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 <u>scope, goals, and risk assessment report</u>. For more details about each compliance regulation, review the <u>controls, frameworks, and compliance</u> reading.

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

Compliance checklist

<u>Payment Card Industry Data Security Standard (PCI DSS)</u>

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.

<u>General Data Protection Regulation (GDPR)</u>

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.

Yes	No	
☑	☐	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.

1. **Limit Access to Sensitive Info**
   Right now, everyone can see internal data, including customer info. It is necessary to limit access so only the right people can view or change it. This will protect data from mistakes and risks.

2. **Create a Backup and Recovery Plan**
   If something goes wrong—like a cyberattack or system crash—there are no backups or a recovery plan. It is recommended to set up automatic backups and write a step-by-step recovery plan to keep the business running smoothly.

3. **Improve Password Rules and Use a Password Manager**
   The current password setup is too weak. Need to implement stronger rules (like longer passwords with numbers and symbols and a capital letter) and a tool to safely store them so employees don't forget or reuse them.

4. **Set Up Intrusion Alerts**
   Right now, there is no a system to alert if someone tries to break into the network. Necessary to install an intrusion detection system to catch threats early.

5. **Encrypt Private Data**
   Customer info—especially credit card data—is stored without encryption. This is a huge risk. It is a must encrypt sensitive data so no one can read it even if it's stolen.

6. **Organize and Label Data**
   It's important to classify and label all data so it can be better protected and managed.

7. **Set Clear User Roles and Access**
   Necessary to define exactly who can access what data and for what purpose. This makes things safer and more organized, and helps to comply with data privacy regulations.