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:

To strengthen Botium Toys' security posture here are the steps I recommend:

1. **Classifying and Inventorying All Company Assets.** Knowing what devices, data, and systems you have makes it easier to prioritize protections, stay organized, and ensure nothing important gets overlooked.
2. **Implement Least Privilege Access Controls** – Giving employees access only to what they need for their role creates safer workflows and builds trust in your systems.
3. **Establish Separation of Duties** – By dividing responsibilities for key processes like customer data handling or financial approvals, you reduce risk.

4. **Introduce Strong Encryption** – Encrypting sensitive data (both in transit and at rest) will help protect your customers and support compliance with regulations like PCI DSS and GDPR.
5. **Adopt Clear Password Policies and a Password Manager** – These tools make it easier for the team to follow best practices and reduce the burden of remembering secure passwords.
6. **Build and Test a Disaster Recovery Plan** – Having a plan in place ensures you're ready to respond quickly and effectively if anything goes wrong.
7. **Deploy an Intrusion Detection System (IDS)** – An IDS will help you catch unusual activity early and keep your environment safe without relying solely on manual monitoring.
8. **Set Up Regular Maintenance for Legacy Systems** – Older systems still in use can be supported with scheduled check-ins and extra attention until they're ready to be replaced.
9. **Strengthen Physical and Endpoint Security** – Locking down access points, using antivirus, and ensuring surveillance and fire systems are in place rounds out our protection of both digital and physical spaces.

In terms of compliance, these changes will help Botium Toys align with best practices for PCI DSS, GDPR, and SOC 2. Some areas to focus on include encrypting payment data, limiting access to customer information, ensuring timely breach notifications for E.U. customers, and creating documented user access policies.

Taking these steps will reduce risk and create a more secure and supportive environment for the company.