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/1DWmu8rVrIY_vGR3nRCUl7sxekN2fGRYypcF6ej8YheA/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: (Samad Ali)  
DATE: (05/12/2023)  
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:** Botium Toys entire internal IT audit

1) Current user permissions set in the following systems

2) Current implemented controls in the following systems

3) Current procedures and protocols set for the following systems

4) Ensure current user permissions, controls, procedures, and protocols in place

align with necessary compliance requirements.

5) 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):

-) Must protect the data of the customer and consult with the General Data Protection Regulation (GDPR)

-) Must consult with Payment Card Industry Data Security Standard (PCI DSS) for customer credit card payments and reports and follow there guidelines.

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

-) should consult with System and Organizations Controls (SOC type 1, SOC type 2) for overall companies financial data security.

**Summary/Recommendations:**

Botium Toys should follow the guidelines by GDPR, PCI DSS, and SOC Type1 and SOC Type2 to protect cand secure ompany and customer data, other finding also includes that company should also have to use strong password policies to for un authorize acces of the users, so that it can function and sell toys securely online.