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 HYPERLINK "https://docs.google.com/document/d/1DWmu8rVrIY\_vGR3nRCUl7sxekN2fGRYypcF6ej8YheA/template/preview"goals](https://docs.google.com/document/d/1DWmu8rVrIY_vGR3nRCUl7sxekN2fGRYypcF6ej8YheA/template/preview)
* 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: Derek Skinner  
DATE: 6/7/2023  
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.

**Goals:**

* Adhere to the National Institute of Standards and Technology Cybersecurity Framework.
* Establish a better process for their systems to ensure they are compliant.
* Fortify system controls.
* Adapt to 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):

* These critical findings must be implemented immediately:
* Control of Least Privilege and Separation of Duties
* Disaster recovery plans
* Password, access control, and account management policies, including the implementation of a password management system
* Encryption
* Intrusion Detection System
* Backups
* Antivirus (AV) software
* Closed-Circuit Television (CCTV) surveillance
* Locks
* Manual monitoring, maintenance, and intervention for legacy systems
* Policies need to be developed and implemented to meet PCI DSS and GDPR compliance requirements.
* Policies need to be developed and implemented to align to SOC1 and SOC2 guidance related to user access policies and overall data safety.

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

The following controls should be implemented when possible:

* Time-controlled safe
* Adequate lighting
* Locking cabinets
* Signage indicating alarm service provider

**Summary/Recommendations:**

Based on the audit findings, it is crucial to address the critical findings immediately to mitigate potential risks and ensure compliance. The implementation of controls such as Least Privilege and Separation of Duties, disaster recovery plans, strong password and access management policies, encryption, intrusion detection, backups, antivirus software, CCTV surveillance, locks, and legacy system monitoring is paramount for strengthening the security posture.

Additionally, it is recommended to develop and implement policies aligned with PCI DSS and GDPR compliance requirements, as well as adhere to SOC1 and SOC2 guidance for user access policies and overall data safety. These measures will enhance the organization's security, protect sensitive data, and mitigate potential vulnerabilities.

Furthermore, while not immediately critical, addressing the findings related to time-controlled safe, adequate lighting, locking cabinets, and signage indicating the alarm service provider will contribute to improving the physical security of the premises.

It is essential to prioritize these recommendations and allocate the necessary resources to address the identified gaps promptly. Regular monitoring, maintenance, and reassessment of the implemented controls and procedures will help maintain a robust and secure IT environment.