**Stakeholder Memorandum**

TO: IT Manager, Stakeholders

FROM: John Lizano

DATE: 3 OCTOBER 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 following systems are in scope: accounting, endpoint detection, firewalls, intrusion detection systems, security information, and event management (SIEM) tools. The systems are being accessed for:
  + Current user permissions
  + Current implemented controls
  + Current procedures and protocols
* Ensure current user permissions, controls, procedures, and protocols align with necessary compliance requirements.
* Ensure current technology is accounted for both hardware and system access.

**Goals**

* Adhere to the NIST CSF.
* 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 include their playbooks.
* Ensure they are meeting compliance requirements.

**Critical Findings** (must be addressed immediately)

* Various controls must be reviewed and utilized to meet audit goals. The controls include:
  + Control of Least Privilege and Separation of Duties
  + Disaster recovery plans
  + Intrusion Detection System (IDS)
  + Backups
  + Manual monitoring, maintenance, and intervention for legacy systems
  + Password, access control, and account management policies, including the implementation of a password management system
  + Encryption
  + Policies need to be formulated and utilized to meet PCI DSS and GDPR compliance requirements.
  + Policies must be formulated and utilized to align with SOC1 and SOC2 guidance related to user access policies and sensitive data.

**Summary/Recommendations:** The critical findings about compliance with PCI DSS and GDPR should immediately be addressed since Botium Toys accepts online payments worldwide. Also, immediately developing appropriate policies and procedures through the guidance of SOC1 and SOC2’s user access policies and data safety will fulfill the goal of adapting the concept of least permissions. It is important to implement disaster recovery plans and backups are critical to support business continuity in the event of a breach. Additionally, implementing an IDS system will help identify and mitigate potential risks through effective intrusion detection since legacy systems require manual monitoring and intervention. To further secure legacy systems, it is recommended to clearly state intervention methods and establish a schedule to monitor and maintain them. Password policies should be revised with a focus on current minimum password complexity requirements to improve Botium Toy’s security posture.