# 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: Nicholas Hoang  
DATE: 6/8/2023  
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 security audit performed assessed 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 were:

* 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):

Botium currently has a large problem with mishandling of assets. A major proportion of assets is in the hands of IT employees. A company should usually use more of their resources to separate the responsibilities of assets to multiple departments. The IT department simply has access to too many assets and needs to divide their responsibilities among other departments. The IT department also does not follow the rule of least priority, a rule meaning that the employees should only have enough access to perform their jobs and no more.

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

The creation of more physical controls should be increased. Although it does not pose an immediate threat to safety, the lack of controls may cause more problems later on and should be considered.

**Summary/Recommendations:**

Although these are the problems right now, the problems have already been identified and this is the first step to repairing the system. While mishandling of assets is a large problem, a simple restructuring of how the company performs its duties is all that it will take to resolve this issue. I urge you as a shareholder to remain patient with the company, as it will likely correct it diligently. The purpose of security audits are to identify the potential threats and a company that is dedicated enough to perform security audits shows that they are taking these issues very seriously and doing actions such as this shows that security is a priority for the company and that they can be trusted to maintain their integrity as a company.