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: Suman
DATE: 23-07-2023
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:

- The audit will focus on Botium Toys' cybersecurity program and aims to align its current business practices with industry standards and best practices.
- The scope includes assessing all assets and internal processes related to accounting, endpoint detection, firewalls, intrusion detection systems, and Security Information and Event Management (SIEM) tools.

- The audit will verify that user permissions, controls, procedures, and protocols are in place and compliant with requirements.
- It will also ensure that all technology, including hardware and system access, is properly accounted for.

Goals:

- Identify and classify high-risk vulnerabilities within Botium Toys' cybersecurity program.
- Provide recommendations to mitigate high-risk vulnerabilities and enhance the organization's overall security posture.
- Evaluate the alignment of current practices with industry standards and best practices in the cybersecurity domain.
- Assess the effectiveness of implemented controls in the specified systems.
- Ensure compliance with relevant requirements related to user permissions, controls, and protocols.
- Establish policies and procedures, including playbooks, to strengthen cybersecurity measures at Botium Toys.

Critical findings (must be addressed immediately):

- To meet the audit goals:
    - Administrative Controls needed to be set up, like
        - Least Privilege
        - Disaster Recovery Plans
        - Password, Access control, and Account Management Policies
        - Separation of duties
    - Technical Controls needed to be set up, like
        - Encryption
        - Backups
        - Password Management System
        - Antivirus (AV) software
        - Intrusion Detection System (IDS)
    - Physical Controls needed to be set up, like
        - Closed-circuit television (CCTV) surveillance
        - Locks
        - Fire detection and prevention (fire alarm, sprinkler system, etc.)

- Compliance standards like GDPR and PCI-DSS should be met for customer safety & be safe from Govt. Regulations; while SOC1 & SOC2 frameworks should be adhered to keep the infrastructure & information about our business safe.

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

- These should be implemented with time:
    - Time-controlled safe
    - Adequate lighting
    - Locking cabinets
    - Signage indicating the alarm service provider

Summary/Recommendations:

The risk assessment highlights critical vulnerabilities and compliance gaps that demand immediate attention. To mitigate these risks, Botium Toys must prioritize compliance with GDPR and fully implement the necessary SOC reports. Developing and regularly testing a comprehensive disaster recovery plan is vital to ensure business continuity and resilience.

Enhancing access controls and password policies will significantly reduce the risk of unauthorized access and data breaches. Additionally, the toy store should invest in updating or replacing legacy systems to eliminate potential security weaknesses.

For improved physical security, Botium Toys should consider expanding CCTV surveillance and implementing more robust access controls for network gear and critical infrastructure.

Overall, by addressing these critical and other findings, Botium Toys can bolster its security posture, safeguard customer data, and protect its reputation in the market. Regular audits and ongoing monitoring of security measures are essential to maintain a strong and proactive security stance.