Comprehensive GRC Strategy Report

Prepared by: Michael Jordan
Date: 6-30-2025

Section 1: Governance Policies

1.1 Policy Framework

- Data Protection Policy
- Vendor Management Policy
- Access Control Policy
- Incident Response Policy

1.2 Roles and Responsibilities

- Data Protection Officer: Privacy Officer (Ensures compliance with data protection laws, GDPR).
- Incident Response Lead: IT Security Officer (Manages and coordinates incident response activities).
- Compliance Officer: Existing compliance staff or an External Consultant (Oversees policy development and adherence).

1.3 Escalation Paths

- Level 1: On-call IT Support
- Level 2: Compliance Manager
- Level 3: Executive Leadership

Section 2: Risk Assessment Findings

2.1 Key Risks Identified

Risk	Likelihood	Impact	Priority
Data Breaches (Encryption gaps)	High	High	High
Third-Party Vendor Risks	Moderate	High	High

Non-compliance Penalties	Moderate	Moderate	Moderate
Incident Response Gaps	High	High	High

2.2 Risk Details and Mitigation Steps

Risk	Details	Mitigation Steps
Data Breaches (Encryption gaps)	Cardholder data is currently protected using outdated encryption protocols, increasing vulnerability to unauthorized access.	Upgrade to modern encryption standards and implement a Hardware Security Module (HSM) to securely manage and rotate encryption keys.
Third-Party Vendor Risks	The current cloud storage provider does not hold a SOC 2 certification, posing compliance and data security concerns.	Require the vendor to obtain SOC 2 compliance or migrate to a vendor with appropriate certifications and security assurances.
Non-compliance Penalties	Data Protection Impact Assessments (DPIAs) are incomplete, and responses to CCPA requests are delayed, risking regulatory fines.	Automate DPIA documentation and streamline privacy request handling through workflow tools to ensure timely and consistent compliance.
Incident Response Gaps	Lack of recent incident response drills and reliance on email delays threat detection and containment.	Conduct regular tabletop exercises and deploy a centralized ticketing system to enable real-time incident reporting and faster response coordination.

Section 3: Compliance Roadmap

3.1 Immediate Actions (0–3 Months)

- Strengthen data security by upgrading encryption standards and rotating cryptographic keys using a Hardware Security Module (HSM).

- Secure privileged access by implementing multi-factor authentication (MFA) for all administrative accounts.
- Initiate a detailed vendor risk evaluation to uncover and mitigate existing compliance vulnerabilities.

3.2 Mid-Term Goals (3–6 Months)

- Streamline compliance by automating the processing of CCPA data privacy requests to reduce delays and improve response accuracy.
- Enhance incident readiness by organizing quarterly tabletop simulations to test and refine response procedures.
- Complete GDPR-compliant Data Protection Impact Assessments (DPIAs) for processing activities that present elevated privacy risks.

3.3 Long-Term Objectives (6–12 Months)

- Deploy continuous compliance monitoring tools to support proactive adherence to PCI DSS requirements.
- Build a centralized system for ongoing oversight and management of vendor-related risks.
- Implement periodic SOC 2 certification assessments for all key third-party vendors.

Section 4: Incident Response Plan

4.1 Roles and Responsibilities During Incidents

- Incident Commander: Compliance Manager
- Forensics Lead: IT Security Officer
- Communications Lead: Public Relations Team

4.2 Reporting and Escalation Steps

- Real-time reporting system: Incident ticketing software with escalation alerts.
- Timeline: Notify affected parties and regulators within 72 hours.

4.3 Testing Schedule

- Tabletop Exercises: Biannual (next one scheduled for 12-31-2025).
- Live Drills: Annual (next one scheduled for 6-30-2026).

Section 5: Executive Summary

5.1 Key Highlights

- The incident response plan is documented but remains untested and not fully integrated into operational procedures, limiting the organization's ability to respond effectively to security events.
- Current encryption key management practices fall short of PCI DSS requirements, significantly heightening the risk of unauthorized data access.
- Gaps in GDPR and CCPA compliance were identified, particularly in the automation and timely handling of data subject requests.
- The use of cloud storage providers without SOC 2 certification increases the organization's exposure to third-party security and compliance risks.

5.2 Overall Compliance Posture

- DataServe Solutions is progressing toward compliance with PCI DSS, GDPR, and CCPA. However, immediate remediation is needed around encryption key management, third-party vendor assessments, and privacy automation. If actions outlined in this report are executed within the next 6-12 months, full compliance is achievable.