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 were in the audit scope: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool. The focus on each system was:
    - Current user permissions
    - Current implemented controls
    - Current procedures and protocols

- Ensuring systems follow compliance for PCI DSS and GDPR as stated in the compliance checklist.
- Ensure technology for hardware and software systems are accounted for.

Goals:

- Adhere (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):
Following the controls assessment the following must be immediately implemented to meet audit goals:

- Control of Least Privilege and Separation of Duties
- Disaster recovery plans
- Password, access control, and account management policies
- Password management system
- Encryption (for secure website transactions)
- IDS
- Backups
- AV software
- CCTV
- Locks
- Manual monitoring, maintenance, and intervention for legacy systems
- Fire detection and prevention systems

These policies and controls must be developed to meet compliance with:

- PCI DSS
- GDPR
- SOC1
- SOC2

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

The following should be addressed when possible:

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

Summary/Recommendations:

- It is recommended that the critical findings be addressed immediately to avoid possible fines for not meeting compliance (especially in the case of PCI DSS and GDPR).
- For continued security, compliance to SOC1 and SOC2 will aid in mitigating future risk to assets and customers along with implementing IDS and AV software.
- Implementation of disaster recovery is critical to business continuity.
- Due to Botium Toys having a single physical location it is also recommended to implement locks and CCTV for increased security.