# Stakeholder memorandum

*TO: IT Manager, Stakeholders*

*FROM: Josue Ramos*

*DATE: 09/04/2023*

*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 scope of the Botium Toys internal IT audit includes the assessment of the following areas:*

* *Current User Permissions:*

*Evaluation of user permissions in specific systems: accounting, endpoint detection, firewalls, intrusion detection system, and Security Information and Event Management (SIEM) tool.*

* *Current Implemented Controls:*

*Assessment of the controls that are currently in place within the specified systems: accounting, endpoint detection, firewalls, intrusion detection system, and SIEM tool.*

* *Current Procedures and Protocols:*

*Review of the procedures and protocols established for the designated systems: accounting, endpoint detection, firewall, intrusion detection system, and SIEM tool.*

* *Alignment with Compliance Requirements:*

*Ensuring that the current user permissions, controls, procedures, and protocols align with the necessary compliance requirements, which may include regulatory standards and industry best practices.*

* *Technology Inventory:*

*Verification of the presence and accounting for both hardware and system access to ensure that the organization has an accurate inventory of its technology assets.*

***Goals****:*

* *Adhere to the NIST CSF*
* *Establish a better process for their systems to ensure they are compliant*
* *Fortify system controls*
* *Implement the concept of least permissions when it comes to user credential management*
* *Establish policies and procedures, which includes their playbooks*
* *Ensure compliance requirements are meeting*

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

*The following controls should be implemented immediately:*

* *Least Privilege*
* *Disaster recovery plans*
* *Password policies*
* *Access control policies*
* *Account management policies*
* *Separation of duties*
* *Intrusion Detection System (IDS)*
* *Encryption*
* *Backups*
* *Password management system*
* *Antivirus (AV) software*
* *Manual monitoring, maintenance, and intervention*
* *Closed-circuit television (CCTV) surveillance*
* *Locking cabinets (for network gear)*
* *Locks*
* *Fire detection and prevention (fire alarm, sprinkler system, etc.)*

*Also, it is important to comply with the following regulations:*

* *General Data Protection Regulation (GDPR)*
* *Payment Card Industry Data Security Standard (PCI DSS)*
* *System and Organizations Controls (SOC type 1, SOC type 2)*

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

*The following controls should be implemented when possible:*

* *Time-controlled safe*
* *Adequate lighting*
* *Signage indicating alarm service provider*

***Summary/Recommendations****:*

*The Botium Toys internal IT audit has identified critical findings that demand immediate attention. These include implementing controls related to least privilege, disaster recovery, password policies, access control, and compliance with regulations such as GDPR, PCI DSS, and SOC types 1 and 2.*

*Additionally, it is crucial to prioritize the implementation of essential security measures such as intrusion detection systems, encryption, backups, antivirus software, and physical security enhancements like CCTV surveillance and locking cabinets.*

*While some findings may not require immediate action but should be addressed when feasible, they should not be overlooked. These findings encompass physical security improvements, such as time-controlled safes, lighting enhancements, and clear signage indicating alarm service providers.*

*Addressing these recommendations will not only fortify Botium Toys' security posture but also help the organization comply with industry regulations and protect critical assets in an ever-evolving threat landscape.*