Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: (Your Name)
DATE: (Today's Date)
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. Those systems are implemented in these 3 areas:
  - Current user permissions
  - Current implemented controls
  - Current procedures and protocols
- Ensure current user permissions, controls, procedures, and protocols in place align with PCI DSS and GDPR requirements.
- Ensure current technology is accounted for both hardware and system access.

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 their policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements

Critical findings (must be addressed immediately):

- Multiple controls are needed to be developed and implemented to meet the audit goals:
  - Control of the least privilege
  - Disaster recovery plans
  - Password, access control, account management policies including an password management system
  - Separation of duties
  - IDS
  - Encryption
  - Backups
  - AV software
  - Manual monitoring, maintenance and intervention
  - Locks
- Policies need to be developed and implemented to meet PCI DSS and GDPR requirements.

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

- The followings controls should be implemented when possible:
  - Time control safe
  - Adequate lighting
  - Locking cabinets
  - Signage indicating alarm service providers
  - Fire detection and prevention

Summary/Recommendations: It is recommended that critical findings relating to compliance with PCI DSS and GDPR are applies as soon as simple since Botium Toys accepts online payments from customers worldwide. Overall data safety should be implemented because one of their goals of the audit is to adapt to the concept of least permissions, SOC1 and SOC2 guidance should be used. Having disaster recovery plans and backups is crucial because they support business continuity in the event of an accident. Implementing an IDS and AV software is a way to mitigate potential risks, and could help with intrusion detection. While it is not necessary immediately, using encryption and having a time-controlled safe, adequate lighting, locking cabinets, fire

detection and signage indicating alarm service providers will further improve Botium Toys' security even more.