Cybersecurity Compliance Gap Assessment & Remediation Plan

Date: June 13, 2025

# Executive Summary

This document provides an evaluation of current cybersecurity and compliance controls based on NIST Cybersecurity Framework (NIST CSF), PCI DSS, and GDPR. Key deficiencies have been identified, prioritized by risk level, and addressed with recommended timelines and estimated cost implications of non-remediation.

# High Priority Remediations (0–3 Months)

|  |  |  |  |
| --- | --- | --- | --- |
| Control | Risk / Why Fix | Timeline | Cost of Not Fixing |
| Least Privilege | Violates NIST ID.AM-3, increases attack surface | 1 month | $4.45M+ (data breach risk) |
| Password Policy | Violates NIST PR.AC-1, PCI DSS 8 | 1 month | Credential theft, compliance fines |
| Password Management System | No centralized control, poor hygiene | 2 months | Shadow IT exposure |
| Disaster Recovery Plan | Violates NIST PR.IP-9, PCI 12.10 | 2 months | $5,600/min downtime |
| Encryption | PCI DSS 3, GDPR Article 32 | 2 months | Data theft, €20M fines |
| Intrusion Detection System | NIST DE.CM-1, PCI DSS 11.4 | 3 months | Unknown breaches |
| Backups | NIST PR.IP-4, PCI DSS 9.5 | 2 months | Data unrecoverable after ransomware |
| Firewall | PCI DSS 1, NIST PR.AC-5 | 1 month | External attack entry point |
| Access Control for Credit Card Data | PCI DSS 7 | 1 month | Legal penalties |
| Credit Card Data Storage | PCI DSS 3–4 | 1 month | Breach liabilities |
| EU Breach Notification Plan | GDPR Article 33 | 3 months | €10–20M GDPR fine |

# Medium Priority Remediations (3–6 Months)

Controls that impact governance, data quality, and access management but have less immediate exposure.

# Low Priority Remediations (6–12 Months)

Long-term improvements focused on physical security, environmental safety, and secondary availability controls.

# Cumulative Cost of Inaction

- Regulatory fines (PCI + GDPR): $11M–$25M  
- Operational downtime: $50K–$1M  
- Breach recovery costs: $4.45M average  
- Reputational damage: Intangible but long-lasting

# Conclusion

The organization must immediately address high-risk security gaps to meet baseline compliance standards and prevent financial, legal, and operational losses. Implementation of the outlined plan should begin within the next 30 days.