Date: 12 March, 2025
Auditor Name: Nazish Khalid

Project Overview

- **Company:** Botium Toys
- **Objective:** Conduct an internal IT audit to assess security controls and compliance gaps.
- **Frameworks Used:** NIST CSF, PCI DSS, GDPR, SOC 2
- **Deliverables:**
    - Audit Scope & Goals
    - Risk Assessment Report
    - Controls & Compliance Checklist
    - Remediation Plan & Recommendations
    - Final Executive Summary Report

Scope & Goals

- **Scope:**
  The audit covers all IT security aspects at Botium Toys, including employee devices, internal networks, software, and compliance with cybersecurity best practices.

- **Goals:**
  Identify security weaknesses, assess compliance gaps, and recommend improvements to protect data and ensure regulatory compliance.

Current IT Assets

- **Hardware:**
  On-site office equipment, employee devices (laptops, smartphones, peripherals), warehouse/storefront products.

- **Software & Systems:**
  Accounting, telecom, security, e-commerce, inventory, databases.

- **Network & Storage:**
  Internal network, data retention, legacy system maintenance, internet access.

Risk Assessment

- **Key Risks:**

    - Poor asset management.
    - Non-compliance with U.S. & international regulations (e.g., data privacy laws).
    - Lack of proper security controls.
- **Risk Score:** 8/10 (High Risk)

- **Potential Impact:** Medium to High. IT lacks full understanding of asset risks, and fines for compliance failures could be severe.

Security & Compliance Gaps

- **Major Issues:**

    - **Lack of Data Access Controls:** Employees can access sensitive customer payment data.

    - **No Encryption for Credit Card Data:** Payment information is stored without encryption.
    - **No Least Privilege Access:** Employees have more access than necessary.
    - **No Intrusion Detection System (IDS):** System monitoring is weak.
    - **No Disaster Recovery Plan & Backups:** No data recovery strategy if systems fail.
    - **Weak Password Policy:** No strict password requirements, no centralized password management.
    - **Unclear Legacy System Maintenance:** No clear update/maintenance schedule.
- **Moderate Issues:**
    - Data Integrity & Availability: Some security controls exist (firewall, antivirus).
    - EU Data Breach Notification Policy: In place, but overall compliance is unclear.
- **Strengths:**
    - **Physical Security:** Locks, CCTV, fire detection systems are working well.
    - **Firewall & Antivirus:** Properly configured and monitored.

Controls assessment checklist

Yes	No	Control
☐	☑	Least Privilege
☐	☑	Disaster recovery plans
☑	☐	Password policies
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	Antivirus software
☑	☐	Manual monitoring, maintenance, and intervention for legacy systems
☐	☑	Encryption
☐	☑	Password management system

☑	☐	Locks (offices, storefront, warehouse)
☑	☐	Closed-circuit television (CCTV) surveillance
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
☐	☑	Only authorized users have access to customers' credit card information.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
☐	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	☑	E.U. customers' data is kept private/secured.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☐	☑	Ensure data is properly classified and inventoried.
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice
☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is confidential/private.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☑	☐	Data is available to individuals authorized to access it.

Remediation Plan & Recommendations

Immediate Actions:

1. **Implement Least Privilege & Separation of Duties:**
    - Restrict access to customer payment data and personal information.
    - Ensure employees only have access to what they need for their job roles.
2. **Secure Credit Card Transactions:**
    - Encrypt all stored and transmitted credit card data in compliance with PCI DSS.
    - Limit access to payment data to authorized users only.
3. **Strengthen Password Security:**
    - Update the password policy to require longer passwords, special characters, and multi-factor authentication (MFA).
    - Implement a centralized password management system.

Short-Term Solutions:

1. **Deploy an Intrusion Detection System (IDS):**
    - Implement an IDS to monitor network activity and detect security threats in real-time.
2. **Establish a Disaster Recovery Plan & Regular Backups:**
    - Create and document a backup strategy for critical data.
    - Develop a business continuity plan to recover from unexpected failures.
3. **Classify & Inventory Sensitive Data (GDPR & SOC Compliance):**
    - Organize and document what data is stored, where it is located, and who has access.
    - Implement privacy controls for E.U. customers to comply with GDPR.

Long-Term Improvements:

1. **Maintain & Upgrade Legacy Systems:**
    - Set up a routine maintenance schedule and define clear intervention methods.
    - Develop a migration plan for replacing outdated systems.
2. **Enhance Physical Security Measures:**
    - Conduct regular security assessments of physical access controls, including CCTV monitoring and door locks.
    - Implement an access control system for employees to restrict unauthorized entry.
3. **Improve Compliance & Audit Readiness:**
    - Conduct regular internal IT audits to assess compliance with NIST CSF, PCI DSS, and GDPR.
    - Provide ongoing security training for employees to enforce best cybersecurity practices.

Executive Summary

This audit has highlighted critical gaps in security and compliance at Botium Toys, ranging from poor data access controls to lack of disaster recovery planning. Immediate, short-term, and long-term remediation steps have been outlined to address these issues, ensuring a more secure environment and improved compliance with industry standards. By implementing these recommendations, Botium Toys can significantly reduce risks, safeguard sensitive data, and be better prepared for future regulatory audits.