# Stakeholder memorandum

TO: IT Manager, Stakeholders

FROM: Ignacio René  
DATE: 01/08/2023  
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, summary and recommendations.

**Scope:**

* The following systems are in scope: accounting, end point detection, firewalls,
* intrusion detection system, SIEM tool. The systems will be evaluated for:
  + Current user permissions
  + Current implemented controls
  + Current procedures and protocols
* Ensure current user permissions, controls, procedures, and protocols in place
* align with PCI DSS and GDPR compliance requirements.
* Ensure current technology is accounted for both hardware and system access.

**Goals:**

* Adhere to the NIST CSF.
* Establish a better process for their systems to ensure they are compliant.
* Fortify system controls.
* Adapt to 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 needs to be implemented to meet the audit goals:
  + Control of Least Privilege and Separation of Duties
  + Disaster recovery plans
  + Password, access control, and account management policies, including
  + the implementation of a password management system
  + Encryption (for secure website transactions)
  + IDS
  + Backups
  + CCTV
  + Locks
  + Manual monitoring, maintenance, and intervention for legacy systems
  + Fire detection and prevention systems
* The company needs to develop policies to meet the following compliance:
  + GDPR
  + PCI DSS
* The company needs to develop and apply the following guidelines related to user access, and data safety:
  + SOC 1 and SOC 2

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

* The following controls should be implemented when possible:
  + Time-controlled safe
  + Adequate lighting
  + Locking cabinets
  + Signage indicating alarm service provider

**Summary/Recommendations:**

We propose implementing essential policies to ensure compliance with GDPR and PCI DSS regulations, considering our global operations and the processing of customer credit card information. Adopting guidelines from SOC 1 and SOC 2 will enhance data security and access controls. By integrating Least Privilege and Separation of Duties principles, along with robust recovery plans and other specified controls, we can effectively minimize the risk of data loss and safeguard valuable company assets currently vulnerable to potential threats.