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: (Your Name)
DATE: (Today’s Date)
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

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

Critical findings (must be addressed immediately):

- Compliance – develop policies and procedures for
  - General Data Protection Regulation (GDPR)
  - Payment Card Industry Data Security Standard (PCI DSS)
  - System and Organizations Controls (SOC Type 1, SOC Type 2)
- Administrative controls that need to be put in place
  - Least Privilege
  - Password Policies
  - Account Management Policies
  - Separation of duties
- Technical controls that need to be put in place
  - Intrusion Detection System (IDS)
  - Encryption
  - Backups
  - Password Management System
  - Antivirus (AV) Software
  - Manual Monitoring, maintenance, and intervention
- Physical controls that need to be put in place
  - Locking cabinets (for network gear)
  - Locks
  - Fire Detection and Prevention

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

- Administrative controls that need to be put in place
  - Disaster Recovery Plans
  - Access Control Policies
- Physical controls that need to be put in place
  - Time- controlled safe
  - Adequate lighting
  - Closed-Circuit Television (CCTV) Surveillance
  - Signage Indicating Alarm Service Provider

Summary/Recommendations:

Currently Botium Toys does not meet the compliance requirements for expanding their online presence in the US and abroad. SOC type 1 and SOC type 2 based policies and procedures need to be developed to protect data from unauthorized access. PCI DSS is a standard for storing, accepting, processing, and transmitting credit card information so BT needs to develop policies and procedures to adhere to PCI DSS. GDPR protects EU citizen user data within the EU and abroad, so BT needs to develop policies and procedures to ensure that EU citizens data is secure.

Also, there are several administrative, technical, and physical controls that BT needs to implement immediately to meet compliance and to ensure that the CIA triad is maintained, if CT decides to expand. However, that is not all, there are a few administrative and physical controls CT needs to address but not immediately to meet the goals laid out in this internal audit. Please see the Critical Findings and Findings sections above for those items that need to be addressed.