Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Shahid Foy
DATE: May 5th, 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 will focus on existing user permissions, controls, procedures, and protocols within various systems including accounting, endpoint detection, firewalls, intrusion detection systems, and Security Information and Event Management (SIEM) tools. This audit will address current user permissions and technology to check that they are in compliance with necessary requirements.

Goals: The goal is to get Botium Toys in compliance with regulatory requirements and practice the NIST Cybersecurity Framework. The company seeks to establish robust processes to ensure compliance throughout their systems and networks. Concepts like least permissions are considered high priority as well.

Critical findings (must be addressed immediately):

- Policies need to be implemented to address PCI DSS to handle credit card information. GDPR should be addressed to handle personal information of residents residing in the E.U.
- Controls for Least Privilege and Separation of Duties
- Disaster recovery plans should be implemented to back up servers and databases.

- Develop policies that align with SOC1 and SOC2

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

- Adequate lighting
- Locking cabinets
- Locks
- Time-controlled safe

Summary/Recommendations: The company should focus on the critical findings specifically compliance with PCI DSS and GDPR. This will allow for the company to handle payments internationally and help them stay compliant with the E.U. Guidance from SOC1 and SOC2 can be utilized to implement Lease Privileges and Separation of Duties. Lastly the company should focus on creating Disaster recovery plan to help with business continuity. The company can also look into utilizing different detection software to identify malware or unwanted intrusion by installing antivirus software and Intrusion Detection Systems.