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: Kyle Neely
DATE: 7/9/23
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: Assessment of user permissions, implementations, and current procedures and protocols in: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool. Audit to ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements. Ensure current technology is accounted for. Both hardware and system access.

Goals: Audit aims to adhere to NIST CSF and ensure compliance requirements are being met. Botium Toys aims to fortify their system controls and implement the concept of least privileges. Botium Toys desires to establish a better complacency system and policy and procedures (such as playbooks).

Critical findings (must be addressed immediately): The following are security controls that must be developed implemented to fulfill audit goals:

- Control of Least Privilege and Separation of Duties
- Disaster recovery plans
- Password, access control, and account management policies, including the implementation of a password management system
- Encryption
- IDS
- Backups
- AV software
- CCTV
- Locks
- Manual monitoring, maintenance, and intervention for legacy systems
- Fire detection and prevention systems

Policies must be developed and implemented to adhere to GDPR, PCI DSS, and align with SOC1 and SOC2 requirements.

Findings (should be addressed, but no immediate need): These controls should be implemented when possible:

- Time-controlled safe
- Adequate lighting
- Locking cabinets
- Signage indicating alarm service provider

Summary/Recommendations: Botium Toys should promptly address compliance with GDPR and PCI DSS requirements as Botium Toys is an international online retailer. SOC1 and SOC2 guidelines should be followed to allow least permissions policies and overall data safety. IDS and AV software should be integrated to allow Botium Toys to identify and mitigate risks while locks and CCTV should be used to secure physical assets. Botium Toys, when able, should integrate time-controlled safes, adequate lighting, locking cabinets, etc. to strengthen security posture.