# Stakeholder Memorandum

TO: IT Manager, Stakeholders

FROM: Arik Schroetlin  
DATE: July 31, 2023  
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Company’s internal audit scope, goals, critical findings, summary and recommendations.

**Scope:**

This assessment looked at the current user permissions, current implemented controls, and current procedures and protocols for the following systems:

* Accounting
* End point detection
* Firewalls
* Intrusion Detection Systems
* SIEM tools

Additionally, compliance with PCI DSS and GDPR policies was investigated. Lastly, having all current technology accounted for was assessed.

**Goals:**

* To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
* Establish a better process for their systems to ensure they are compliant
* Fortify system controls
* Implement the concept of least permissions when it comes to user credential management
* Establish their policies and procedures, which includes their playbooks
* Ensure they are meeting compliance requirements

**Critical findings** (must be addressed immediately):

The following controls need to be implemented to achieve the company’s goals:

* Least Privilege
* Disaster recovery plans
* Password policies
* Access control policies
* Account management policies
* Separation of duties
* Intrusion Detection System
* Encryption
* Backups
* Password management system
* Antivirus software
* Manual monitoring, maintenance, and intervention
* CCTV surveillance
* Locks
* Fire detection and preventation

Further, policies need to be implemented to adhere to PCI DSS and GDPR requirements and additional policies will be required for following SOC1 and SOC2 guidance.

**Findings** (should be addressed, but no immediate need):

The following controls will also need to be added:

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

**Summary/Recommendations:**

It is recommended that the controls found in the critical findings section be implemented immediately to ensure PCI DSS and GDPR compliance. Once these controls are implemented, the controls in the findings section can be implemented to further improve the company’s security posture.