Memorandum

**To:** IT Manager, Stakeholders

**From:** Samuel Hendrix

**Date:** 1/19/2024

**Subject:** Internal IT Audit Findings and Recommendations

Dear Colleagues,

I trust that this memorandum finds you well. Please find below the outcomes of the recent internal IT audit conducted at XYZ Financial Services, outlining the audit scope, goals, critical findings, and recommendations for immediate attention.

**Scope:**

The audit focused on the following systems:

* Accounting
* Endpoint Detection
* Firewalls
* Intrusion Detection System
* SIEM Tool

Evaluation Criteria:

1. Current user permissions
2. Implemented controls
3. Procedures and protocols

Objective:

* Ensure alignment with PCI DSS and GDPR compliance requirements.
* Account for both hardware and system access.

**Goals:**

1. Adhere to the NIST CSF.
2. Establish a compliant process for systems.
3. Fortify system controls.
4. Implement the concept of least permissions for user credential management.
5. Develop and establish policies, including playbooks.
6. Ensure compliance requirements are met.

**Critical Findings (Immediate Attention):**

Multiple controls need development and implementation to meet audit goals:

* Control of Least Privilege and Separation of Duties
* Disaster recovery plans
* Password, access control, and account management policies
* Encryption (for secure website transactions)
* IDS, Backups, AV software
* CCTV, Locks
* Manual monitoring, maintenance, and intervention for legacy systems
* Fire detection and prevention systems

Policies must be developed and implemented to meet PCI DSS, GDPR, SOC1, and SOC2 compliance requirements.

**Findings (Address in Due Course):**

* Time-controlled safe
* Adequate lighting
* Locking cabinets
* Signage indicating alarm service provider

**Summary/Recommendations:**

Immediate attention is required for critical findings related to PCI DSS and GDPR compliance, given XYZ Financial Services' role in the financial industry. Additionally:

* Adapt to the least permissions concept using SOC1 and SOC2 guidance.
* Develop disaster recovery plans and backups for business continuity.
* Integrate IDS and AV software for risk identification and mitigation.
* Secure physical assets with locks and CCTV.

While not immediate, consider implementing encryption, time-controlled safe, adequate lighting, locking cabinets, fire detection and prevention systems, and signage for further security enhancements.

Thank you for your attention to these critical matters.