**Stakeholders Memorandum for Botium Toys**

**To**: IT Manager, Stakeholders

**From**: Esene Priscilla

**Date**: 29th January, 2024.

**Subject**: Internal IT Audit Findings and Recommendation.

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings and recommendation.

**Scope**: The scope of the audit was to assess the entire security program at Botium Toys which includes all assets, internal processes and procedures.

**Goal**: The goal of the audit was to assess and determine control and compliance best practices needed to be implemented to improve Botium Toys’ security posture.

**Critical Findings**: The Cybersecurity analyst made a list of the current assets owned by Botium Toys. After, all existing assets being managed by the IT department was assessed and it was discovered that there was an inadequate management of assets. The potential impact from the loss of an asset was assessed as Medium. Also, proper controls were not in place and Botium Toys was not fully compliant with the US and International regulations and standards of keeping critical data private and secure as all staff had access to internally stored data and may be able to access cardholder data and customers’ PII/SPII. The risk score was rated high (8 on a scale of 10) due to a lack of controls and adherence to compliance best practices.

**Findings**: The analyst discovered that the IT department is currently not using an Intrusion detection system. Also, there was no backup for critical data as well as no regular schedule for legacy systems. There was no centralized password management system and password policy was not in line with current minimum password complexity requirement which could affect productivity in the case of a breach.

**Recommendations:** Multiple controls need to be implemented to improve Botium Toys security posture and to ensure confidentiality of sensitive information. Based on the findings, the following controls are hereby recommended;

1. The principle of least privilege should be implemented to reduce the risk of a breach as well as separation of duties to reduce the possibility of fraud or access to critical data.
2. Encryption is needed to provide greater confidentiality of customers’ credit card information.
3. Password policies should follow the current minimum password complexity requirements (at least eight characters, a combination of letters and at least one number, special characters). The password management system should be implemented to improve employee productivity.
4. Intrusion detection system is highly recommended to help identify possible intrusions by threat actors.
5. Disaster recovery plans and backups of critical data should be in place to ensure business continuity in the case of a breach.

**Compliance**

Password management policies and confidentiality of customers’ financial information should be in adherence to the Payment Card Industry Data Securing Standards (PCI DSS). Also, current assets should be properly classified and data should be kept private and secure according to the General Data Protection Regulation (GDPR). In addition, user access policies, authorization and encryption should comply with the System and Organizations Controls (SOC type 1, SOC type 2).