Risk Audit of Botium Toys

1. *Current Asset Evaluation:*

- 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.

- Management of systems, software, and services: accounting, telecommunications, database, security, e-commerce, and inventory management.

- Internet access.

- Internal network.

- Vendor access management.

- Data center hosting services.

- Data retention and storage.

- Badge readers.

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

2. *Risk Description:*

Currently, there is inadequate asset management. Additionally, Botium Toys lacks proper controls and may not be compliant with U.S. and international regulations and standards.

3. *Control Best Practices:*

The first of the five functions of the NIST Cybersecurity Framework is Identify. Botium Toys will need to allocate resources to asset management. Additionally, they will need to determine the impact of the loss of existing assets, including systems, on business continuity.

4. *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 necessary compliance regulations and standards.

5. *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 lost. The likelihood of a lost asset or fines from governing bodies is high because Botium Toys does not have all the necessary controls in place and is not adhering to required regulations and standards related to keeping customer data private.

Audit Recommendations:

- Establish a robust asset management process that includes an up-to-date inventory of all organization assets.

- Implement adequate controls in systems and services used by Botium Toys, such as access controls, firewalls, and intrusion detection systems.

- Conduct a comprehensive review of regulations and standards applicable to the industry of Botium Toys, both at the national and international level, and ensure full compliance.

- Develop and document clear policies and procedures related to information security, including password management, customer data privacy, and security incident response.

- Allocate adequate resources to the cybersecurity department, including hiring additional cybersecurity personnel.

- Conduct regular audits to assess and continuously improve the security posture of the organization.