# Stakeholder Memorandum

TO: IT Manager, stakeholders

FROM: Cristian Rodriguez Sakas  
DATE: (Today’s Date)  
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 National Institute of Standards and Technology Cybersecurity Framework.
* 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):

* Multiple controls need to be implemented to meet the audit goals, including but not limited to:
  + 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
  + Intrusion Detection System
  + Backups
  + Antivirus (AV) software
  + Closed-Circuit Television (CCTV) surveillance
  + Locks
  + Manual monitoring, maintenance, and intervention for legacy systems
* Policies need to be developed and implemented to meet PCI DSS and GDPR compliance requirements.
* Policies need to be developed and implemented to align to SOC1 and SOC2 guidance related to user access policies and overall data safety.

**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:**

Prompt action should be taken into action and address critical findings related to PCI DSS and GDPR compliance, as Botium Toys processes online payments from customers worldwide, including the European Union. Moreover, to align with the principle of least permissions, it is advised to refer to SOC1 and SOC2 guidelines concerning user access policies and overall data safety in order to establish suitable procedures and policies. There are high priority implementations that should be taken into consideration urgently, such as maintaining disaster recovery plans and backups is crucial to ensure uninterrupted business operations during incidents. Enhancing the current systems with an Intrusion Detection System (IDS) and antivirus software will aid in identifying and mitigating potential risks, especially considering the manual monitoring and intervention required by existing legacy systems. Safeguarding physical assets and enhancing security at Botium Toys' single location can be achieved through the use of locks, CCTV surveillance, and thorough investigation of potential threats. Although not immediately necessary, in the future there should be more additional measures taken such as encryption, time-controlled safes, proper lighting, locked cabinets, fire detection and prevention systems, and clear signage indicating the alarm service provider will further enhance Botium Toys' overall security posture.