



CONSULTING ADVISORY REPORT

Cybersecurity Governance, Risk & Compliance Assessment

Strategic Framework for ISO 27001 Certification and SOC 2 Readiness

Mustafa Alobaidy

Cybersecurity Governance, Risk & Compliance Specialist

Prepared for: CloudVault Technologies Inc.

March 5, 2026

CONFIDENTIAL — FOR INTERNAL USE
ONLY

Table of Contents

1	Executive Summary	3
2	Organizational Context	3
3	Risk Assessment Methodology	4
4	Risk Register	4
5	Security Maturity Assessment	5
6	Control Mapping Across Frameworks	6
7	Key Security Controls	6
8	Governance Structure	7
9	12-Month Compliance Roadmap	7
10	Conclusion	8

1 Executive Summary

This Governance, Risk, and Compliance (GRC) assessment has been conducted for **CloudVault Technologies Inc.**, a mid-sized SaaS organization seeking to establish a comprehensive security program aligned with industry-leading frameworks. The assessment evaluates the organization's current security posture and provides a strategic roadmap toward achieving ISO 27001 certification and SOC 2 Type II readiness.

Key Findings:

- Current security maturity level is assessed at **Developing** across most NIST CSF functions
- Critical gaps identified in access management, vendor oversight, and incident response capabilities
- Significant compliance exposure exists regarding GDPR and PCI-DSS requirements
- Strong foundation exists in cloud infrastructure security, requiring formalization and documentation

The organization faces increasing pressure from enterprise customers demanding evidence of robust security controls and compliance certifications. A structured GRC program is essential to systematically address identified risks, demonstrate regulatory compliance, and build competitive advantage through verified security assurances.

Strategic Objectives:

- Achieve ISO 27001:2022 certification within 12 months
- Attain SOC 2 Type II readiness for enterprise customer requirements
- Establish continuous compliance monitoring and risk management processes
- Reduce overall cybersecurity risk exposure by implementing prioritized controls

2 Organizational Context

2.1 Company Profile

CloudVault Technologies Inc. is a B2B SaaS company providing cloud-based document management and collaboration solutions. Founded in 2019, the organization has experienced rapid growth and currently serves over 2,500 business customers across North America and Europe.

Attribute	Description
Industry	Cloud Software / SaaS
Employees	185 full-time employees across 3 locations
Cloud Infrastructure	Multi-cloud environment (AWS primary, Azure secondary)
Data Processing	Customer PII, business documents, payment information
Geographic Scope	North America, European Union (UK, Germany, France)
Annual Revenue	\$28M ARR (2025)

2.2 Compliance Drivers

Several business and regulatory factors necessitate a formalized GRC program:

- **GDPR Compliance:** Processing personal data of EU residents requires adherence to data protection principles, including lawful basis for processing, data subject rights, and cross-border transfer safeguards.
- **PCI-DSS Requirements:** Integration with payment processors and handling of cardholder data necessitates compliance with Payment Card Industry standards.
- **Enterprise Customer Demands:** Fortune 500 prospects require ISO 27001 certification and SOC 2 reports as prerequisites for vendor approval.
- **Cyber Insurance Requirements:** Insurers mandate demonstrated security controls for policy eligibility and favorable premium rates.

3

Risk Assessment Methodology

The risk assessment methodology employed in this engagement aligns with **ISO 27005:2022** (Information Security Risk Management) and **NIST SP 800-30** (Guide for Conducting Risk Assessments). This approach ensures systematic identification, analysis, and evaluation of information security risks.

3.1 Methodology Components

Asset Identification

Critical assets were inventoried across categories including information assets (customer data, intellectual property), technology assets (cloud infrastructure, applications), and human assets (key personnel, third-party relationships).

Threat Identification

Threat sources were identified through analysis of industry threat intelligence, historical incident data, and organizational context. Sources include external actors (cybercriminals, nation-states), internal threats (malicious insiders, negligent employees), and environmental factors.

Vulnerability Assessment

Vulnerabilities were assessed through technical scanning, configuration reviews, policy gap analysis, and interviews with key stakeholders. Both technical and procedural weaknesses were documented.

3.2 Risk Scoring Matrix

Likelihood / Impact	Negligible (1)	Minor (2)	Moderate (3)	Major (4)	Severe (5)
Almost Certain (5)	Medium	Medium	High	Critical	Critical
Likely (4)	Low	Medium	High	High	Critical
Possible (3)	Low	Medium	Medium	High	High
Unlikely (2)	Low	Low	Medium	Medium	High
Rare (1)	Low	Low	Low	Medium	Medium

4

Risk Register

The following risk register documents identified cybersecurity risks, their assessment, and recommended mitigation controls. Risks are prioritized based on their calculated risk rating to guide remediation efforts.

Risk ID	Asset	Threat	Vulnerability	Impact	Likelihood	Rating	Recommended Mitigation Controls
R-001	Customer Database	Unauthorized access by external attacker	Weak authentication mechanisms; lack of MFA	Severe (5)	Likely (4)	Critical	Implement MFA for all privileged access; deploy PAM solution; enhance monitoring
R-002	AWS Cloud Infrastructure	Cloud misconfiguration leading to data exposure	Inconsistent IaC practices; lack of CSPM tools	Major (4)	Possible (3)	High	Deploy CSPM solution; implement IaC scanning; establish configuration baselines
R-003	Third-Party Integrations	Supply chain compromise through vendor	Insufficient vendor security assessments	Major (4)	Possible (3)	High	Implement vendor risk management program; require SOC 2 reports; contractual security requirements
R-004	Employee Workstations	Phishing attack compromising credentials	Limited security awareness; no email security gateway	Moderate (3)	Almost Certain (5)	High	Deploy email security gateway; implement phishing simulations; mandatory security training

R-005	Intellectual Property	Data exfiltration by malicious insider	Excessive access privileges; limited DLP controls	Major (4)	Unlikely (2)	Medium	Implement principle of least privilege; deploy DLP solution; enhance access logging
R-006	Customer PII	GDPR non-compliance penalty	Incomplete data inventory; unclear lawful basis documentation	Severe (5)	Possible (3)	High	Conduct data mapping exercise; document lawful basis; implement DSAR process

5 Security Maturity Assessment

The security maturity assessment evaluates CloudVault's capabilities against the **NIST Cybersecurity Framework (CSF)** five core functions. Maturity levels range from Initial (ad-hoc) to Optimized (continuous improvement).

NIST Function	Current Maturity	Key Gaps Identified	Recommended Improvements
IDENTIFY <i>Asset Management, Risk Assessment, Governance</i>	Developing	Incomplete asset inventory; informal risk assessment processes; governance structure undefined	Deploy CMDB solution; establish formal risk assessment schedule; define security governance committee
PROTECT <i>Access Control, Awareness Training, Data Security</i>	Developing	MFA not enforced universally; security training ad-hoc; encryption standards inconsistent	Mandate MFA organization-wide; implement structured awareness program; standardize encryption practices
DETECT <i>Continuous Monitoring, Detection Processes</i>	Initial	Limited SIEM coverage; no 24/7 monitoring; detection rules not optimized	Expand SIEM deployment; establish SOC capability (internal or MDR); tune detection use cases
RESPOND <i>Response Planning, Communications, Mitigation</i>	Initial	Incident response plan outdated; no regular tabletop exercises; unclear escalation paths	Update IRP documentation; conduct quarterly exercises; define RACI for incident handling
RECOVER <i>Recovery Planning, Improvements, Communications</i>	Developing	BCP/DR plans exist but untested; recovery objectives undefined; lessons learned not formalized	Define RTO/RPO targets; conduct annual DR tests; implement post-incident review process

Path to Compliance: Improving maturity from "Developing" to "Defined" or higher across all functions will directly support ISO 27001 Annex A control requirements, satisfy SOC 2 Trust Service Criteria, and establish the foundation for continuous security improvement essential to maintaining certifications.

6

Control Mapping Across Frameworks

The following control mapping demonstrates how implementing key security controls simultaneously satisfies requirements across multiple compliance frameworks, enabling efficient multi-framework compliance.

Security Control	ISO 27001:2022	NIST CSF	SOC 2 TSC	GDPR
Multi-Factor Authentication (MFA)	A.8.5 Secure Authentication	PR.AC-7	CC6.1	Art. 32 (Security)
Access Control Policy	A.5.15 Access Control	PR.AC-1, PR.AC-4	CC6.1, CC6.2, CC6.3	Art. 25 (Data Protection by Design)
Security Awareness Training	A.6.3 Information Security Awareness	PR.AT-1	CC1.4, CC2.2	Art. 39(1)(b) (DPO Training)
Incident Response Plan	A.5.24-A.5.28 Incident Management	RS.RP-1, RS.CO-1	CC7.3, CC7.4, CC7.5	Art. 33, 34 (Breach Notification)
Logging and Monitoring	A.8.15 Logging, A.8.16 Monitoring	DE.CM-1, DE.CM-7	CC7.1, CC7.2	Art. 30 (Records of Processing)
Vendor Risk Management	A.5.19-A.5.22 Supplier Relationships	ID.SC-1, ID.SC-2	CC9.2	Art. 28 (Processor Requirements)

7

Key Security Controls

7.1 Identity & Access Management

Implement Role-Based Access Control (RBAC) with clearly defined roles mapped to job functions. Enforce Multi-Factor Authentication (MFA) for all system access, prioritizing privileged accounts. Deploy Privileged Access Management (PAM) for administrative credentials with session recording and just-in-time access provisioning.

7.2 Security Monitoring & Detection

Establish centralized logging infrastructure aggregating events from cloud workloads, endpoints, network devices, and applications. Deploy a Security Information and Event

Management (SIEM) platform with detection rules aligned to the MITRE ATT&CK framework. Consider Managed Detection and Response (MDR) services for 24/7 monitoring capability.

7.3 Vendor Risk Management

Develop a formal vendor risk assessment program requiring security questionnaires, SOC 2 reports, or equivalent certifications from critical vendors. Establish contractual security requirements including data protection addenda and right-to-audit clauses. Conduct periodic reassessments based on vendor criticality tiers.

7.4 Security Awareness Program

Implement comprehensive security awareness training for all employees with role-specific modules for developers, administrators, and executives. Conduct regular phishing simulations with progressive difficulty. Track completion rates and simulation results as security metrics.

7.5 Incident Response Capability

Develop and maintain incident response playbooks for common scenarios including ransomware, data breach, and insider threat. Define clear escalation procedures with designated incident commanders. Conduct quarterly tabletop exercises and annual technical simulations. Establish relationships with external IR retainer services.

8

Governance Structure

Effective security governance requires clear accountability, defined responsibilities, and independent assurance. The **Three Lines Model** (formerly Three Lines of Defence) provides a framework for structuring governance roles.



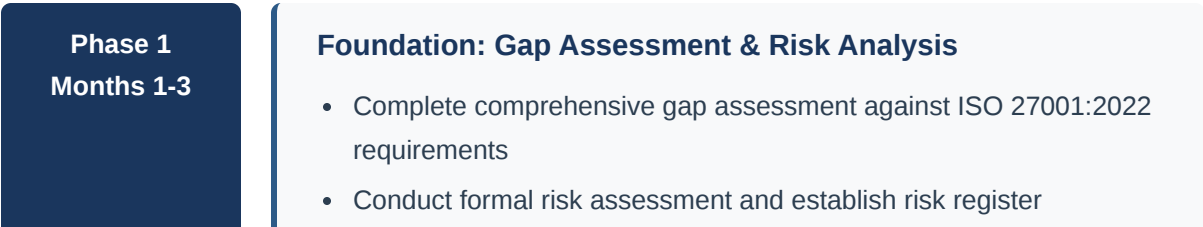
8.1 Recommended Governance Bodies

- **Security Steering Committee:** Executive-level oversight meeting quarterly to review risk posture, approve policies, and allocate resources.
- **Risk Management Committee:** Operational committee meeting monthly to review risk register, track remediation, and assess emerging threats.
- **Change Advisory Board:** Technical committee reviewing security implications of infrastructure and application changes.

9

12-Month Compliance Roadmap

The following roadmap outlines key activities and milestones to achieve ISO 27001 certification and SOC 2 Type II readiness within 12 months.



- Define ISMS scope and Statement of Applicability
- Establish security governance structure and committees
- Develop project plan with resource allocation

Phase 2 Months 3-6

Build: Policy Development & Control Implementation

- Develop and approve information security policies
- Implement priority controls addressing critical and high risks
- Deploy MFA and PAM solutions organization-wide
- Establish vendor risk management program
- Launch security awareness training program
- Document procedures and work instructions

Phase 3 Months 6-9

Verify: Internal Audits & Control Testing

- Conduct internal ISMS audit against ISO 27001 requirements
- Perform SOC 2 readiness assessment
- Execute penetration testing and vulnerability assessments
- Conduct incident response tabletop exercises
- Address audit findings and implement corrective actions
- Collect evidence demonstrating control effectiveness

Phase 4 Months 9-12

Certify: External Audit Preparation & Certification

- Conduct management review of ISMS
- Finalize documentation and evidence packages
- Engage certification body for ISO 27001 Stage 1 audit
- Address any non-conformities from Stage 1
- Complete ISO 27001 Stage 2 certification audit
- Initiate SOC 2 Type II audit period

10

Conclusion

The implementation of a structured Governance, Risk, and Compliance program represents a strategic investment in CloudVault Technologies' security posture and business sustainability. This assessment has identified clear improvement opportunities and provided a practical roadmap toward achieving compliance objectives.

Expected Outcomes

Benefit Area	Expected Improvements
Risk Management	Systematic identification, assessment, and treatment of cybersecurity risks. Reduced likelihood and impact of security incidents through proactive controls. Informed decision-making through quantified risk visibility.
Regulatory Compliance	Demonstrated compliance with GDPR, PCI-DSS, and contractual security requirements. Reduced regulatory exposure and potential penalties. Efficient multi-framework compliance through control harmonization.
Operational Resilience	Enhanced ability to detect, respond to, and recover from security incidents. Documented procedures ensuring consistent security operations. Reduced business disruption through tested continuity plans.
Customer Trust	ISO 27001 certification and SOC 2 reports provide verifiable security assurance. Competitive differentiation in enterprise sales cycles. Foundation for secure growth and market expansion.

Next Steps: To initiate the compliance program, CloudVault Technologies should formally approve the roadmap, allocate necessary resources, and establish the security steering committee within the next 30 days. The consulting team is available to support Phase 1 gap assessment activities and provide ongoing advisory services throughout the certification journey.

This document is intended for authorized recipients only. Distribution without prior approval is prohibited.

Prepared by:
Mustafa Alobaidy
Cybersecurity Governance, Risk & Compliance Specialist
March 5, 2026