Gap Analysis Report

Prepared for:
Prepared by: Alexis Collier
Date: January 28, 2025

Executive Summary

This Gap Analysis Report identifies security vulnerabilities and deficiencies in current security posture. The analysis is aligned with the NIST 800-53 framework and highlights areas where security controls are insufficient or missing. The report also provides structured recommendations to mitigate risks, improve compliance, and enhance security resilience.

Identified Gaps

The following gaps were identified based on the current state of security controls compared to NIST 800-53 requirements:

1. Physical Security *(Aligned with NIST PE-3, PE-6)*

- Unsecured Equipment Storage: Laptops and servers are stored in rooms with broken or weak locks.
- Weak Physical Access Controls: Inconsistent visitor logging and escort policies.
- Surveillance Gaps: Cameras are installed but not actively monitored or verified for recording reliability.

2. Cybersecurity *(Aligned with NIST SI-4, SC-12, AC-3)*

- No Penetration Testing: Lack of vulnerability assessments increases exposure to cyber threats.
- Unsegmented Network: Public, staff, and administrative systems share the same network.
- Weak Email Security: Lack of DMARC, SPF, and DKIM, leaving users vulnerable to phishing attacks.

3. Incident Response & Monitoring *(Aligned with NIST IR-8, SI-4, AU-6)*

- No Documented Incident Response Plan (IRP): No structured response plan to mitigate security threats.
- Single Point of Failure: Incident response relies on a single person, increasing operational risks.
- Limited Logging & Monitoring: No centralized SIEM (Security Information and Event Management) system for real-time threat detection.

4. Access Control *(Aligned with NIST AC-5, AC-6)*

- No Role-Based Access Control (RBAC): Access is granted informally without a structured framework.
- No Multi-Factor Authentication (MFA): Critical systems lack MFA protections.
- Weak Server Room Security: The basement server room is accessible via broader building access permissions.

5. Policy & Compliance *(Aligned with NIST PM-9, RA-3)*

- Absence of Formal Policies: No documented Access Control, Incident Response, or Asset Management policies.

- No Compliance Strategy: Aspirational NIST compliance goals for 2025 lack a concrete implementation roadmap.
- Lack of Security Audits: No third-party assessments to validate security posture.

6. Security Awareness Training *(Aligned with NIST AT-2, AT-3)*

- No Formal Security Awareness Training: Employees are not consistently trained on phishing, ransomware, or insider threats.
- No Simulated Security Exercises: No phishing simulations or tabletop exercises to test staff readiness.

Recommendations

1. Strengthen Physical Security *(PE-3, PE-6)*

- Secure Equipment Storage:
    - Install electronic keycard locks and replace hollow doors with reinforced steel doors.
    - Require visitor escorts at all times in sensitive areas.
- Improve Visitor Management:
    - Implement a visitor logging system with badge issuance.
    - Restrict visitor movement through controlled access.
- Enhance Surveillance:
    - Install motion-detection cameras in critical locations.
    - Verify camera recording retention policies to ensure footage is stored and reviewed.

2. Improve Cybersecurity Posture *(SI-4, SC-12, AC-3)*

- Conduct Vulnerability Assessments:
    - Perform quarterly penetration testing to identify security weaknesses.
    - Maintain an updated network/system diagram to track critical assets.
- Segment the Network:
    - Separate public, staff, and administrative systems using Virtual LANs (VLANs).
    - Restrict communication between segments to limit lateral movement risks.
- Enhance Email Security:
    - Implement DMARC, SPF, and DKIM to prevent spoofing attacks.
    - Deploy email filtering solutions to block phishing attempts.

3. Develop a Comprehensive Incident Response Plan (IRP) *(IR-8, AU-6)*

- Document a Formal IRP:
    - Define roles, responsibilities, and escalation procedures.
    - Create a communication plan for internal & external incident reporting.
- Train Backup Incident Responders:
    - Ensure at least two additional staff members are trained in handling security incidents.
- Conduct Regular Incident Simulations:
    - Perform quarterly tabletop exercises to validate the effectiveness of the IRP.
- Deploy Real-Time Security Monitoring:
    - Implement an SIEM (Security Information and Event Management) system for real-time log correlation and threat detection.

4. Strengthen Access Control *(AC-5, AC-6)*

- Enforce Multi-Factor Authentication (MFA):
    - Require MFA for access to all critical systems and privileged accounts.
- Implement Role-Based Access Control (RBAC):
    - Define user roles and least-privilege principles.
    - Conduct quarterly access reviews to remove unnecessary permissions.
- Secure Server Rooms:
    - Require biometric or PIN-based access to server areas.
    - Deploy door sensors & audit logs to track entry attempts.

5. Establish Policy & Compliance Framework *(PM-9, RA-3)*

- Develop & Implement Security Policies:
    - Draft formal Access Control, Incident Response, and Asset Management Policies. ○ Require employees to sign policy acknowledgment forms.
- Align Compliance with NIST 800-53:
    - Establish a roadmap to meet NIST 800-53 controls by 2025, prioritizing high-impact areas. • Schedule Third-Party Security Audits:
    - Conduct annual security assessments to verify compliance.

6. Enhance Security Awareness Training *(AT-2, AT-3)*

- Launch Quarterly Security Awareness Training:
    - Focus on phishing, social engineering, insider threats, and ransomware response. • Conduct Simulated Phishing Attacks:
    - Test employee readiness with realistic phishing simulations.
- Require Executive Cybersecurity Training:
    - Train senior leadership on cybersecurity risks & compliance requirements.

Conclusion

faces significant security and compliance risks due to physical security gaps, weak access controls, lack of incident response preparedness, and cybersecurity vulnerabilities.

By implementing these recommendations, will:

- Enhance Security & Resilience through stricter access controls & monitoring.
- Mitigate Compliance Risks by aligning with NIST 800-53 standards.
- Improve Incident Readiness through structured IRP & security awareness training.