# 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”)

TO: IT Manager, Stakeholders

FROM: James H.  
DATE: 09-07-2023  
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 scope of the internal IT audit was to assess the information security controls and practices implemented by Botium Toys. The audit covered the company's information systems, policies, and procedures related to information security.

**Goals:** The goals of the audit were to identify any vulnerabilities or weaknesses in Botium Toys' information security controls and provide recommendations for improving the company's security posture.

**Critical findings** (must be addressed immediately): During the audit, several critical findings were identified that require immediate attention. These findings include:

1. Lack of regular backups and disaster recovery plan: Botium Toys does not have a proper backup plan and disaster recovery strategy, which poses a significant risk to the company's operations in the event of a system failure or a cyber attack.

2. Weak password policies: The password policies in place are not sufficient to protect the company's sensitive information from unauthorized access. Password complexity rules need to be strengthened and enforced.

3. Unpatched software and systems: Several systems and software used by Botium Toys are not up-to-date with the latest patches and updates, which leaves the company vulnerable to known security threats.

**Findings** (should be addressed, but no immediate need): The following findings were also identified during the audit, which should be addressed for overall improvement in the company's security posture:

1. Lack of regular security awareness training for employees.

2. Incomplete inventory of company assets and software licenses.

3. Inadequate monitoring and logging of network activity.

**Summary/Recommendations:** To improve Botium Toys' overall security posture, we recommend the following actions be taken:

1. Implement regular backups and disaster recovery plan.

2. Strengthen password policies and enforce them.

3. Update and patch all systems and software.

4. Provide regular security awareness training for employees.

5. Complete inventory of company assets and software licenses.

6. Implement proper monitoring and logging of network activity.

We appreciate the opportunity for our company to conduct this audit and offer recommendations to improve Botium Toys' information security. If you require additional information or have any questions or concerns, please don't hesitate to contact us.

Sincerely,

James H.