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: (Eric Brown)
DATE: (5/29/2023)
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, implemented controls, procedures and protocols set in the following systems: accounting, end point detection. Firewalls, intrusion detection system, Security Information and Event Management (SIEM). 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: To adhere to the 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:

- Multiple controls need to be developed and implemented to meet the audit goals including:
    - Least privilege
    - Disaster recovery plans
    - Password policies
    - Access control policies
    - Account management policies
    - Separation of duties
    - Intrusion detection system
    - Encryption (for secure website transactions)
    - Backups
    - Password management system
    - Antivirus software
    - Manual monitoring, Maintenance and Intervention
    - Time-controlled safe
    - Closed-circuit television surveillance
    - Locking cabinets for network gear
    - Locks
    - Fire detection and prevention
- 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:

- The following controls should be implemented when possible:
    - Adequate lighting
    - Signage indicating alarm service provider

Summary/Recommendations:

There are a lot of risks, vulnerabilities and lack of compliance with regulations with-in Botium Toys. I recommend adhering to the following compliance regulations and standards, which consist of GDPR because of the companies involvement with E.U. citizens, PCI DSS because of credit card information being stored, and transmitted in person and online, and lastly SOC 1 SOC2 to ensure the appropriate users are being given access to mitigate risk and ensure data safety. Having Disaster recovery plans and backups of data will support business continuity in case of an incident. Integrating the use of IDS and AV software into current systems will support our ability to identify and mitigate potential risks, and could help with intrusion detection. To further secure physical assets of Botium Toys, implementing Locks, Cabinet locks, and CCTV surveillance will work well and also allow monitoring and investigations into potential threats. While not top priority, having Adequate lighting and Signage indicating alarm service provider will still further improve Botium Toys security posture.