# Stakeholder Memorandum

TO: IT Manager, Stakeholders

FROM: Brian Mach  
DATE: 8/5/2023  
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 system, and SIEM tool are all in scope
  + Systems will be evaluated for current user permissions, implemented controls, and procedures/protocols
* Ensure current user permissions, controls, procedures, and protocols comply with PCI DSS and GDPR requirements
* Ensure the latest technology is accounted for both hardware and system access

**Goals:**

* Adhere to the NIST CSF
* Establish a better process for Botium Toys’ systems for ensuring compliance
* Fortify system controls
* Adapt the concept of least permissions for user credential management
* Establish Botium Toys’ policies, procedures, and playbooks
* Ensure Botium Toys meet compliance requirements

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

* These controls need to be developed and implemented to meet the audit goals

1. Least Privilege
   1. To reduce risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs
2. Disaster Recovery Plans
   1. For business continuity to ensure systems are able to run in the event of an incident and to ensure there is limited to no loss of productivity
   2. Makes sure there is little to no impact to system components
      1. computer room environment
      2. hardware
      3. applications
      4. data and restorations
3. Password Policies
   1. To establish password strength rules so that security is improved and the likelihood of account compromisation through brute force or dictionary attack techniques to be reduced
4. Access Control Policies
   1. To increase confidentiality and integrity of data
5. Account Management Policies
   1. To reduce attack surface and limit overall impact from disgruntled/former employees
6. Intrusion Detection System (IDS)
   1. To allow IT team to identify possible intrusions quickly
7. Encryption
   1. To make confidential information and data more secure
8. Backups
   1. To support ongoing productivity in the case of an event
9. Separation of Duties
   1. To ensure no one has so much access that they can abuse the system for personal gain
10. Password Management Systems
    1. For password recovery, reset, and lock out notifications systems
11. Antivirus Software
    1. To detect and quarantine known threats
12. Manual monitoring, maintenance, and intervention
    1. Compliance requirements for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities
13. Closed-circuit television (CCTV) surveillance
    1. To reduce risk of certain events and can be used after an event for investigation
14. Locks
    1. To increase security for physical and digital assets

* Policies need to be developed and implemented to meet compliance requirements of PCI DSS and GDPR
* Policies need to be developed and implemented to align the user access policies and overall data safety to SOC1 and SOC2 guidelines

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

1. Time-controlled Safe
   1. To reduce attack surface and impact of physical threats
2. Adequate lighting
   1. To limit “hiding” places, deterring threats
3. Locking cabinets (for network gear)
   1. To increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear
4. Signage indicating alarm service provider
   1. To make the likelihood of a successful attack seem low
5. Fire detection and prevention (fire alarm, sprinkler system, etc.)
   1. To detect fire in the toy store’s physical location to prevent damage to inventory, servers, etc.

**Summary/Recommendations:**

It is recommended that the critical findings regarding compliance with PCI DSS and GDPR be immediately addressed since Botium Toys accepts online payments from customers worldwide, including the E.U. Additionally, SOC1 and SOC2 guidance related to user access policies and procedures should be used to develop the appropriate policies and procedures so that Botium Toys adapts the concept of least permissions. In the event of an incident, having the necessary backup and recovery plans is crucial because they support business continuity. Integrating an IDS and AV software into the current systems will support Botium Toys’ ability to identify and mitigate potential risks, especially for monitoring legacy systems. Physical assets should also be more secured through the implementation of locks and CCTV at Botium Toys. While it is 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 the security posture of Botium Toys.