# 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: Al.ortiztique  
DATE: 21/01/2024  
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 was to evaluate the technical, physical and digital aspects as well as the compliance elements to be met with priority levels.**

**● 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** (must be addressed immediately):

1. There are no technical or digital security measures in place and they must be implemented urgently.

2. Compliance is null and there are many physical risk points.

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

1. The physical measures and distribution of functions and powers of the administrator.

**Summary/Recommendations:**

Use the Availability, Integrity and Confidentiality scheme as the main guideline for the initial security work.