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 audit's scope: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool. We will be assessing:
    - Current user permissions
    - Current implemented controls
    - Current procedures and protocols

- Ensure current users permissions, controls, procedures and protocols are aligned with GDPR and PCI DSS compliance requirements.
- Ensure all current technology is accounted for (hardware and system access).

Goals:

- To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for their systems to ensure they are compliant
- Fortify system controls
- Implement the concept of least permissions when it comes to user credential management
- Establish their policies and procedures, which includes their playbooks
- Ensure they are meeting compliance requirements

Critical findings (must be addressed immediately):

- Multiple controls are needed to be developed and implemented to achieve the audit's goals, including:
    - Control of least privilege and separation of duties
    - Disaster recovery plans
    - Password, access control, and account management policies, including a password management system.
    - Intrusion Detection System (IDS)
    - Encryption
    - Backups
    - Antivirus (AV) software
    - Manual monitoring, maintenance, and intervention
    - Closed-circuit television (CCTV) surveillance
    - Locks
- Policies need to be developed and implemented to meet PCI DSS and GDPR compliance requirements.
- Policies need to be developed and implemented to align with SOC1 and SOC2 guidance related to user access policies and overall data safety.

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

- The following controls should be implemented when possible:
    - Time-controlled safe
    - Adequate lighting

- Signage indication alarm service provider
- Locking cabinets (for network gear)
- Fire detection and prevention (fire alarm, sprinkler system, etc.)

Summary/Recommendations: It is recommended that critical findings relating to compliance with PCI DSS and GDPR be addressed immediately due to Botium Toys handling orders from all over the world, including the European Union. Also, since one of the goals of the audit is to implement the concept of least permissions, SOC1 and SOC2 guidelines related to user access policies and overall data safety should be followed to develop and implement appropriate procedures and policies for Botium Toys. Having a disaster recovery plan and backups in place must be addressed immediately too, as that will allow for business continuity in the event of an incident. Botium Toys should also implement an Intrusion Detection System and Antivirus software to identify and defend against risks, as well as detect intrusions into Botium Toys' systems, since Botium Toys' existing legacy systems require manual monitoring and intervention. Additional controls that should be implemented immediately are locks and CCTV surveillance, as that will help mitigate physical break-ins and monitor/identify potential threats. Some security controls that should be implemented when possible are a time-controlled safe, adequate lighting,
Signage indicating an alarm service provider, locking cabinets (for network gear), and a fire detection/prevention system.