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 following systems are in the scope: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool. These systems are evaluated for:

- Current user permissions
- Current implemented controls
- Current procedures and protocols

Ensure current user permissions, control, procedures, and protocols in place align with necessary compliance requirements.
Ensure current technology is accounted for. Both hardware and system access.

Goals:

- Adhere to the NIST CSF
- Establish a better process for systems to ensure compliance
- Forlify system controls
- Implement the concept of least permissions for user credential management
- Establish policies and procedures, including playbooks
- Ensure compliance requirements are met

Critical findings (must be addressed immediately):

- Least privilege
- Disaster recovery plans
- Password policies and password management systems
- Access control policies
- Separation of duties
- IDS
- Encryption (for secure transactions)
- Backups
- AV software
- Manual monitoring, maintenance, and intervention
- CCTV
- Locks
- Policies need to be developed, and implemented to meet the PCI DSS compliance requirements
- Policies need to be developed, and implemented to meet the GDPR compliance requirements
- Policies need to be developed, and implemented to meet the SOC1 and SOC2 compliance requirements

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

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

- Fire detection and prevention

Summary/Recommendations:
Botium Toys is strongly advised to prioritize addressing critical findings related to compliance with PCI DSS and GDPR promptly. As an organization that accepts online payments from customers worldwide, including the European Union, ensuring compliance with these regulations is paramount. Implementing the concept of least permission is essential, and guidance from SOC1 and SOC2 can be leveraged to develop appropriate policies and procedures for user access and data safety.

Disaster recovery plans and backups should be given high priority to ensure business continuity in case of unforeseen events. Integrating an Intrusion Detection System (IDS) and antivirus software will greatly enhance the ability to detect and mitigate potential risks, particularly in contrast to the current manual monitoring and intervention practices.

To bolster physical activity, Botium Toys should employ locks and CCTV systems to protect their assets and effectively monitor potential threats. While not immediately urgent, time-controlled safes, adequate lighting, locking cabinets, fire detection and prevention systems, and appropriate signage will further enhance the organization's security measures.

By promptly addressing these recommendations, Botium Toys can achieve a higher level of compliance, strengthen data security, and safeguard both their online and physical assets.