**Botium Toys – Final Security Audit Report**

**Prepared by:** Tsegbemi Oghenetega Ukubeyinje  
**Date:** April 23, 2025

## **Executive Summary**

Following a recent security audit of Botium Toys, several critical gaps were identified in the company’s technical controls and compliance practices. This report outlines prioritized recommendations aligned with frameworks such as NIST CSF, PCI DSS, GDPR, and SOC 2. Timely implementation of these measures is essential to reduce organizational risk, prevent data breaches, and maintain regulatory compliance.

## **Scope and Goals**

**Scope:**  
The scope of this audit encompasses Botium Toys’ entire security program, including IT-managed assets, internal systems, on-premise and remote infrastructure, data storage, and network operations.

**Goals:**

* Identify and assess current assets
* Evaluate technical, administrative, and physical controls
* Identify compliance gaps and assign risk scores
* Recommend improvements to enhance security posture

## **Risk Assessment Summary**

* **Risk Score:** 8/10 (High)
* **Key Issues Identified:**
  + Inadequate asset classification and inventory
  + Absence of key security controls (IDS, backups, encryption)
  + Non-compliance with GDPR and PCI DSS standards
  + Weak password policies and no centralized password management

## **High-Priority Recommendations (Immediate Action)**

1. **Intrusion Detection System (IDS)**  
   Risk: Breaches may go undetected.  
   Recommendation: Deploy a network-based IDS for real-time monitoring.
2. **Data Encryption**  
   Risk: Sensitive customer/payment data exposed.  
   Recommendation: Encrypt data at rest and in transit across all systems.
3. **Password Management System**  
   Risk: Vulnerability due to reused/weak passwords.  
   Recommendation: Implement a centralized password manager with MFA.
4. **Disaster Recovery Plan**  
   Risk: Prolonged downtime and data loss during incidents.  
   Recommendation: Develop, test, and regularly update a DR plan.
5. **GDPR Compliance Implementation**  
   Risk: Legal/regulatory penalties for data mishandling.  
   Recommendation: Finalize data classification and breach protocols.

## **Medium-Priority Recommendations (3–6 Months)**

1. **Legacy System Maintenance**  
   Recommendation: Set a formal schedule for patching and manual monitoring.
2. **Separation of Duties**  
   Recommendation: Enforce access boundaries to reduce insider risk.
3. **SOC 2 Control Alignment**  
   Recommendation: Establish policies for user access, availability, and data integrity.

## **Compliance Best Practices**

### ****PCI DSS Enhancements****

* Restrict access to credit card data
* Encrypt transaction data
* Apply secure password practices

### ****GDPR Improvements****

* Classify and inventory E.U. customer data
* Ensure 72-hour breach notification readiness
* Document data handling procedures

## **Conclusion**

The findings of this audit highlight significant risks that Botium Toys must address to ensure data security, maintain operational resilience, and avoid regulatory penalties. Implementing the outlined recommendations will not only reduce vulnerabilities but also strengthen the company's overall cybersecurity maturity.

**Prepared by:**  
Tsegbemi Oghenetega Ukubeyinje  
📧 tsegbemiukubeyinje@gmail.com  
Security Analyst