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: Alexis Perez-Gomez
DATE: August 15, 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 covered a comprehensive evaluation of Botium Toys' cybersecurity program, particularly focusing on user permissions, controls, procedures, and protocols for accounting, end point detection, firewalls, intrusion detection system, and the Security Information and Event Management (SIEM) tool. Furthermore, the audit ensured alignment with necessary compliance requirements and considered both hardware and system access.

Goals:

- Improve Botium Toys' security posture by aligning with industry best practices, particularly with reference to the NIST CSF.
- Offer actionable mitigation recommendations based on identified high-risk vulnerabilities.
- Identify and align with compliance regulations, especially concerning business location and payment processing methods.

Critical findings (must be addressed immediately):

- Inadequate Asset Management: There's a clear lack of systematic asset management, making it difficult to ensure the security and compliance of all assets.
- Absence of Controls: Many systems, especially legacy systems, lack necessary controls, increasing the organization's vulnerability.
- Non-compliance Risks: There's a high risk of non-adherence to U.S. and international regulations, particularly GDPR and PCI DSS, which can lead to severe penalties and loss of customer trust.

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

- Password Policies: While there might be some measures in place, strengthening password policies can significantly reduce account compromise risks.
- Physical Controls: Enhancements like better lighting, more comprehensive CCTV surveillance, and fire detection/prevention measures should be considered for overall safety and asset protection.
- Legacy System Maintenance: Although not immediate, strategies should be in place to phase out end-of-life systems that require manual monitoring, reducing long-term vulnerabilities.

Summary/Recommendations: The audit highlights crucial vulnerabilities that pose significant risks to Botium Toys. It's essential to prioritize the implementation of recommended controls, starting with the critical findings to mitigate high-risk vulnerabilities. In addition, aligning with compliance standards like GDPR and PCI DSS will not only ensure regulatory adherence but will also bolster customer and

stakeholder trust. Long-term plans should also be set in motion to address findings of lesser immediacy, ensuring a holistic improvement in Botium Toys' security posture.
Best regards,

Alexis Perez-Gomez