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: Camden Scholl
DATE: 05/26/2023
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.

We are looking mainly at accounting, end point detection, firewalls, IDS, and SIEM tools, to ensure that they have the correct user permissions, controls, and procedures and protocols in place. Then, we must make sure that each of these meet compliance regulations in the U.S. and internationally so that the company can expand. Finally, we need to consider our asset management, making sure that all current technology is clean and tallied. Also, we need to ensure that both system and hardware access is limited to authorized users.

Goals:

- 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

Compliance is currently a pressing issue, so implementing NIST CIF will allow Botium Toys to increase their security and cybersecurity, which will then enable them to meet compliance requirements, both domestically in the U.S. and internationally. The current procedures and processes are lacking, so we want to create more playbooks and establish a more efficient system for handling breaches and general business continuity. Specifically, we want to implement the concept of least permissions to limit unnecessary access to data, in this case user credentials.

Critical findings (must be addressed immediately):

- Least Privilege
- Disaster Recovery Plans

- Password Policies
- Access control policies
- Account management policies
- Separation of duties
- Intrusion Detection System
- Encryption
- Backups
- Password Management System
- Antivirus software
- Manual Monitoring, maintenance, and intervention

The current administrative and technical controls are severely lacking, so Botium toys needs to update and implement those immediately. They do have a firewall in place, which is a good start, but there is much more to do before they can meet compliance requirements for PCI DSS and GDPR, and match the guidelines of SOC1 and SOC2's user access policies.

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

- Time-controlled safe
- Adequate lighting
- CCTV surveillance
- Locking cabinets (for network gear)
- Signage indicating alarm service provider
- Locks
- Fire detection and prevention (fire alarm, sprinkler system, etc)

The physical controls are needed, but are less of a priority since Botium Toys operates out of a single building. These safety measures should be implemented to prevent unwanted or unauthorized individuals from accessing physical assets, such as the company network gear. Furthermore, there should be physical systems in place to protect the employees of Botium Toys from trespassers.

Summary/Recommendations:

Botium Toys' main focus should be on implementing new protective systems for their accounting, end point detection, firewalls, IDS, and SIEM tools. They are severely lacking in both administrative and technical controls, and these need to be updated

and fixed soon. Disaster plans and backups are necessary to maintain business continuity in the event of a breach, and IDS and AV software will help proactively prevent breaches and attacks. Without these, the company will not be able to meet compliance regulations, thus hindering their international expansion. Since the company takes online payments and stores users' credit card information, they need to comply with GDPR and PCI DSS. Furthermore, using SOC1 and SOC2 guidelines is recommended in order to implement the desired concept of least permissions and manage other user access policies. The company is also lacking many physical controls, such as locking cabinets and CCTV, which will protect both the company's physical assets, such as their network gear, as well as their employees. Overall, there are many urgent control implementations that Botium Toys needs to complete in order to meet compliance regulations and prepare to expand into international markets.