Controls and compliance checklist

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.

- [x] [ ] Data integrity ensures the data is consistent, complete, accurate, and has been validated.
- [x] [ ] Data is available to individuals authorized to access it.

Summary

Review of Scope, Goals, and Risk Assessment Report

Scope and Goals of the Audit:

Scope:

>Comprehensive review of Botium Toys' entire security program.

>Assessment of all assets including on-premises equipment, employee devices, retail products, and IT systems.

>Evaluation of internal processes and procedures for control implementation and compliance.

Goals:

>Identify and assess existing assets.

>Complete controls and compliance checklist to identify necessary improvements.

>Enhance Botium Toys' security posture by implementing required controls and best practices.

Current Assets:

>On-premises business equipment.

>Employee devices (desktops, laptops, smartphones, etc.).

>Retail products stored on-site and in the warehouse.

>Systems and services management (accounting, telecommunication, database, security, ecommerce, inventory management).

>Internet access and internal network.

>Data retention and storage.

>Legacy systems requiring human monitoring.

Risk Assessment:

Risk Description:

>Inadequate asset management.

>Lack of proper controls and potential non-compliance with regulations.

>Need for asset identification and classification to manage them effectively.

Risk Score:

>Score: 8 out of 10 (high risk).

>Impact: Medium due to unknown at-risk assets.

>Compliance Risk: High due to insufficient controls and non-adherence to regulations.

Control Best Practices and Issues:

>All employees have access to sensitive data (PII/SPII).

>No encryption for customer credit card information.

>Lack of least privilege and separation of duties controls.

>Firewall and antivirus software in place.

>No intrusion detection system (IDS) or disaster recovery plans.

>No backups of critical data.

>Notification plan for E.U. customers in case of a breach.

>Inadequate password policies and no centralized password management system.

>Physical security measures (locks, CCTV, fire detection) are sufficient.

Conclusion

<>Botium Toys has several critical controls missing, such as least privilege, separation of duties, IDS, backups, and encryption.

<>Compliance with PCI DSS and SOC requirements is inadequate, posing significant risks.

<>GDPR compliance is better but still needs improvement in data classification and inventory.