**Company:** Botium Toys  
**Auditor:** Sami Naeeb  
**Date:** 21/02/2025  
**Audit Scope:** Internal IT Security Controls and Compliance  
**Framework:** NIST Cybersecurity Framework (NIST CSF), PCI DSS, GDPR, SOC 2

**1. Introduction**

The purpose of this internal security audit is to assess Botium Toys' current security posture, identify risks, and recommend improvements to enhance data protection and regulatory compliance. This audit evaluates key security controls, access management, encryption, system integrity, and compliance with industry standards such as PCI DSS, GDPR, and SOC frameworks.

**2. Findings and Observations**

**Access Control and Data Security**

* Currently, all employees have access to internally stored data, including cardholder data and customers’ PII/SPII, which increases the risk of unauthorized access.
* Least privilege and separation of duties have not been implemented, which could lead to potential misuse of sensitive information.
* User access policies have not been clearly defined or enforced.
* **Recommendation:** Implement strict access control policies and role-based access management to restrict access to only those who require it.

**Encryption and Secure Transactions**

* Encryption is not currently used for storing or transmitting customers’ credit card information, leaving data vulnerable to breaches.
* **Recommendation:** Adopt encryption protocols to secure credit card data at all transaction touchpoints.

**Compliance with GDPR**

* There is a plan in place to notify E.U. customers within 72 hours in case of a data breach.
* Privacy policies, procedures, and processes have been established but need reinforcement across departments.
* **Recommendation:** Strengthen GDPR compliance by properly classifying and inventorying customer data and ensuring privacy policies are strictly followed.

**System Integrity and Maintenance**

* The IT department has ensured data integrity measures are in place.
* Firewalls are configured correctly and follow security best practices.
* Antivirus software is installed and regularly monitored.
* An intrusion detection system (IDS) has not been installed.
* Legacy systems are monitored but do not follow a strict maintenance schedule.
* **Recommendation:** Deploy an IDS to enhance threat monitoring and establish a regular maintenance schedule for legacy systems.

**Disaster Recovery and Backup Plans**

* There are no documented disaster recovery plans in place.
* Critical business data is not regularly backed up, creating a high risk of data loss.
* **Recommendation:** Develop a formal disaster recovery plan and implement automated backups for critical data.

**Password Management and Security**

* Password policy requirements are outdated and not aligned with current security best practices.
* No centralized password management system is in place, causing inefficiencies in password recovery processes.
* **Recommendation:** Enforce strong password policies (minimum eight characters, a mix of uppercase, lowercase, numbers, and special characters) and implement a centralized password management system.

**3. Conclusion and Next Steps**

The security audit has identified several critical areas that require immediate attention, including access control, encryption, password security, and disaster recovery planning. Addressing these vulnerabilities will significantly enhance Botium Toys’ overall security posture.

The next steps involve implementing the recommended security controls, enforcing stricter compliance measures, and scheduling regular security reviews to maintain data integrity and business continuity.

**Prepared by:**  
**Sami Naeeb**