# 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: Matthew Lam  
DATE: 2023-08-24  
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 this audit included the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool. The systems were audited for:

1. Current User Permissions
2. Current Implemented Controls
3. Current Procedures and Protocols

Additionally, ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements as well as 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** (must be addressed immediately):

Lack of controls gives Botium Toys a risk assessment of 8/10

These controls need to be immediately implemented:

* Least privilege
* Disaster Recovery Plans
* Separation of duties
* IDS
* Data Encryption
* Backups
* Manual Monitoring for legacy systems
* CCTV
* Antivirus
* Locking Cabinets
* Locks

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

* Password Policies
* Access Control Policies
* Account Management Policies
* Password Management Systems
* Adequate lighting
* Alarm Service Signage
* Fire Detection System

**Summary/Recommendations:**

It is important to adhere to GDPR, PCI DSS Guidelines and Regulations as Botium will be handling transactions online with E.U. customers. SOC Guidelines will help reduce risk when implementing user permissions and policies within and outside the organization.

Implementing backups and disaster recovery plans are extremely important for business continuity, especially since the organization is at HIGH risk. IDS, Antivirus and CCTV will be the basic line of defense for detecting anomalies. With a physical location in America, locks and cabinets will physically secure the hardware storing data and SPII. These controls are especially important with a legacy system that requires manual monitoring.

Password and account policies are important, but aren’t as immediately required as the earlier recommendations. Lastly, adequate lighting, signage and a fire detection system will be required, but not urgent to the organization's operations.