# 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: Kirk Hendrix L. Bulaong  
DATE: August 30, 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 audit encompassed a comprehensive evaluation of Botium Toys' security program, including user permissions, controls, procedures, and protocols across various systems. The assessment aimed to align practices with industry standards, identify and mitigate high-risk vulnerabilities, and enhance overall security posture.

**Goals:**

The audit's objectives were to conform to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establish compliant processes, reinforce system controls, enforce least privilege principles, establish policies and procedures, and ensure adherence to compliance requirements.

**Critical findings** (must be addressed immediately):

* **Least Privilege**: Urgent implementation is necessary to limit unauthorized access and reduce risks.
* **Disaster Recovery Plans**: Immediate action is vital to ensure swift recovery and uninterrupted business operations after incidents.
* **Password Policies**: Prompt enforcement of robust password rules is essential to prevent compromise and breaches.
* **Access Control Policies**: Urgent enforcement is required to safeguard data integrity and confidentiality.
* **Account Management Policies**: Immediate implementation will restrict access and prevent unauthorized actions.
* **Separation of Duties**: Immediate action will prevent misuse of privileges through role segregation.
* **Intrusion Detection System** (IDS): Swift deployment is crucial to detect and respond to network threats.
* **Encryption**: Immediate implementation will secure data during transmission and storage.
* **Backups**: High-priority implementation is needed for data recovery and reduced disruptions.
* **Password Management System**: Immediate enforcement will manage passwords and prevent unauthorized access.
* **Antivirus (AV) Software**: Immediate implementation will identify and isolate known threats.
* **Manual Monitoring, Maintenance, and Intervention**: Urgent implementation will mitigate vulnerabilities in legacy systems.

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

* **Encryption**: Enhancement of data protection during transmission/storage in the future is recommended.
* **Password Management System**: Strengthening of password practices is advised for future improvement.
* **Time-Controlled Safe**: Adding a security layer against physical threats in the future is suggested.
* **Adequate Lighting**: Improving physical security by minimizing hiding spots for potential threats in the future is recommended.
* **Closed-Circuit Television** (CCTV) **Surveillance**: Enhanced monitoring for incident visibility and response in the future is suggested.
* **Locking Cabinets** (for Network Gear): Preventing unauthorized access to network equipment through implementation in the future is advised.
* **Fire Detection and Prevention**: Enhancement of fire safety measures for asset protection in the future is recommended.

**Summary/Recommendations:**

* Immediate implementation of high-priority controls, including least privilege, disaster recovery plans, access control, intrusion detection, encryption, backups, and antivirus software.
* Prompt implementation of separation of duties and locking cabinets for heightened security.
* Addressing medium/low-priority controls in the near future for comprehensive improvement.
* Adherence to GDPR and PCI DSS for international business and credit card handling.
* Alignment with industry standards, strengthening of security posture, and ensuring compliance are central to our approach.

Please feel free to reach out with any questions or clarifications. Thank you for your attention to these critical matters.

Sincerely,

Kirk Hendrix L. Bulaong