BOTIUM TOYS: SCOPE, GOALS, AND RISK ASSESSMENT REPORT

SCOPE AND GOALS OF THE AUDIT

**Scope:** The scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures related to the implementation of controls and compliance best practices.

**Goals:** 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.

CURRENT ASSETS

Assets managed by the IT Department include:

● On-premises equipment for in-office business needs

● Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.

● Storefront products available for retail sale on site and online; stored in the company’s adjoining warehouse

● Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management

● Internet access

● Internal network

● Data retention and storage

● Legacy system maintenance: end-of-life systems that require human monitoring

RISK ASSESSMENT

Risk description

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper controls in place and may not be fully compliant with U.S. and international regulations and standards.

CONTROL BEST PRACTICES

The first of the five functions of the NIST CSF is Identify. Botium Toys will need to dedicate resources to identify assets so they can appropriately manage them.

Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity.

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.

ADDITIONAL COMMENTS

The potential impact from the loss of an asset is rated as medium, because the IT department does not know which assets would be at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure.

RECOMMENDATIONS

After the assessment of the existing assets, the following controls are recommended:

* Access controls pertaining to least privilege and separation of duties should be implemented
* Disaster recovery plans such as backups of critical data needs to be put in place
* 4There should be centralized password management system that will enforce the password policy’s minimum requirements
* While firewalls and Antivirus software are acknowledged, there is need for other technical controls like Intrusion Detection Systems and encryption to further strengthen the existing assets protection
* There should be regular schedule in place for monitoring, maintenance and intervention of legacy systems.

Also, the regulations of the following frameworks should be strictly followed for compliance:

* Payment Card Industry Data Security Standard (PCI DSS)
* General Data Protection Regulation (GDPR)
* System and Organizations Controls (SOC type 1, SOC type 2)