Botium Toys: Scope, Goals, and Risk Assessment Report

Scope and Goals of the Audit

Scope: *The audit encompasses Botium Toys' entire security program, including its assets such as employee devices, internal network, and systems. This includes reviewing assets, controls, and compliance practices.*

Goals: *Evaluate existing assets and complete a controls and compliance checklist to identify areas needing improvement to enhance Botium Toys' security posture.*

Current Assets:

- ***On-premises Equipment:*** *Devices for in-office business needs.*
- ***Employee Equipment:*** *Desktops, laptops, smartphones, headsets, keyboards, mice, docking stations, surveillance cameras.*
- ***Storefront Products:*** *Retail products stored on-site and in the warehouse.*
- ***System Management:*** *Accounting, telecommunication, database, security, ecommerce, and inventory systems.*
- ***Internet Access & Internal Network***
- ***Data Retention & Storage***
- ***Legacy Systems:*** *End-of-life systems requiring manual monitoring.*

Risk Assessment:

Risk Description:

- *Inadequate asset management.*
- *Missing key controls and non-compliance with U.S. and international standards.*

Control Best Practices:

- *Identify and classify assets per NIST CSF guidelines.*
- *Assess the impact of asset loss on business continuity.*

Risk Score: *8/10 (High)*

Additional Comments:

- ***Data Access:*** *Unrestricted employee access to sensitive data.*
- ***Encryption:*** *Missing for credit card data.*
- ***Access Controls:*** *No least privilege or duty separation.*
- ***Security Tools:*** *Firewall and antivirus installed; no IDS.*
- ***Disaster Recovery:*** *No backup or recovery plans.*
- ***Password Policy:*** *Weak standards and no centralized management.*
- ***Legacy Systems:*** *Monitored but without a clear schedule.*
- ***Physical Security:*** *Locks, CCTV, and fire detection systems in place.*

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.

Recommendations:

- Implement encryption for sensitive data.
- Enforce least privilege and duty separation policies.
- Establish a disaster recovery and backup plan.
- Strengthen password policies and adopt a password management system.
- Install an intrusion detection system (IDS).
- Schedule regular maintenance for legacy systems.

These measures will reduce risks and enhance Botium Toys' security posture.