

ISO 27001:2022

Gap Assessment & Implementation Roadmap

Representative Consulting Scenario

Prepared for: CloudSync Technologies

Prepared by: Mustafa Alobaidy

Senior GRC & Cybersecurity Awareness Consultant

March 2026

Table of Contents

1. Executive Summary
2. Organizational Context
3. Assessment Methodology
4. Gap Assessment Findings
5. Risk Prioritization Matrix
6. Implementation Roadmap
7. ISO 27001 Readiness Scorecard
8. Final Recommendations

1. Executive Summary

CloudSync Technologies engaged Mustafa Alobaidy, Senior GRC & Cybersecurity Awareness Consultant, to conduct a comprehensive ISO 27001:2022 gap assessment and develop an implementation roadmap. This engagement aims to evaluate the organization's current information security posture against the ISO 27001:2022 standard requirements and Annex A controls, identify gaps, and provide a prioritized remediation strategy.

CloudSync Technologies, a mid-sized SaaS provider with approximately 200 employees, operates critical AWS infrastructure supporting B2B clients across North America and Europe. The organization seeks ISO 27001 certification to meet contractual obligations, enhance market competitiveness, and strengthen its security governance framework.

Key Findings Summary

Metric	Value
Overall Maturity Score	2.8 / 5.0 (Developing)
Critical Gaps Identified	12
High-Risk Gaps	8
Medium-Risk Gaps	15
Estimated Certification Timeline	9-12 months
Recommended Investment	\$180,000 - \$250,000

2. Organizational Context

2.1 Company Profile

Attribute	Details
Organization Name	CloudSync Technologies Inc.
Industry	Software as a Service (SaaS)
Headquarters	Austin, Texas, USA
Employee Count	200 (including 45 remote workers)
Primary Infrastructure	Amazon Web Services (AWS)
Key Services	Cloud-based document collaboration and workflow automation
Client Base	500+ B2B clients (Healthcare, Financial Services, Manufacturing)
Annual Revenue	\$35M USD

2.2 Compliance Drivers

Several factors drive CloudSync Technologies' pursuit of ISO 27001 certification:

- Contractual Requirements: 65% of enterprise clients require ISO 27001 certification in vendor agreements
- Regulatory Landscape: GDPR compliance for EU clients, SOC 2 Type II alignment requirements
- Competitive Advantage: Market differentiation in the crowded SaaS landscape
- Risk Management: Formalization of security practices to reduce operational risk
- Board Mandate: Corporate governance directive for enhanced security posture

2.3 Current Security Environment

Domain	Tool/Platform	Status
Identity Management	Okta (SSO/MFA)	Partially Implemented
Cloud Security	AWS Security Hub, GuardDuty	Active
SIEM	Splunk Enterprise	Limited Configuration
Endpoint Protection	CrowdStrike Falcon	Fully Deployed
Vulnerability Management	Qualys VMDR	Quarterly Scans Only
Backup & Recovery	AWS Backup, Veeam	Implemented

3. Assessment Methodology

3.1 Assessment Framework

This assessment was conducted in alignment with ISO/IEC 27001:2022 requirements, utilizing a structured methodology encompassing document review, stakeholder interviews, technical validation, and control testing. The assessment covered all 93 Annex A controls across 4 themes: Organizational, People, Physical, and Technological.

3.2 Control Maturity Scoring Model

Level	Maturity Stage	Description
0	Non-Existent	Control not implemented; no awareness of requirement
1	Initial/Ad Hoc	Control exists but is informal, reactive, and inconsistent
2	Repeatable	Control is documented and consistently applied in some areas
3	Defined	Control is standardized, documented, and communicated organization-wide
4	Managed	Control is measured, monitored, and continuously improved
5	Optimized	Control is fully integrated, automated where possible, and continuously enhanced

3.3 Risk Evaluation Criteria

Risk Level	Definition
Critical	Immediate threat to business operations; regulatory non-compliance; significant financial/reputational impact
High	Significant security exposure; likely to result in data breach or compliance failure
Medium	Notable gap requiring attention within 6 months; moderate risk exposure
Low	Minor improvement opportunity; limited immediate risk

4. Gap Assessment Findings

The following table presents detailed findings across key ISO 27001:2022 Annex A control domains. Each control area has been evaluated for current state, identified gaps, associated risk level, and recommended remediation actions.

4.1 Detailed Gap Assessment Matrix

Control Domain	Current State	Identified Gap	Risk Level	Recommended Remediation
A.5 Access Control	MFA enabled for critical systems via Okta; no privileged access management (PAM) solution; manual access reviews conducted annually	No PAM solution; infrequent access reviews; lack of least-privilege enforcement	High	Implement CyberArk or BeyondTrust PAM; quarterly access recertification; implement RBAC model
A.5 Asset Management	Partial CMDB in ServiceNow; cloud assets tracked via AWS Config	No comprehensive asset inventory; shadow IT not addressed; asset classification incomplete	High	Deploy automated asset discovery (Qualys/Axonius); implement data classification framework; update CMDB
A.5 Vendor Risk	Basic vendor questionnaires; no continuous monitoring; 120+ third-party vendors	No formal TPRM program; no vendor risk scoring; limited due diligence	Critical	Establish TPRM framework; implement SecurityScorecard/Bi tSight; tiered vendor classification
A.5 Incident Response	Basic IR playbook exists; Splunk SIEM deployed; no tabletop exercises	Outdated IR procedures; no automated response; limited forensic capability	High	Update IR playbooks; implement SOAR (Splunk SOAR/Palo Alto XSOAR); quarterly tabletop exercises
A.8 Logging & Monitoring	Splunk deployed; AWS CloudTrail enabled; limited alerting rules	Insufficient log retention (30 days); limited correlation rules; no 24/7 monitoring	High	Extend log retention to 1 year; develop comprehensive use cases; consider MDR service
A.6 Security Awareness	Annual security training via KnowBe4; basic phishing simulations	Low training completion rates (68%); no role-based training; limited metrics	Medium	Implement continuous awareness program; role-based training tracks; monthly phishing campaigns
A.8 Encryption	TLS 1.2/1.3 for transit; AWS KMS for data at rest; laptop encryption enforced	Inconsistent key management; no cryptographic policy; some legacy TLS 1.0 systems	Medium	Develop cryptographic policy; centralize key management; deprecate TLS 1.0/1.1
A.8 Backup & Recovery	AWS Backup configured; Veeam for on-prem; annual DR test	Untested backup restoration; RTO/RPO not validated; no immutable backups	Medium	Quarterly restoration tests; implement immutable backup (AWS Backup Vault

ISO 27001 Gap Assessment & Implementation Roadmap

				Lock); document RTO/RPO
A.8 Vulnerability Mgmt	Qualys quarterly scans; ad hoc patching; no vulnerability SLAs	Infrequent scanning; no patch management policy; 45-day average remediation time	High	Weekly vulnerability scans; patch management SLAs (Critical: 7 days, High: 14 days); automated patching
A.8 Change Management	ServiceNow Change Management module; CAB reviews for major changes	Emergency changes bypass CAB; limited security review in change process; no rollback testing	Medium	Integrate security review in change process; mandatory rollback procedures; automate change validation

5. Risk Prioritization Matrix

The following matrix prioritizes identified gaps based on risk severity and implementation complexity, enabling CloudSync Technologies to allocate resources effectively and address the most critical vulnerabilities first.

Priority	Control Area	Risk Level	Complexity	Timeline
1	Third-Party Risk Management Program	Critical	Medium	Immediate
2	Privileged Access Management	High	High	Phase 1
3	Vulnerability Management Enhancement	High	Medium	Phase 1
4	Incident Response Maturation	High	Medium	Phase 1
5	SIEM Optimization	High	Medium	Phase 1
6	Asset Inventory & Classification	High	Medium	Phase 2
7	Security Awareness Program	Medium	Low	Phase 2
8	Cryptographic Controls	Medium	Medium	Phase 2
9	Backup & Recovery Testing	Medium	Low	Phase 2
10	Change Management Enhancement	Medium	Low	Phase 3

6. Implementation Roadmap

The following phased implementation roadmap provides a structured approach to achieving ISO 27001:2022 certification readiness. Each phase includes specific deliverables, resource requirements, and success criteria.

Phase 1: Foundation (Months 0-3)

Initiative	Deliverable	Owner	Est. Cost
ISMS Documentation	Develop Information Security Policy, ISMS scope, Statement of Applicability	GRC Consultant	\$25,000
Risk Assessment	Conduct formal risk assessment using ISO 27005 methodology	Risk Manager	\$15,000
TPRM Program	Establish Third-Party Risk Management framework and vendor assessments	GRC Consultant	\$20,000
PAM Implementation	Deploy CyberArk/BeyondTrust for privileged access management	Security Engineer	\$45,000
Vulnerability Mgmt	Implement weekly scanning, patch management SLAs, remediation tracking	IT Operations	\$15,000

Phase 2: Enhancement (Months 3-6)

Initiative	Deliverable	Owner	Est. Cost
Asset Management	Complete asset inventory, implement data classification, update CMDB	IT Manager	\$20,000
SIEM Optimization	Develop 50+ use cases, extend log retention, implement alerting	SOC Lead	\$25,000
Security Awareness	Launch continuous awareness program, monthly phishing campaigns	HR/Security	\$15,000
Cryptographic Policy	Develop policy, centralize key management, deprecate legacy protocols	Security Architect	\$10,000
Internal Audit	Conduct internal ISMS audit, identify non-conformities	GRC Consultant	\$15,000

Phase 3: Certification (Months 6-12)

Initiative	Deliverable	Owner	Est. Cost
Management Review	Conduct management review, address audit findings	CISO	\$5,000
DR/BCP Testing	Quarterly restoration tests, tabletop exercises, RTO/RPO validation	IT Manager	\$15,000

ISO 27001 Gap Assessment & Implementation Roadmap

Change Management	Integrate security review, rollback procedures, automated validation	IT Operations	\$10,000
Pre-Certification Audit	Engage certification body for Stage 1 audit preparation	External Auditor	\$20,000
Certification Audit	Stage 1 and Stage 2 certification audits	Certification Body	\$30,000

7. ISO 27001 Readiness Scorecard

The following scorecard provides a snapshot of CloudSync Technologies' current readiness across ISO 27001:2022 control themes and key ISMS requirements.

Control Theme / Clause	Current Score	Target (6 months)	Target (12 months)
Organizational Controls (A.5)	2.5	3.5	4.0
People Controls (A.6)	2.8	3.5	4.0
Physical Controls (A.7)	3.2	3.8	4.0
Technological Controls (A.8)	2.6	3.5	4.0
Context of Organization (Clause 4)	2.0	3.5	4.0
Leadership (Clause 5)	2.5	3.5	4.0
Planning (Clause 6)	2.0	3.5	4.0
Support (Clause 7)	2.8	3.5	4.0
Operation (Clause 8)	2.5	3.5	4.0
Performance Evaluation (Clause 9)	1.5	3.5	4.0
Improvement (Clause 10)	2.0	3.5	4.0
OVERALL SCORE	2.4	3.5	4.0

8. Final Recommendations

8.1 Strategic Recommendations

- Executive Sponsorship: Secure C-suite commitment with dedicated budget allocation and regular steering committee meetings
- Dedicated ISMS Owner: Appoint a full-time Information Security Manager to lead certification efforts
- Quick Wins: Prioritize high-impact, low-effort initiatives to demonstrate early progress and maintain momentum
- Culture Shift: Embed security awareness into organizational culture through continuous training and recognition programs
- Continuous Improvement: Establish metrics-driven approach to security governance beyond certification

8.2 Resource Requirements

Category	Requirement/Estimate
Internal Resources	1 FTE Information Security Manager, 0.5 FTE IT Security Engineer
External Support	GRC Consultant (160 hours), Penetration Testing (40 hours)
Technology Investment	\$80,000 - \$120,000 (PAM, SIEM enhancements, TPRM tools)
Training & Awareness	\$15,000 - \$25,000
Certification Costs	\$40,000 - \$60,000 (audit fees, certification body)
Total Estimated Investment	\$180,000 - \$250,000

8.3 Success Factors

- Executive visibility and regular progress reporting
- Cross-functional collaboration between IT, Security, HR, and Legal
- Realistic timeline expectations with buffer for unforeseen challenges
- Integration of ISMS requirements into existing business processes
- Engagement of experienced ISO 27001 implementation consultants

This assessment provides CloudSync Technologies with a comprehensive understanding of their current security posture and a clear path to ISO 27001:2022 certification. With committed leadership, appropriate resource allocation, and disciplined execution, certification is achievable within the proposed 9-12 month timeline.