# 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”)

TO: IT Manager, Stakeholders

FROM: Adam Kruppenbacher  
DATE: 6/2/2023  
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:**

1. Assess the following for accounting, end point detection, firewalls, SIEM:

* Currently implemented controls
* User Permissions
* Procedures and Protocols

1. Ensure current procedures align with GDPR and PCI DSS compliance requirements
2. Ensure current technology is accounted for

**Goals:**

1. Adhere to NIST CSF
2. Establish better processes for system compliance and meeting compliance requirements including playbooks
3. Fortify system controls
4. Implement policies and procedures like least permissions

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

1. These controls are missing and need to be implemented:

Least Privilege – To ensure vendors only have access they need

Disaster recovery – To ensure business continuity in the event of an incident

Encryption – Secure/confidential data

Password management – For password recovery, reset, in case an employee gets locked out

Password policies – reduces the likelihood of brute forcing/account compromise

Access control policy – increases confidentiality/integrity of data

Account management – reduce attack surface and impact from disgruntled employees

Separation of duties – Ensure that noone can abuse power for personal gain

Locking cabinets – prevents unauthorized individuals from accessing network equipment, mitigates hacks

Locks – secures physical assets

1. Policies for PCI DSS and GDPR compliance need to be implemented
2. Playbooks need to be made for policy implementation

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

IDS – helps detect attackers

Backups – limits downtime caused by data loss

Antivirus – prevents malware

Manual monitoring, maintenance, intervention – monitors legacy systems

Time-controlled safe – reduces attack surface/physical threats

Lighting – limits hiding places to deter threats

CCTV – can reduce risk of events and used after event for investigations

Security Signage – can deter some threats

Fire detection/prevention – can reduce/prevent damage in case of fire

**Summary/Recommendations:**

Our audit of Botium Toy’s security posture showed that there is a very high risk of loss. We recommend several policy changes that will not only mitigate loss, but also strengthen your organization’s overall security posture. We believe implementing least privilege, encryption, password policies and password management, access control policy and account management, separation of duties, implementing disaster recovery, ensuring the correct types of locks are used on location, and using locking cabinets for your network equipment are critical to meeting our goals of adhering to the NIST CSF, establishing a better process that can help ensure system and regulatory compliance, fortifying system controls, and could be used to help establish policies and procedures for your playbook.

Meanwhile, additional but helpful recommendations we have are implementing physical controls like manual monitoring, time controlled-safes for your store, better lighting, CCTV systems, security signage, and fire detection and prevention would better equip your organization to handle an incident if they were to occur. In addition, you could also implement an IDS, backups for your data, and antivirus on your endpoints in order to maximize your overall security posture.