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: (Your Name)
DATE: (Today’s Date)
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 was to assess the entire Internal IT infrastructure of the company with emphasis on ensuring current technology is accounted for, current user permissions is up to industry standards, current implemented controls are in place and adequate in securing the Confidentiality, Integrity and Availability of data and to ensure current protocols, procedures, controls and user permissions are in line with compliance requirements

Goals:The goals where to ensure that the company’s It infrastructure was adhering to the NIST CSF, ensure that all controls, procedures and policies where meeting compliance requirements and to fortify security using administrative, technical and physical controls.

Critical findings (must be addressed immediately): The following controls are high priority and they must be fortified and implemented immediately

- □ Administrative controls like least privilege, disaster recovery plans, password policies, access control policies and separation of duties must be implemented immediately.
- □ Technical controls like Intrusion detection systems, backups, password management system, encryption, anti-virus software and manual monitoring, maintenance and Intervention must be implemented as a matter of urgency.
- □ Physical controls like CCTV surveillance, Locks, locking cabinets{for network gear} and fire detection and prevention must be implemented immediately.
- □ Also, the General Data Protection Regulation (GDPR), the Payment Card Industry Data Security Standard (PCI DSS) and the System and Organizations Controls (SOC type 1, SOC type 2) regulations must be urgently adhered to so that compliance is maintained.

Findings (should be addressed, but no immediate need): Other contorls that need to be addressed but not urgently include:

- □ Account management policies
- □ Adequate lighting
- □ Signage indicating alarm service provider

Summary/Recommendations: My recommendation is that the things listed above as urgent and high priority be swiftly implemented to mitigate risks, shut down vulnerabilities, prevent fines due to non-compliance and deter threat actors from taking advantage of these vulnerabilities.