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: (Kabilashwaran)
DATE: (30/07/2023)
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 user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
● Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.

● Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
● Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
● Ensure current technology is accounted for. Both hardware and system access.

Goals:
The goals for Botium Toys' internal IT audit are:
● 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 need to be developed and implemented to meet the audit goals, including:
    ○ Control of Least Privilege and Separation of Duties
    ○ Disaster recovery plans
    ○ Password, access control, and account management policies, including the implementation of a password management system
    ○ Encryption (for secure website transactions)
    ○ IDS
    ○ Firewall
    ○ Backups
    ○ AV software
    ○ CCTV
    ○ Locks
    ○ Manual monitoring, maintenance, and intervention for legacy systems

● Policies need to be developed and implemented to meet PCI DSS and GDPR compliance requirements.
● Policies need to be developed and implemented to align to 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
    - Locking cabinets
    - Signage indicating alarm service provider
    - Fire detection and prevention

Summary/Recommendations:

The GDPR and PCI DSS needed to be developed since the company accepts and sends transactions via online. SOC1 and SOC2 also needed to be developed to make sure the data is safe and secure with the CIA triad. The user privileges needed to be revised to make sure only authorized and needed people can access the data. Disaster recovery plans needed to be achieved to make sure the system is running even in the worst case. Furthermore, the password, access control, and account management policies need to be tightened up to prevent any loopholes to the system access. The duties are needed to be separated to prevent the system abuse by anyone intentionally. Firewall is needed to filter out malicious traffic to the network. IDS is needed to detect any possible attacks. All the sensitive data should be encrypted. Backing up, system that managing the passwords and antivirus software and needed to be implemented and updated. CCTV and Locks to the assets needed to be implemented as well to give a great security and surveillance. The less important actions are installing adequate lighting, time-controlled safe, locking cabinet, signage indicating alarm service provider and fire detection and prevention system