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: Christian Puebla
DATE: 8/20/2023
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:

We will be conducting a comprehensive assessment of several key systems within the organization, including accounting, endpoint detection, firewalls, intrusion detection systems, and the SIEM tool. Our assessment will encompass three critical aspects:

Current User Permissions: We will thoroughly examine the existing permissions granted to users within these systems. Our goal is to ensure that users have the appropriate levels of access and privileges that match their specific roles and responsibilities.

Current Implemented Controls: Our assessment will delve into the controls that are currently in place for each of these systems. We will analyze the various security mechanisms, policies, and practices that have been implemented to mitigate risks and uphold the security of sensitive data.

Current Procedures and Protocols: We will carefully review the documented procedures and protocols that govern the utilization and management of these systems. This encompasses a wide range of operational guidelines, incident response strategies, and procedural documentation.

The overarching objective of this assessment is to confirm that the existing user permissions, controls, procedures, and protocols align seamlessly with the compliance requirements stipulated by both the Payment Card Industry Data Security Standard (PCI DSS) and the General Data Protection Regulation (GDPR). These regulatory frameworks are known for their stringent demands in terms of data security and privacy.

To achieve this alignment with PCI DSS and GDPR requirements, our assessment will specifically focus on the following key areas:

- User Permissions: We will rigorously validate that user access to sensitive data adheres to the principle of granting the least privilege necessary. This approach ensures that individuals are only granted access to the information that is directly relevant to their designated tasks.
- Controls: Our assessment will closely examine the technical and procedural controls that are currently in place. This scrutiny ensures that mechanisms are established to protect data, identify breaches, and prevent unauthorized access.
- Procedures and Protocols: We will confirm that the established procedures and protocols are in accordance with the guidelines mandated by PCI DSS and GDPR. This includes verifying the effectiveness of incident response procedures, data retention policies, and privacy protocols.

Furthermore, our evaluation will also account for the technology that is currently utilized, covering both hardware components and the means of accessing these systems. This comprehensive approach ensures that all facets of the organization's technological landscape are taken into consideration during the assessment, encompassing both physical and digital security measures.

In conclusion, our assessment of these pivotal systems is driven by the goal of ensuring that the current user permissions, controls, procedures, and protocols seamlessly align with the rigorous demands of PCI DSS and GDPR compliance. By conducting this meticulous evaluation, we aim to identify any potential gaps and ensure that the organization's data security and privacy measures are robust and fully compliant.

Goals:

Follow the guidance provided by the NIST Cybersecurity Framework (NIST CSF).

- Create an enhanced system approach to ensure alignment with compliance standards.
- Strengthen and reinforce system controls.
- Embrace the principle of granting minimum necessary permissions for managing user credentials.

- Develop and formalize organizational policies and procedures, including comprehensive playbooks.
- Verify that all compliance obligations are consistently met.

Critical findings :

A range of controls must be formulated and put into effect in order to achieve the audit objectives. These controls encompass:

- The implementation of the "Least Privilege" and "Separation of Duties" principles to ensure restricted access.
- The formulation of disaster recovery strategies to tackle unforeseen disruptions.
- The establishment of policies governing passwords, access control, and account management, including the deployment of a robust password management system.
- The integration of encryption mechanisms for secure online transactions.
- Intrusion Detection Systems (IDS) to detect unauthorized access.
- System backups to safeguard data.
- Anti-virus (AV) software to fend off malware threats.
- Closed-circuit television (CCTV) for physical security monitoring.
- Locking mechanisms to protect physical assets.
- Hands-on monitoring, upkeep, and intervention for legacy systems.
- Implementation of fire detection and prevention systems.

In addition to controls, it is imperative to craft and enforce policies that align with the compliance requirements of both PCI DSS and GDPR.

Furthermore, policies need to be formulated and put into practice to ensure alignment with the guidance outlined in SOC1 and SOC2, specifically concerning user access policies and overall data security.

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

It is recommended to put in place the following controls whenever feasible:

- Utilize time-controlled safes.
- Ensure sufficient lighting in relevant areas.
- Employ locking cabinets to secure valuable items.
- Display signage that indicates the presence of an alarm service provider.

Summary/Recommendations:

It is advisable to promptly address significant compliance issues with respect to PCI DSS and GDPR, given that Botium Toys accepts online payments from customers worldwide, including those in the European Union (EU). Moreover, as part of the audit's objectives involving the adoption of the principle of least permissions, it is recommended to incorporate the guidance provided by SOC1 and SOC2 regarding user access policies and the overall safeguarding of data.

Given the global nature of online transactions and the potential risks, having robust disaster recovery plans and reliable backups is of paramount importance to ensure the continuity of business operations in the face of any unforeseen incidents. Integrating an Intrusion Detection System (IDS) and Anti-Virus (AV) software into the existing systems would enhance the organization's capability to identify and mitigate potential risks. This is particularly crucial considering that certain legacy systems necessitate manual monitoring and intervention.

To bolster the security of assets housed at Botium Toys' central physical location, it is advisable to utilize locks and Closed-Circuit Television (CCTV) systems. These measures serve to both secure physical assets, including equipment, and to provide monitoring and investigation capabilities for any potential threats.

While not immediately imperative, the organization could enhance its security posture by considering the implementation of encryption, as well as incorporating additional measures such as a time-controlled safe, ensuring adequate lighting, employing locking cabinets, and installing fire detection and prevention systems. The inclusion of signage indicating the presence of an alarm service provider would further contribute to bolstering security measures.

Collectively, these recommendations aim to enhance Botium Toys' overall security framework, aligning it with industry best practices and compliance requirements, and mitigating potential risks that could impact the organization's operations and customer trust.