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.

Audit Recommendations

Based on the audit findings, the following actions are recommended to bring Botium Toys into compliance with PCI DSS and GDPR, and to align with the NIST Cybersecurity Framework.

Priority 1: Critical & Immediate Actions (Fix these NOW)

- **Implement Encryption (PCI DSS Requirement):**
  - Immediately migrate the e-commerce website from HTTP to **HTTPS** using TLS 1.2 or higher.
  - Ensure all credit card data stored or transmitted is encrypted to prevent theft during a breach.
- **Establish Separation of Duties:**
  - Revoke "Super Admin" access for general staff.
  - Create distinct user roles so that the employee who *approves* a payment is not the same person who *processes* it. This prevents internal fraud.
- **Enforce Least Privilege:**
  - Conduct a User Access Review. Remove access to sensitive customer data for any employee who does not strictly need it for their daily job function.

Priority 2: High Priority (Fix within 30 days)

- **Develop & Enforce Policies:**
  - Draft and sign a formal **Password Policy** requiring a minimum of 12 characters and complexity (numbers/symbols).
  - Implement **Multi-Factor Authentication (MFA)** for all internal accounts to stop credential stuffing attacks.
- **Disaster Recovery Plan:**
  - Implement an automated daily backup solution for the customer database.
  - Store one backup copy "off-site" (e.g., in a secure cloud bucket) to ensure data survives a physical fire or server crash (Availability).

Priority 3: Medium Priority (Fix within 90 days)

- **GDPR Compliance Updates:**
  - Update the website to include a "Cookie Consent" banner for E.U. visitors.
  - Create a "Data Privacy Policy" page explaining how customer data is used and how they can request deletion.
- **Legacy System Management:**
  - Identify all "Legacy" (outdated) software. Isolate these systems from the main internet network until they can be replaced or patched.