**BOTIUM TOYS ASSESSMENT REPORT**

**Scope:** Scope of this audit is to assess and ensure Botium Toys IT practices, internal processes and procedures meets industry and organization standards.

**Goal:** The goals of the audit is to assess the existing assets and check to to determine the controls and compliance practices that needs to be incorporated to improve Botium Toys capability to manage its defense of critical assets, data and react to change

**Current assets**

Assets managed by the IT Department include

* Internet access
* Internet network
* Employee Equipment: End-user devices (desktops, laptops, smartphones), remote workstations, cables, keyboards, mice, docking stations, surveillance cameras etc
* Management of systems, software and services: accounting, telecommunication, database, security, e-commerce and inventory management
* Data retention and storage
* End-of-life systems that require human monitoring
* Storefront products available for retail sale on site and online; stored in the company’s adjoining warehouse.

**RISK ASSESSMENT**

**Existing Risk**

Botiun Toys does not have all the proper controls in place and may not be fully compliant with U.S. and international standards and regulations. Botium Toys presently does not have adequate management of assets.

**Control Practices**

Botium Toys will need to dedicate resources to identify assets so they can monitor them and identify potential security issues being the first function stated in NIST Cybersecurity control framework. Secondly, they will also need to separate duties to prevent individuals from carrying out fraudulent or illegal activities. Thas is no one should be given so many chances that can misuse system. Moreso, they need to classify existing assets and determine the effect of loss of existing assets including systems on business continuity.

**Risk Score**

Due to a lack of controls and adherence to compliance best practices, the risk score is high and rated 7 on the scale of 1 to 10.

**Recommendations**

Botium Toys needs to implement multiple controls to improve their security posture and to ensure the confidentiality, integrity and availability of sensitive information. The controls including: Intrusion detection system, disaster recovery plans, password policies, separation of duties, least privilege, encryption.

The company needs to properly classify assets, in other to address the gaps in compliance, to improve their security posture and better protect sensitive information. They also need to implement controls such as least privilege, separation of duties and encryption.