# Stakeholder memorandum

TO: IT Manager, Stakeholders

FROM: Nick Hodge  
DATE: 8/16/2023  
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:**

* Accounting, end point detection, firewalls, intrusion detection systems, and SIEM tools are included in the scope. The systems will be assessed in terms of:
  + Users' current permissions
  + Users’ current implemented controls
  + Users’ current procedures and protocols
* Verify that the user permissions, controls, processes, and protocols currently in use comply with PCI DSS and GDPR compliance standards.
* Be mindful to consider current hardware and system access technology.

**Goals:**

* Improve the systems' processes to make sure they are compliant.
* Align the organization with the NIST CSF framework.
* Accept the principle of least privilege when it comes to managing user credentials.
* Strengthen the system controls.
* Verify the organization is meeting compliance requirements.
* Establish the playbooks and the organization's policies and procedures.

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

* To achieve the audit objectives, several controls must be created and put into place, including:
  + Control of least privilege and separation of duties.
  + Disaster recovery plans.
  + Policies for managing passwords, accounts, and access controls, including the use of a password management system.
  + Encryption (for use in safe website transactions).
  + Backups
  + Intrusion Detection System (IDS)
  + Anti-Virus software
  + CCTV
  + Locks
  + Monitoring, upkeep, and intervention manually for legacy systems.
  + Fire detection and prevention systems.
* To achieve the criteria of PCI DSS and GDPR compliance, policies must be created and put into place.
* To align with SOC1 and SOC2 recommendations regarding user access policies and overall data safety, policies must be designed and put into place.

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

* When practical, the following controls should be implemented:
  + Locking cabinets
  + Time-controlled safe
  + Adequate lighting
  + Signage indicating alarm service provider.

**Summary/Recommendations:**

Following a comprehensive analysis of Botium Toys' IT framework, it is crucial to swiftly implement the above recommendations to prevent potential cyber threats, especially given the storage of customer financial data in alignment with the PCI DSS. Ignoring these changes risks breaches that would violate this standard. Additionally, as the company intends to operate in Europe, any data breach would necessitate informing European customers within 72 hours, per the General Data Protection Regulation (GDPR). Non-compliance risks significant legal, financial consequences, and irreparable damage to the company's reputation. To comply with SOC1 and SOC2 guidelines, it's vital to develop policies and procedures focused on user access and data protection, aligning with the "least permissions" principle. Ensuring backups and disaster recovery plans are essential for business continuity. Integrating IDS and AV software in legacy systems would elevate threat detection capabilities. Securing Botium Toys' physical location involves using locks, CCTV, and other safety measures like proper lighting and fire prevention systems. While not urgent, features like time-controlled safes and alarm service provider signage further boost security.