# 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: Trey Griffiths   
DATE: 8/10/2023  
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

I would like to present the findings and recommendations from the recent internal IT audit conducted for Botium Toys. The audit aimed to enhance our security posture, align with industry best practices, and identify compliance requirements. Below is a summary of the audit results:

**Scope:**

The audit covered a comprehensive review of Botium Toys' IT infrastructure, focusing on controls, policies, and compliance standards.

**Goals:**

The primary goals of the audit were to improve our security posture by adhering to industry standards, provide recommendations to mitigate identified risks, and ensure compliance with relevant regulations.

**Critical Findings (Must Be Addressed Immediately):**

The audit identified several critical findings that require immediate attention:

* Least Privilege: Implement access controls to limit unauthorized access.
* Disaster Recovery Plans: Establish comprehensive plans for business continuity.
* Password Policies: Strengthen password requirements to enhance security.
* Access Control Policies: Enhance confidentiality and integrity of data through proper access controls.
* Account Management Policies: Reduce attack surface and limit impact from former employees.
* Password Management System: Implement a system for secure password management.
* Antivirus (AV) Software: Deploy AV software to detect and quarantine threats.
* Manual Monitoring and Maintenance: Essential for legacy systems' security.
* Physical Controls (Time-controlled safe, adequate lighting, CCTV, locking cabinets, signage, locks, fire detection): Implement physical measures to safeguard assets.

**Findings (Should Be Addressed, But No Immediate Need):**

Additionally, the audit highlighted areas for future consideration:

* Separation of Duties: Implement controls to prevent potential misuse.
* Encryption: Explore encryption methods to secure sensitive data.
* Firewall and Intrusion Detection System (IDS): Consider implementation for enhanced network security.
* System and Organizations Controls (SOC type 1, SOC type 2): Assess for financial compliance and data safety.

**Summary/Recommendations:**

In summary, immediate attention is required to address critical findings that pose significant risks to our security and compliance. By implementing the recommended controls and policies, we can enhance our security posture, mitigate risks, and align with industry standards. Additionally, we should plan for future improvements to ensure comprehensive security measures.

Thank you for your attention to these findings. Your commitment to addressing these issues is vital for safeguarding our company's assets, data, and reputation. Please feel free to reach out if you have any questions or require further clarification.

Best Regards,

Trey Griffiths