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: Mirza Rayyan
DATE: 17/06/2023
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:

● The following systems are in scope: accounting, end point detection, firewalls, intrusion detection system, SIEM tool. The systems will be evaluated for:

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

● 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 system access.**

Goals:

- **The following systems are in scope: accounting, end point detection, firewalls, intrusion detection system, SIEM tool. The systems will be evaluated for:**
  - **Current user permissions**
  - **Current implemented controls**
  - **Current procedures and protocols**
- **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 system access.**

Critical findings (must be addressed immediately):
The following controls and/or policies need to implemented immediately:
Least Privilege,Disaster recovery plans,Password policies,Access control policies,Separation of duties,Firewall
Intrusion Detection System (IDS),Backups,Antivirus (AV) software,Manual monitoring,maintenance, and intervention,Locks, Encryption.

The following regulations need to be adhered:

General Data Protection Regulation (GDPR)

Payment Card Industry Data Security Standard (PCI DSS)

System and Organizations Controls (SOC type 1, SOC type 2)

Findings (should be addressed, but no immediate need): The following controls and policies which can be implemented in future :
Time-controlled safe,Adequate lighting,Closed-circuit television (CCTV) surveillance,Locking cabinets ,Signage indicating alarm service provider,Fire detection and prevention (fire alarm, sprinkler system, etc.).

Summary/Recommendations:

Summary/Recommendations: It is recommended that critical findings relating to compliance with PCI DSS and GDPR be promptly addressed since Botium Toys accepts online payments from customers worldwide, including the E.U. Additionally, since one of the goals of the audit is to adapt to the concept of least permissions, SOC1 and SOC2 guidance related to user access policies and overall data safety should be used to develop appropriate policies and procedures. Having disaster recovery plans and backups is also critical because they support business continuity in the event of an incident. Integrating an IDS and AV software into the current systems will support our ability to identify and mitigate potential risks, and could help with intrusion detection, since existing legacy systems require manual monitoring and intervention. To further