# 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: Suliman Shonibare   
DATE: 05/30/23  
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: Botium Toys internal IT audit will assess the following:**

**● 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: The goals for Botium Toys’ internal IT audit are:**

**● 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): Some of the Things that present the highest vulnerabilities

Regulations/ policies : we need to get into complinace with :

General Data Protection Regulation because we operate internationally and wouldnt want to infringe upon policies in places we might conduct business.

Payment Card Industry Data Security Standard, since we process payments online we have to make sure that we are in compliance with this standard to avoid future issues.

Lastly we should be in compliance with the System and Organization Controls guidelines so that we have proper data protection and management

Administrative : We need to set up least privilege controls , disaster recovery plans , stricter password policies , our access control policies need to be stricter . And implement seperation of duties .

Technical : We need to dedicate resources to an intrusion detection system , we should start adpoting the practice of encryption, and backups. We could also benefit from implementing a password management system, and antivirus software

Cctv surveillance : We have physical assets so we must keep track of whos handling what incase of any mishaps

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

Manual monitoring, maintenance and intervention for our legacy systems : because we do have some older systems in place so it is pivotal for us to have someone monitoring these systems at all times .

Adequate lighting for our cctv systems : There are some areas of the premises that do provide a nice blind spot for would be attackers and we could minimize risk by adding adequate lighting

Locking cabinets for our network gear : having network gear that anyone can have access to is a threat to business operations and data security by adding locking cabinets we have more control over who has access to these assets

Signage indicating alarm service provider: By having a sign identifying who our alarm service provider is can make potential threats think twice before acting and in a best case scenario deter them completely from attempting to break in our location.

**Summary/Recommendations:**

All in all Botium has a lot of vulnerabilities and with a risk score of 8 out of 10 its best to act now before the issues above hinder business continuity. There are some changes that can be made to be done later rather than sooner but we made sure to identify which issues need to be addressed soonest . If we can start with the risks that are high priority we can slowly implement the rest as the threats that pose the highest risk have been mitigated.