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: Bichuk Oleksii
DATE: 06.09.2023
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 scope of the audit at Botium Toys encompasses their entire security program, including assets, internal processes, and procedures. It involves assessing and evaluating all aspects of their security measures. This comprehensive approach ensures a thorough examination of their security practices. By examining the entire security program, the audit aims to identify strengths, weaknesses, and areas for improvement to enhance overall security posture.

Goals: Botium Toys is committed to adhering to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The NIST CSF provides a set of guidelines and best practices for managing and improving cybersecurity. By aligning with the framework, Botium Toys aims to strengthen its security posture and mitigate potential risks

Critical findings:

Administrative Controls:

1. Least Privilege: Implement this control to ensure that vendors and non-authorized staff only have access to the assets and data they need for their job roles.
2. Disaster Recovery Plans: Establish comprehensive plans to ensure business continuity and minimize productivity downtime in the event of an incident. This includes maintaining the computer room environment, hardware, connectivity, applications, data, and restoration.
3. Access Control Policies: Enhance access control policies to increase the confidentiality and integrity of data.
4. Account Management Policies: Implement robust policies to reduce the attack surface and limit the overall impact from disgruntled or former employees.

Technical Controls:

1. Intrusion Detection System (IDS): Deploy an IDS to quickly identify possible intrusions and anomalous traffic.
2. Backups: Implement regular and reliable backups to support ongoing productivity and align with the disaster recovery plan.
3. Password Management System: Implement a password management system that enables password recovery, reset, and lockout notifications.

Physical Controls:

1. Locking Cabinets (for network gear): Secure network infrastructure gear by implementing locking cabinets to prevent unauthorized access and modifications.
2. Locks: Enhance the security of physical and digital assets by implementing robust lock mechanisms.

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

Administrative Controls:

1. Password Policies: Establish password strength rules to improve security and reduce the likelihood of account compromise through brute force or dictionary attacks. This control has a low priority.

Technical Controls:

1. Encryption: Implement encryption to make confidential information and data more secure, particularly for website payment transactions. This control has a medium priority.

Physical Controls:

1. CCTV Surveillance: Deploy CCTV surveillance to provide preventative and detective capabilities, reducing the risk of certain events and aiding investigations after incidents. This control has a medium priority.

Summary/Recommendations: Botium Toys is undergoing a comprehensive security audit that covers their entire security program, including assets, internal processes, and procedures. The audit aims to identify strengths, weaknesses, and areas for improvement to enhance overall security posture. The company is committed to adhering to the NIST CSF, a set of cybersecurity guidelines and best practices. Critical findings include the need to implement controls such as least privilege, disaster recovery plans, access control policies, and account management policies. Technical controls like intrusion detection, backups, and password management are also important. While password policies, encryption, and CCTV surveillance are lower priority findings, they should still be addressed to further strengthen security.