# Stakeholder memorandum

TO: IT Manager, Stakeholders

FROM: Prasenjit Malakar  
DATE: 19-06-2023  
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. Those systems will be

evaluated for

* Current user permissions set
* Current implemented controls
* Current procedures and protocols
* Ensure current user permissions, controls, procedures, and protocols in place

align with necessary compliance requirements.

* Ensure current technology is accounted for. Both hardware and system access.

**Goals:**

The goals for Botium Toys’ internal IT audit are:

* To adhere to the NIST CSF
* Establish a better process for their systems to ensure they are compliant
* Fortify system controls
* Adapt 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 and developed to meet the audit goals:

* Least Privileges control
* Disaster recovery plans
* Password, Access control and account management policies including implementation of password management system
* Intrusion detection system
* Encryption( For payments and other secure transactions)
* Backups
* Antivirus software
* Manual monitoring, maintenance, and intervention to identify and mitigate potential threats, risks, and vulnerabilities
* CCTV
* Locks for physical and digital assets
* Fire detection and prevention

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

The following controls need to implemented when possible:

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

**Summary/Recommendations:**

Since the Botium Toy’s collect personal information and online payments from people worldwide, including E.U., It is recommended that critical findings related to compliance with GDPR regulations and PCI DSS be promptly addressed. As the goal of the audit is to achieve the concept of least permission and enforce appropriate user access, SOC1 and SOC2 guidance related to user access policies and overall data safety should be used to develop appropriate policies and procedures. Having a disaster recovery plan and backup as it supports ongoing productivity in the case of an event or disaster is critical. Password management systems with proper password recovery, reset, lock out notifications should be implemented. Integration of IDS and AV software into the current systems will support our ability to identify and mitigate potential risks, and could help with intrusion detection, since existing legacy systems require manual monitoring and intervention. And to further secure the assets housed at Botium Toys’ physical location CCTV and locks should be implemented to secure physical assets (including equipment) and to monitor and investigate potential threats. While not necessary immediately, using encryption and having a time-controlled safe, adequate lighting, locking cabinets, fire detection and prevention systems, and signage indicating alarm service provider will further improve Botium Toys’ security posture.