**TO:** IT Manager, stakeholders

**FROM:** Olanrewaju Adesina

DATE: 25/01/2024

**SUBJECT:** Internal IT audit findings and recommendations for Botium Toys

**Scope**:

The scope is defined as the entire security program at Botium Toys. This includes accessing all assets alongside internal processes and procedures related to the implementation of controls and compliance best practices such as accounting, end point detection, firewalls, intrusion detection system.

The systems will be evaluated for:

Current user permissions, current implemented controls, current procedures and protocols, password policies, encryption method, disaster recovery plan, backups, and compliance with PCI DSS and GDPR requirements.

**Goals**:

The goal of the security audit is to assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve Botium Toys’ security posture. The assessment will include checking if the company:

* Adhere to the NIST CSF.
* Establish a process for their systems to ensure they are compliant.
* Fortify system controls.
* Adopt secure password management policies and the concept of least permissions when it comes to user credential management.
* Implement data encryption procedures.
* Establish policies and procedures, which includes their playbooks.
* Ensure they are meeting compliance requirements such as GDPR, PCI DSS.

**Risk Score**

On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to compliance best practices which will be evaluated below.

**Critical findings (should be addressed immediately):**

Multiple controls that needs to be developed and implemented to meet the audit goals, include:

* Implementation of the Principle of Least Privilege and Separation of Duties.
* Establishing, access control, and account management.
* Disaster recovery plans should be put in place to ensure business continuity.
* Data encryption.
* Backups of critical data, in the case of a breach, to ensure business continuity.
* Intrusion Detection System (IDS) should be put in place.
* Policies need to be developed and implemented to meet PCI DSS and GDPR compliance requirements.
* Policies need to be developed and implemented to align to SOC1 and SOC2 guidance related to user access policies and overall data safety.

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

The following controls should be implemented when possible:

* Clear procedures/policies and regular schedule for manual monitoring, maintenance, and intervention for legacy systems.

**Summary/Recommendations:**

It is recommended that critical findings relating to compliance with PCI DSS and GDPR be promptly addressed since Botium Toys’ online presence is growing and it accepts online payments from customers worldwide, including the E.U. Additionally, SOC1 and SOC2 guidance related to user access policies, data integrity, sensitive data encryption and overall data safety should be used to develop appropriate policies and procedures to improve the company’s security posture. Having disaster recovery plans and backups is also critical to the business continuity in the event of an incident.

Additionally, it is recommended that the company should implement the Principle of Least Privilege and Separation of Duties to reduce the risk of an internal and external breach and the possibility of fraud/access to critical data by company employees. Establishing, access control, and account management policies, including the implementation of a password management system to prevent easy access will also help secure data and other assets.

To further improve the security posture of Botium Toys, integrating an Intrusion Detection System into the current systems will support our ability to identify and mitigate potential risks, since there are existing legacy systems which require manual monitoring and intervention. Data encryption should also be used to provide greater confidentiality of sensitive information (PII/SPII).

While not necessary immediately, having clear policies and procedures with a regular schedule for manual monitoring, maintenance, and intervention for legacy systems will reduce the chances of a security breach.