

Controls and compliance checklist

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

Controls assessment checklist

Yes	No	Control
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Least Privilege
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Disaster recovery plans
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Password policies
<input type="checkbox"/>	<input type="checkbox"/>	Separation of duties
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Firewall
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Intrusion detection system (IDS)
<input type="checkbox"/>	<input type="checkbox"/>	Backups
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Antivirus software
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Manual monitoring, maintenance, and intervention for legacy systems
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Encryption
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Password management system
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Locks (offices, storefront, warehouse)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Closed-circuit television (CCTV) surveillance
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Fire detection/prevention (fire alarm, sprinkler system, etc.)

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
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Only authorized users have access to customers’ credit card information.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
<input type="checkbox"/>	<input checked="" type="checkbox"/>	E.U. customers’ data is kept private/secured.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
<input type="checkbox"/>	<input type="checkbox"/>	Ensure data is properly classified and inventoried.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	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
<input type="checkbox"/>	<input checked="" type="checkbox"/>	User access policies are established.
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sensitive data (PII/SPII) is confidential/private.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Data is available to individuals authorized to access it.

Recommendations:

To enhance Botium Toys security posture and compliance, the following controls and best practices should be implemented:

1. **Asset Management:** Establish an asset inventory system to classify and track all assets, including hardware, software, and data. Implement regular asset audits to ensure proper management.
2. **Access Controls:** Enforce least privilege and separation of duties to minimize unauthorized access. Implement role-based access controls (RBAC) and monitor access logs.
3. **Data Protection:**
 - Use encryption for all sensitive data, including customers' credit card information and PII/SPII, in transit and at rest.
 - Implement secure password policies with centralized password management tools to enforce complexity and rotation requirements.
4. **Incident Detection and Response:** Deploy an Intrusion Detection System (IDS) to monitor and alert suspicious activities. Develop and implement disaster recovery and business continuity plans, including regular data backups.
5. **Compliance and Training:** Ensure adherence to U.S. and international data privacy regulations, such as GDPR and PCI DSS. Conduct regular employee training on security policies and compliance requirements.

6. **Policy Enforcement:** Update the password policy to align with industry standards. Automate enforcement using password management solutions to enhance productivity and security.
7. **Legacy Systems:** Establish a scheduled maintenance plan for legacy systems and document intervention protocols to ensure reliability and minimize risks.
8. **Physical Security:** Maintain robust physical security measures, including lock systems, CCTV surveillance, and fire prevention mechanisms.