Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories document.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently have this control 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.)

To complete the compliance checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each compliance regulation, review the controls, frameworks, and compliance reading.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

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.

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

Recommendations (optional): In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.

Summary of Recommendations for Botium Toys

Based on the controls assessment, compliance gaps, and high-risk score (8/10), the following recommendations are prioritized to reduce risks and improve security posture:

1. Administrative/Managerial Controls

Implement Least Privilege & Separation of Duties

- **Why:** All employees currently have unrestricted access to sensitive data (e.g., cardholder data, PII).

- **Action:** Restrict access to critical systems/data based on roles. Separate duties to prevent single points of compromise.

Develop Disaster Recovery Plans & Regular Backups

- **Why:** No backups or recovery plans exist, risking business continuity during incidents.
- **Action:** Create and test a disaster recovery plan. Schedule automated backups for critical data.

Strengthen Password Policies & Centralized Management

- **Why:** Weak password requirements and manual resets hinder security and productivity.
- **Action:** Enforce minimum complexity (e.g., 12+ characters, special symbols). Deploy a centralized password management system.

Establish Compliance Training & Asset Classification

- **Why:** Employees lack awareness of compliance obligations (PCI DSS, GDPR).
- **Action:** Train staff on data handling and regulatory requirements. Classify data (e.g., PII, SPII) to prioritize protection.

2. Technical Controls

Deploy Encryption for Sensitive Data

- **Why:** Credit card data is unencrypted, violating PCI DSS and GDPR.
- **Action:** Encrypt data at rest and in transit, especially for payment processing and customer PII.

Install Intrusion Detection System (IDS)

- **Why:** No IDS exists to detect malicious activity, increasing breach risks.
- **Action:** Implement an IDS/IPS to monitor network traffic for anomalies.

Enhance Legacy System Maintenance

- **Why:** Manual, irregular monitoring of legacy systems creates vulnerabilities.
- **Action:** Create a maintenance schedule and automate alerts for legacy systems.

3. Physical/Operational Controls

Review Physical Access Controls

- **Why:** While locks and CCTV are in place, gaps in access logs or badge systems may exist.
- **Action:** Implement badge readers/access logs for restricted areas (e.g., server rooms).

4. Compliance Priorities

PCI DSS Requirements

- Restrict credit card data access to authorized personnel only.
- Secure card data environments (e.g., encrypted storage, secure transmission).

GDPR Obligations

- Formalize a 72-hour breach notification process for E.U. customers.
- Conduct a data inventory to ensure proper classification and protection of E.U. data.

SOC Compliance

- Document user access policies and validate data integrity controls.
- Ensure data availability aligns with SOC requirements (e.g., redundancy).

5. Additional Urgent Actions

Conduct a Risk Assessment Update

- Re-evaluate assets and risks after control implementation to adjust priorities.

Regular Audits & Third-Party Testing

- Perform penetration testing and compliance audits to validate controls.

Impact of Inaction: Failure to address these gaps risks significant fines (e.g., GDPR penalties up to 4% of global revenue), reputational damage from breaches, and operational disruption due to unmitigated cyberattacks.

Existing Strengths to Build On: Firewall, antivirus, CCTV, and physical locks provide a foundation. Expand these with layered controls (e.g., IDS, encryption) for defense-in-depth.
By addressing these recommendations, Botium Toys can reduce its risk score, achieve compliance, and safeguard critical assets.