Cybersecurity Audit Report for Botium Toys

Prepared by: Ezechias KUMBU KUMBU, ICT Engineer
Date: February 19, 2025

1. Introduction

This audit report provides an assessment of Botium Toys' cybersecurity posture, integrating best practices from the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), International Organization for Standardization (ISO) 27001, and Control Objectives for Information and Related Technologies (COBIT) frameworks. The report identifies existing gaps, risks, and compliance issues, and provides recommendations to improve security and ensure regulatory compliance.

2. Audit Scope and Objectives

Scope:

- Review of the entire security program at Botium Toys, including on-premises and cloud-based assets.
- Analysis of employee equipment, internal networks, systems, and applications.
- Assessment of compliance with U.S. and international regulations (e.g., PCI DSS, GDPR).

Objectives:

- Identify security risks and vulnerabilities.
- Evaluate compliance with NIST CSF, ISO 27001, and COBIT.
- Recommend corrective actions and security enhancements.

3. Risk Assessment Summary

Risk Description	Impact	Likelihood	Risk Score (1-10)
Lack of asset management	High	High	8
Uncontrolled access to sensitive data	High	High	9
Lack of encryption for credit card data	Critical	High	10
No Intrusion Detection System (IDS)	Medium	High	7
No disaster recovery plan	Critical	Medium	9
Weak password policies	High	High	8
Legacy system vulnerabilities	Medium	High	7

4. Security Controls Assessment

4.1 Administrative Controls

Control	Type	Status
Least Privilege	Preventative	Not Implemented
Disaster Recovery Plans	Corrective	Not Implemented
Access Control Policies	Preventative	Partially Implemented
Separation of Duties	Preventative	Not Implemented

4.2 Technical Controls

Control	Type	Status
Firewall	Preventative	Implemented
IDS/IPS	Detective	Not Implemented
Encryption	Deterrent	Not Implemented
Antivirus Software	Preventative	Implemented
Password Management	Preventative	Not Implemented
Backups	Corrective	Not Implemented

4.3 Physical Controls

Control	Type	Status
CCTV Surveillance	Preventative/Detective	Implemented
Locks & Badge Readers	Preventative	Implemented
Fire Detection Systems	Preventative	Implemented

5. Compliance Alignment with NIST CSF, ISO 27001, and COBIT

5.1 NIST Cybersecurity Framework (CSF) Implementation

NIST CSF Function	Implementation Status
Identify	Partially Implemented
Protect	Partially Implemented
Detect	Not Implemented
Respond	Not Implemented
Recover	Not Implemented

5.2 ISO 27001 Controls Overview

- Asset Management: Partially Implemented
- Access Control: Not Implemented
- Cryptographic Controls: Not Implemented
- Incident Response: Not Implemented
- Business Continuity: Not Implemented

5.3 COBIT Governance Maturity Level

- Risk Management: Low Maturity
- Compliance & Audit: Low Maturity
- IT Governance: Medium Maturity

---

6. Recommendations

6.1 Immediate Actions (High Priority)

- Implement encryption for sensitive data to comply with PCI DSS and GDPR.
- Enforce least privilege and access control policies.
- Deploy an Intrusion Detection System (IDS).
- Establish a disaster recovery plan.

- Strengthen password policies and deploy a centralized password manager.

6.2 Medium-Term Actions

- Conduct regular risk assessments.
- Improve legacy system monitoring.
- Increase security awareness training for employees.

6.3 Long-Term Actions

- Fully align cybersecurity governance with ISO 27001 and COBIT.
- Establish a Security Operations Center (SOC) for continuous monitoring.

---

7. Conclusion

The current cybersecurity posture of Botium Toys presents significant risks, particularly in data protection, access control, and compliance. Immediate action is required to enhance security measures, reduce vulnerabilities, and ensure compliance with industry standards. This report serves as a roadmap for improving the company's security infrastructure and achieving compliance with best practices.