GRC Strategy Proposal for SecureTech Solutions

Prepared by: Michael Jordan
Date: 6-30-25

1. Key Takeaways

Throughout this project, I've gained hands-on experience in evaluating governance structures, identifying and prioritizing risks, and aligning compliance efforts with industry standards such as ISO 27001, PCI DSS, GDPR, and CCPA. I conducted gap assessments across access control, backups, and incident response, and developed realistic mitigation plans. I also learned the importance of tying technical gaps to broader business risks, such as reputational damage, legal penalties, and operational disruptions. This experience has equipped me to develop a proactive GRC strategy that balances security needs with business goals.

2. Forward-Looking GRC Strategy

Strategic Priority 1: Strengthening Data Protection and Encryption Practices

Rationale:
As SecureTech handles sensitive cardholder and customer data, weaknesses in encryption and key management significantly increase the risk of data breaches and non-compliance with PCI DSS.

Recommendations:

- Migrate encryption keys to a secure Hardware Security Module (HSM) or Key Management System (KMS).
- Implement automated alerts for unauthorized access to encryption keys.
- Conduct semi-annual encryption audits to ensure ongoing compliance.

Timeline: 3 months

Strategic Priority 2: Enhancing Third-Party Vendor Risk Management

Rationale:
Vendors with inadequate security controls introduce significant risks, especially when storing or processing regulated data. A lack of SOC 2 or ISO 27001 certification is a red flag.

Recommendations:

- Conduct formal vendor risk assessments using SIG Lite or a similar framework.
- Require security certifications or equivalent evidence for critical third-party vendors.
- Include cybersecurity clauses and exit strategies in all vendor contracts.

Timeline: 4 months

Strategic Priority 3: Operationalizing Incident Response Readiness

Rationale:
An untested incident response plan leaves SecureTech vulnerable to delayed or ineffective breach response, potentially amplifying compliance penalties and reputational harm.

Recommendations:

- Assign formal incident response roles and create an escalation matrix.
- Schedule biannual tabletop exercises and one annual live drill.
- Deploy a real-time incident reporting and tracking system**.**

Timeline: 2 months

3. Implementation Plan

Strategic Area	Actions	Timeline	Resources Needed
Data Protection & Encryption	● Migrate keys to HSM/KMS ● Set up access alerts ● Perform encryption audit	0–3 months	HSM/KMS solution, IT Security Team, Audit Tools
Vendor Risk Management	● Perform vendor assessments ● Require SOC 2/ISO 27001	0–4 months	Legal team, GRC tools (e.g., OneTrust), Compliance Lead

	● Update contracts with security terms		
Incident Response Readiness	● Assign roles ● Schedule drills ● Deploy ticketing/alerting system	0–2 months	IR Plan, Ticketing Software, IR Team, Training Resources

4. Methods to Track Progress

Progress will be tracked using a combination of the following methods:

- **Key Performance Indicators (KPIs):** % of vendors assessed, number of IR drills conducted, compliance audit scores.
- **Dashboards:** GRC dashboards displaying real-time risk levels and control statuses.
- **Audit Reports:** Internal audit results for encryption, vendor due diligence, and incident response.
- **Surveys:** Employee feedback surveys post tabletop exercises to assess awareness and readiness.

5. Conclusion

This GRC strategy is designed to close critical compliance gaps while preparing SecureTech for long-term resilience. By enhancing encryption, vendor oversight, and incident response, SecureTech can strengthen its security posture, reduce regulatory exposure, and build trust with clients and regulators. Over the next 12 months, this roadmap will position SecureTech for strong alignment with PCI DSS, ISO 27001, GDPR, and CCPA standards—ensuring a proactive and sustainable GRC program.