**To: Manager, Heads of unit**

**From: Martins Olu**

**Date: July 3rd, 2023**

**Subject: Security Auditing Report for Botium Toys Company**

1. **Summary of the Scope of audit**

The audit was interested in investigating the threats, risks and vulnerabilities in the physical & digital assets, technologies, protocols, and procedures of the organization’s IT infrastructure and how they contribute to the organization’s current security posture and compliance. This audit also examined the alignment of current user permissions, controls with necessary compliance requirements. Audit covered business units including accounting, telecommunication, database, security, ecommerce, and inventory management.

1. **Summary of the audit goals**

The goals of this audit include:

1. Adherence to all relevant and necessary regulations including the GDPR, PCI DSS, CIS, etc.
2. Observance of all relevance frameworks including NIST RMF & CSF, CTF, etc.
3. Implement all relevant security control principles including defence-in-depth, least privilege access, authentication, encryption, authorization, reducing attack surface area, etc.
4. Fortify system controls using different combinations of technical, administrative, and physical controls including MFA, access control, firewall, etc.
5. Establish that protocols, procedures and processes reflect prescriptions from all relevant playbooks.
6. **Critical findings**
7. **Compliance issues**

It was discovered that the organization lacked compliance with many widely used regulations and standards within the US and internationally e.g., GDPR, PCI DSS. Similarly, the organization had no compliance with relevant security frameworks such as System and Organizations Controls (SOC type 1, SOC type 2), NIST CSF, etc.

1. **Inadequate security control**

Second, it was discovered that there were huge lapses in the enforcement of security controls in everyday procedures and protocols. this precipitates a lack of controls regarding user permission and access.

1. **Other findings**
2. **Huge attack surface area**

Finally, there remains a huge attack surface area given the significant lack of asset control of its technologies, especially those at end-of-life capacity with huge security maintenance appetite. These shortcomings combine to produce a significantly high-risk score for the company.

1. **Summary/recommendations**

Bootium toys has substantial security controls and compliance gaps that need to be quickly attended to. Failure to fix these gaps poses strong risks to the security and business continuity of the organization. To reduce the risk score and avoid the potential financial and reputation damage arising from threat actions, it is recommended that Botium Toys takes the following steps to improve their security posture and level of compliance.

1. ***High priority controls***: these are crucial controls that must be implemented without delay. They have the highest vulnerability and any breach of these poses an existential risk to data, reputation, and business continuity. These are Least Privilege, Password policies, Access control policies, Account management policies, Separation of duties, Intrusion Detection System (IDS), Encryption, Antivirus (AV) software, Locks, and Fire detection and prevention.
2. ***Medium and Low priority controls***: these are controls that are although crucial can either be attended to in the near future or are already available but simply needed some updating. They include Signage indicating alarm service provider, Locking cabinets, CCTV, Time-controlled safe, Adequate lighting, Manual monitoring, maintenance & intervention, Password management system, Backups, and Disaster recovery plans.
3. ***Compliance***

Botium Toys would need to implement processes, controls and protocols that observe and comply with regulatory standards and framework guidelines. Immediate examples include Payment Card Industry Data Security Standard (PCI DSS), GDPR, NIST Cybersecurity Framework (CSF). Failure to implement compliance would soon cause security incidents that would affect user data and financial costs.