# Stakeholder memorandum

Complete each section of the stakeholder memorandum template to communicate your audit results and recommendations to stakeholders:

* Scope
* Goals
* Critical findings (must be addressed immediately)
* Findings (should be addressed, but no immediate need)
* Summary/Recommendations

TO: IT Manager, Stakeholders

FROM: Benton Anestal   
DATE: 6/21/2023  
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 tools. The systems will be evaluated for:
  + Current user permissions
  + Current implemented controls
  + Current procedures and protocols
* Ensure current user permissions, controls, procedures, and protocols in place align with PCI DSS, GDPR and SOC 1 &2 compliance requirements.
* Ensure current technology is accounted for. Both Hardware and system access.

**Goals:**

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

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

* Multiple controls need to be developed and implemented to meet the audit goals, including:
  + Control of Least Privilege and Separation of Duties
  + Disaster recovery plans
  + Password, access control, and account management policies, including the implementation of a password management system.
  + Encryption (for secure website transactions)
  + IDS
  + Backups
  + AV software
  + CCTV
  + Locks
  + Manual monitoring, maintenance, and intervention for legacy systems
  + Fire detection and prevention systems
* 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):

* The following controls should be implemented when possible:
  + Time-controlled safe
  + Adequate lighting
  + Locking cabinets
  + Signage indicating alarm service provider.

**Summary/Recommendations:**

* It's crucial for Botium Toys, given its acceptance of global online payments including those from the E.U., to swiftly address any key findings in compliance with PCI DSS and GDPR. Adapting to a "least permissions" model is a primary aim of our audit, thus using SOC1 and SOC2 guidance to shape suitable user access policies and overall data protection procedures is highly advised. In the face of potential incidents, business continuity relies on comprehensive disaster recovery plans and consistent data backups. Incorporating IDS and AV software into existing systems will enhance our capacity to spot and counter potential threats, offering a solution to the manual monitoring and intervention required by our current legacy systems.
* In order to secure Botium Toys' solitary physical site, installing locks and CCTV is necessary to protect physical assets, like equipment, and to track and probe potential security breaches. Additional security measures, although not immediately essential, include employing encryption, setting up a time-controlled safe, ensuring sufficient lighting, installing lockable cabinets, and integrating fire detection and prevention systems. Indicative signage of the alarm service provider will further fortify Botium Toys' security stance.