# 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
- 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: Nick
DATE: 8/15/2023
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 this security audit was the entire security program at Botium Toys. This means all assets were assessed alongside internal processes and procedures. More specifically, the audit assessed current user permissions in all systems, such as accounting, security information, and firewalls. There was additional assessment of the currently implemented controls of all systems, including the ones listed above, as well as IDS, SIEM, and end-point detection. There was also an assessment of all procedures and protocols for all the systems listed above. Finally, there was an assessment to ensure that all user permissions are in compliance, and all current technology is accounted for.

**Goals:** The internal audit had multiple goals. The first goal was to adhere to the NIST CSF. Additionally, there was the goal to establish a more efficient and effective process to ensure that systems are in compliance, as well as fortifying system controls. Lastly, the audit had the goal of implementing the concept of least permissions when it comes to user credential management. As Botium expands to the EU, it's important to process, handle, and transmit user data securely.

**Critical findings** (must be addressed immediately): It was found that all administrative controls should be implemented with high priority. Those controls include least privilege, disaster plan recovery, strong password policies, access control policies, account management policies, and separation of duties. With regards to technical duties, all controls should be implemented minus a firewall since that's already in place. The technical controls implemented with high priority include IDS, encryption, backups, AV software, and manual monitoring/maintenance/intervention. Lastly, there are two physical controls that should be implemented with high priority, those being locks and a fire detection system.

Additionally, it was found that there must be compliance with GDPR, PCI DSS, and SOC1 and SOC2. These are also high importance.

**Findings** (should be addressed, but no immediate need): Other controls that should be implemented, but with lower priority are password management systems (related to lock out notifications/recovery/reset options), time-controlled safe, adequate lighting, CCTV, locking cabinets, and signage to indicate alarm service provider.

**Summary/Recommendations:** It is recommended that with the look to expand our virtual presence to the EU that administrative and technical controls are implemented first and with high priority. While there are still some physical controls to implement, they can be added later down the line. With our growing virtual network, confidentiality, integrity, and availability must remain our top priority.