Botium Toys Security Audit & Compliance Report

Executive Summary

This report evaluates Botium Toys' current security controls, identifies gaps, and provides clear and practical recommendations. It demonstrates the ability to read and interpret risk assessments, understand compliance needs, and communicate findings in a hybrid format suitable for both technical and non-technical audiences.

Scope of Assessment

The assessment covers all organizational assets, including employee devices, internal network systems, data storage, credit card processing systems, physical security, administrative controls, and compliance with PCI DSS, GDPR, and SOC 2. The goal was to determine what controls are currently in place and identify missing or insufficient controls.

Company-Provided Control Information

- All employees currently have access to internally stored data.
- No encryption is used for customer or credit card information.
- Least privilege and separation of duties are not implemented.
- A firewall is in place and blocks traffic based on defined security rules.
- Antivirus software is installed and monitored.
- No intrusion detection system (IDS) is installed.
- There are no disaster recovery plans and no backups of critical data.
- Password policy exists but is weak and not enforced through a password manager.
- No centralized password management system exists.
- Legacy systems require manual monitoring with no fixed schedule.
- Physical security is strong, including locks, CCTV, and fire detection systems.
- A plan exists to notify E.U. customers within 72 hours of a breach.

Key Findings

- **High Risk:** Missing encryption, no backups or disaster recovery plan, excessive employee access.
- **Medium Risk:** Weak password policy, missing password management tool, incomplete asset classification.
- **Low Risk:** Manual legacy monitoring, strong physical controls already in place.

Recommendations (With Simple Explanations)

Implement Least Privilege: Only allow employees to access the data required for their jobs. This reduces damage if an account is compromised.

Introduce Separation of Duties: Split responsibilities so no one person controls critical tasks, reducing insider threats.

Enable Encryption for Sensitive Data: Protects credit card data and personal information so that even if stolen, it cannot be read.

Create Disaster Recovery & Backup Plans: Allows the company to recover quickly from system failures, breaches, or data loss incidents.

Deploy an Intrusion Detection System (IDS): Helps detect suspicious activity early and warns the IT team of potential attacks.

Strengthen Password Policies: Higher complexity requirements make passwords harder to guess or crack.

Add a Password Management System: Allows users to create and store strong passwords securely, improving compliance.

Classify and Inventory Assets: Knowing what hardware and data exist helps determine what needs protection and what controls to apply.

Schedule Legacy System Maintenance: Regular upkeep reduces the likelihood that outdated systems become weak points.

What I Learned

This project helped build practical skills in analyzing security controls, interpreting compliance requirements, and identifying risks. It also improved the ability to communicate findings clearly in a format similar to what security analysts produce in real-world environments.