**Botium Toys Security Audit Report**

**Prepared By:** Muhammad Murtaza   
**Framework Referenced:** NIST Cybersecurity Framework (CSF)  
**Date:** 4/16/2025

**Executive Summary**

As Botium Toys continues to expand its online presence, the demand for a robust and secure IT infrastructure has intensified. This internal security audit evaluates the organization’s current cybersecurity posture using the NIST Cybersecurity Framework. The audit highlights deficiencies in administrative, technical, and physical controls, assesses compliance with industry regulations, and recommends corrective actions to mitigate potential risks.

**Audit Scope and Objectives**

This audit was conducted to:

* Assess the security of internal systems, infrastructure, and data.
* Identify and evaluate potential risks, threats, and vulnerabilities.
* Verify compliance with PCI DSS (for online payment processing) and GDPR (for operations involving EU customers).
* Provide actionable recommendations in alignment with NIST CSF.

**Risk Assessment Overview**

**Overall Risk Score:** 8/10

**Key Risk Areas:**

* Absence of encryption for sensitive and regulated data.
* Lack of defined access control and account management procedures.
* No formal disaster recovery or backup systems in place.
* Weak or nonexistent identity and password management practices.

**Controls and Compliance Review**

**A. Administrative / Managerial Controls**

| **Control** | **Control Type** | **Implementation Status** | **Recommendations** |
| --- | --- | --- | --- |
| Least Privilege | Preventative | Not Implemented | Adopt role-based access controls to minimize internal threats. |
| Disaster Recovery Plan | Corrective | Not Implemented | Develop and regularly test a comprehensive recovery strategy. |
| Password Policies | Preventative | Partially Implemented | Update password requirements for complexity, length, and expiration. |
| Access Control Policies | Preventative | Not Implemented | Define access levels and approval workflows. |
| Account Management Policies | Preventative | Not Implemented | Introduce formal user account lifecycle procedures. |
| Separation of Duties | Preventative | Not Implemented | Implement division of critical responsibilities. |

**B. Technical Controls**

| **Control** | **Control Type** | **Implementation Status** | **Recommendations** |
| --- | --- | --- | --- |
| Firewall | Preventative | Implemented | Confirm periodic updates and rule review. |
| IDS/IPS | Detective | Not Implemented | Deploy intrusion detection/prevention mechanisms. |
| Data Encryption | Deterrent | Not Implemented | Encrypt sensitive data to comply with GDPR and PCI DSS. |
| Data Backups | Corrective | Not Implemented | Initiate automated and secured backup processes. |
| Password Management Systems | Preventative | Not Implemented | Implement a centralized, secure password manager. |
| Antivirus Software | Corrective | Implemented | Ensure ongoing monitoring and threat intelligence updates. |
| Patch Management | Preventative | Partially Implemented | Establish a regular update and patching routine. |

**C. Physical / Operational Controls**

| **Control** | **Control Type** | **Implementation Status** | **Recommendations** |
| --- | --- | --- | --- |
| Time-Controlled Safe | Deterrent | Not Implemented | Consider for high-value physical assets. |
| Adequate Lighting | Deterrent | Implemented | Continue regular maintenance and inspections. |
| CCTV Surveillance | Preventative / Detective | Implemented | Confirm retention policies and data security. |
| Locking Cabinets | Preventative | Unknown | Audit and secure all networking and storage equipment. |
| Alarm Signage | Deterrent | Unknown | Install visible and clear security signage. |
| Physical Locks | Preventative | Implemented | Review for proper access control enforcement. |
| Fire Detection/Prevention | Preventative / Detective | Implemented | Ensure inspection and certification is current. |

**Compliance Assessment**

**PCI DSS:**  
Non-compliant due to lack of encryption, backup procedures, access control, and audit trail mechanisms.

**GDPR:**  
At risk of non-compliance due to insufficient data encryption, weak access controls, and lack of a formal breach response strategy.

**NIST CSF Alignment:**  
Significant improvement required across the Identify, Protect, and Detect categories.

**Strategic Recommendations**

**Immediate Actions**

* Encrypt all customer and sensitive business data.
* Implement access control and password policies.
* Design and implement a disaster recovery and data backup plan.

**Short-Term Improvements**

* Deploy intrusion detection/prevention systems.
* Update and enforce password complexity rules.
* Introduce role separation to mitigate internal risk.

**Long-Term Goals**

* Establish a culture of continuous monitoring and improvement.
* Conduct regular staff training on cybersecurity best practices.
* Schedule quarterly internal audits and annual compliance checks.

**End of Report**