# Stakeholder memorandum

TO: IT Manager, Stakeholders

FROM: Mancris Ogdol Iboa  
DATE: August 10, 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, security information and event management (SIEM) tool.
* Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements with PCI DSS and GDPR.
* Ensure current technology is accounted for both hardware and system access.

**Goals:**

* Adhere to NIST CSF.
* Establish a better process for their systems to ensure they are compliant.
* Fortify system controls.
* Implement the concept of least privilege permission 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):

* Controls that needs to be developed and implemented to meet the audit goals, including:
  + Control of Least Privilege, Separation of Duties
  + Disaster Recovery Plans for Business Continuity
  + Backups
  + Password Policies
  + Access Control Policies for both Internal and External Users to ensure safety of Data and Assets
  + Intrusion Detection System (IDS)
  + Anti Virus software
  + Encryption
  + Manual Monitoring, Maintenance for Legacy systems
  + Time-controlled safe
  + CCTVs
  + Locking Cabinets for on-premises equipment and employee equipment
  + Locks for Physical and Digital assets to be more secure.
* 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):

* Controls that should be implemented when possible:
  + Account management Policies
  + Password Management system
  + Adequate Lighting
  + Fire detection and prevention

**Summary/Recommendations:** It is recommended that critical findings relating to compliance with PCI DSS be addressed as soon as possible since Botium Toys conducts business with a growing presence abroad and is accepting online payments to ensure processing and transmitting credit card information in a secure environment. Since Botium Toys is more present abroad, including in the European Union (E.U.), through online business transactions, they need to adhere to GDPR to protect the processing of E.U. citizens data and their right to privacy in and out of E.U. territory. Additionally, since one of the goals of the audit is to adapt to the concept of least permissions, SOC1 and SOC2 guidance related to user access policies and overall data safety should be used to develop appropriate policies and procedures. Having Disaster Recovery Plans and Backups is also critical to business continuity in the event of an incident. Password and Access control policies to ensure the safety of data and assets. Also, setting up an intrusion detection system (IDS) and Antivirus software (AV) into current systems to help identify and mitigate potential risks could help with intrusion detection since existing legacy systems require manual monitoring and intervention. Lastly, Botium Toys has a single physical location where physical assets need safeguarding, such as employee equipment and on-premises equipment for in-office business needs. The installation of CCTVs, Locking cabinets, Locks, a time-controlled safe, and Encryption will help further protect external assets for business continuity. While not necessary immediately, having Account management Policies, a password management system, Adequate lighting, and a fire detection and prevention system will further improve the security controls of Botium Toys internal and External assets and the overall security posture of the organization.