quick Wins:** Immediately address critical gaps (Incident Response and Logging & Monitoring) to reduce organizational risk exposure
- **Vendor Engagement:** Consider engaging external consultants for ISMS framework design and SIEM implementation to accelerate timeline
- **Training Investment:** Enroll key personnel in ISO 27001 Lead Implementer and Internal Auditor training courses
- **Monthly Governance:** Establish monthly ISMS steering committee meetings to track progress, resolve roadblocks, and maintain momentum

**Conclusion:** While significant work remains to achieve full ISO 27001 compliance, the organization has established foundational security practices that provide a solid starting point. By following the phased remediation roadmap and dedicating appropriate resources, certification readiness is achievable within the 12-14 month timeframe. The immediate priority must be addressing critical gaps in incident response and security monitoring to reduce current risk exposure.

---

### Confidential & Proprietary

ISO 27001:2022 Gap Assessment & Implementation Roadmap | Prepared by Mustafa Alobaidy, Cybersecurity GRC Specialist | March 5, 2026

This document contains confidential information and is intended solely for the use of the organization's management team.