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 system are in scope with: Accounting, end point detection, firewalls, intrusion detection system, security information and even management (SIEM) tool.
- The system will evaluate current user permissions, controls, procedures, and protocols to align with PCI DSS and GDPR requirements.
- Ensure the system is accounted for hardware and system access.

Goals:

- To adhere to the NIST CSF.
- Establish a better process for their system to ensure they are compliant
- Fortify system controls
- Implement the concept of least permissions when it comes to user credentials management
- Establish policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements

Critical findings (must be addressed immediately):

- Controls that need to be developed and implemented immediately:
    - Least Privilege
    - Disaster recovery plans
    - Password policies
    - Access control policies
    - Separation of duties
    - Firewakk
    - IDS
    - Encryption
    - Backups
    - Password management system
    - Antivirus (AV) software
    - Manual monitoring, maintenance, and intervention
    - Closed-circuit television (CCTV) surveillance
    - Locks
    - Fire detection and prevention (fire alarm, sprinkler system, etc.)
- Policies need to be developed and implement to meet PCI DSS & GDPR requimentest. Implement SOC1 & SOC2 to user guidelines.

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

- The following should implemented when possible:
    - Time-controlled safe
    - Adequate lighting
    - Locking cabinets (for network gear)
    - Signage indicating alarm service provider

Summary/Recommendations: It is recommended that the system are compliance with PCI DSS and GDPR are implemented since Botium Toys take credit card payments worldwide, including the E.U. It is important to implement SOC1 & SOC2 guidelines to user guidelines and data safety to develop appropriate policies and procedures. There are controls that need to be implemented immediately. In case of an event of an emergency, it is important to have a disaster recovery plan. Password policies need to be impletement by implementing password stregth rules to improve security. To identify potentials threats, risk, and vulnerability a manual monitoring, maintenance, and intervention need to be implemented. There are other controls that should be implemented when possible such as Time-controlled safe, adequate lighting, locking cabinets, and signage indicating alarm service provider will improve Botium Toy's security.