# 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

Use information from the following documents:

* [Botium Toys: Audit scope and goals](https://docs.google.com/document/d/1bA-J96jzDVFi9XjNOKd4w2bCR7X7ZTs3_szPElOkyFM/template/preview)
* Controls assessment (completed in “Conduct a security audit, part 1”)
* Compliance checklist (completed in “Conduct a security audit, part 1”)

[***Use the following template to create your 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:**

— Current user permissions set in the following systems: accounting, end point

detection, firewalls, intrusion detection system, security information and event

management (SIEM) tool.

— Current implemented controls in the following systems: accounting, end point

detection, firewalls, intrusion detection system, Security Information and Event

Management (SIEM) tool.

— Current procedures and protocols set for the following systems: accounting,

end point detection, firewall, intrusion detection system, Security Information

and Event Management (SIEM) tool.

— 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:**

— To adhere to the National Institute of Standards and Technology Cybersecurity

Framework (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**

All the below controls needs to be implemented to meet the audit requirements and goals.

* 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:**

PCI-DSS and GDPR. This is crucial because Botium Toys engages in global online payment acceptance, including from customers within the E.U. Furthermore, as part of the audit's objectives to align with the principle of least permissions, it's recommended to utilize SOC1 and SOC2 guidance concerning user access policies and overall data security. This will facilitate the development of suitable policies and procedures.

The establishment of disaster recovery plans and implementing backups holds significant importance. These measures are essential to ensure business continuity in case of any incidents. Enhancing our capability to identify and mitigate potential risks is achievable by integrating Intrusion Detection Systems (IDS) and Anti-Virus (AV) software into the existing systems. This becomes especially relevant since the existing legacy systems rely on manual monitoring and intervention for intrusion detection.

For added security of assets located at Botium Toys' singular physical location, the use of locks and Closed-Circuit Television (CCTV) is recommended. This will serve to safeguard physical assets, including equipment, and provide surveillance for potential threats. While not an immediate requirement, the adoption of encryption, a time-controlled safe, adequate lighting, secured locking cabinets, fire detection and prevention systems, along with signage indicating the alarm service provider, will further enhance the overall security posture of Botium Toys.