# 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: (Caden Izbicki)  
DATE: (6/29/2023)  
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 internal IT audit at Botium Toys encompassed the assessment of the entire security program including the evaluation of user permissions, implemented controls, procedures, protocols, compliance alignment, and technology inventory.

**Goals:** The goals for the internal IT audit at Botium Toys were as follows:

* Adhere to the National Institute of Standards and Technology Cybersecurity Framework.
* Establish a better process for ensuring compliance with relevant regulations and standards.
* Fortify system controls to enhance the overall security posture
* Implement the concept of least permissions for user credential management
* Establish comprehensive policies and procedures including playbooks

**Critical findings** (must be addressed immediately):Based on the audit, the following critical findings require immediate attention:

* **User Permissions**: Several user accounts have excessive privileges in the accounting system, end point detection, firewalls, intrusion detection system, and SIEM tool. This increases the risk of unauthorized access and potential data breaches. Immediate action should be taken to adjust user permissions and align them with the principle of least privilege.
* **Controls Implementation**: Significant gaps were identified in the implementation of controls within the accounting system, end point detection, firewalls, intrusion detection system, and SIEM tool. Failure to address these gaps promptly may expose the organization to security vulnerabilities. Immediate action is required to implement the necessary controls and mitigate risks.
* **Compliance Alignment**: Botium Toys' current user permissions, controls, procedures, and protocols do not fully align with the necessary compliance requirements. It is critical to address these gaps promptly to ensure compliance with applicable regulations and standards.

**Findings** (should be addressed, but no immediate need): The following findings were identified during the audit and should be addressed in a timely manner to enhance the organization's security posture:

* **Procedures and Protocols:** While Botium Toys has established procedures and protocols for the accounting system, end point detection, firewall, intrusion detection system, and SIEM tool, there is room for improvement. These procedures and protocols should be reviewed and updated to reflect industry best practices and address identified gaps.
* **Technology Inventory:** The organization lacks an updated and accurate inventory of its technology assets, including hardware and system access. It is recommended to implement a comprehensive inventory management system to ensure visibility and control over the technology infrastructure.

**Summary/Recommendations:** The internal IT audit at Botium Toys has identified critical findings that require immediate attention. These findings include excessive user privileges in the accounting system, end point detection, firewalls, intrusion detection system, and SIEM tool. Additionally, significant gaps were found in the implementation of controls, and the organization's current user permissions, controls, procedures, and protocols do not align with necessary compliance requirements.

These critical findings pose significant risks to the organization's security and compliance. To mitigate these risks, immediate action must be taken to adjust user permissions, implement necessary controls, and address compliance gaps. By doing so, Botium Toys can strengthen its security posture, reduce the risk of unauthorized access and data breaches, and ensure compliance with applicable regulations and standards.

Addressing these critical findings should be the top priority for the organization, as it will help enhance the overall security and compliance posture. Taking immediate action to rectify these issues will contribute to a more secure and resilient IT environment at Botium Toys.