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: (Michael Leung)
DATE: (8/10/23)
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 settings, controls, procedures, and protocols are set in these systems: systems: accounting, end point,detection, firewalls, 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 both hardware and system access are accounted for**

Goals:

- **Adhere to the National Institute of Standards and Technology Cybersecurity**
- **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):

- **Botium Toys must follow these policies:**
    - **General Data Protection Regulation (GDPR)**
    - **Payment Card Industry Data Security Standard (PCI DSS)**
    - **System and Organizations Controls (SOC type 1, Soc type 2)**
- **The following things need to be addressed immediately:**
    - **Disaster recovery plan**
    - **Control of Least Privilege and Separation of duties**
    - **Password policies**
    - **Access control policies**
    - **Intrusion detection systems**
    - **Have backups**
    - **Manuel monitoring, frequent maintenance, and intervention**
    - **Locks**

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

- **The following should be addressed, but not as critical as above:**
    - **Account management policies**
    - **Encryption of data**
    - **Password management system**
    - **Installing antivirus software**
    - **Time-controlled safe**
    - **Adequate lighting**
    - **CCTV**

- Fire detection

Summary/Recommendations:

Because Botium Toys handles user data and financial information, it is critical to adhere to the GDPR and PCI DSS policies. Additionally, it is recommended to implement control of least privilege and separation of duties. Therefore, Soc type 1 and Soc type 1 should also be considered to avoid fraud. In order to avoid attacks, Intrusion detection systems and password policies should be in place. In the case of an emergency, Botium Toys should have backups that align with the disaster recovery plan. More physically, workplaces should have locks and manual monitoring.