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: Dragon Vue
DATE: 07/24/2023
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:

- Current systems are in scope: accounting, end point detection, firewalls, intrusion detection system, security information and event management, SIEM tool. Systems that will be evaluated:
    - User Permissions
    - Implemented Controls
    - Procedures and protocol

- Ensure current user permissions, controls, procedures, and protocols in place align with PCI DSS and GDPR compliance requirements.
- Ensure current technology is accounted for both hardware and software access.

Goals:

- Adhere to the NIST CSF.
- Establish a better process for their systems to ensure they are compliant.
- Fortify system controls.
- Adapt to 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):

- Many of the controls need to be implemented to meet audit goals:
    - Least Privilege
    - Separation of duties
    - Disaster recovery plans
    - Password, Access control and account management policies, including implementation of a password management system
    - Encryption
    - IDS
    - Backups
    - AV Software
    - CCTV
    - Locks
    - Manual Monitoring, maintenance, and intervention for legacy systems
    - Fire detection and prevention systems

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

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

Summary/Recommendations: Botium Toys will need to make compliance with PCI DSS and GDPR since they are taking payments on their website from customers worldwide.