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):

1. Access Control & Least Privilege

- **Implement Least Privilege Access:** Ensure employees have the minimum level of access required to perform their jobs. This reduces the risk of unauthorized access and helps limit the potential for internal threats.
- **Establish User Access Policies (SOC):** Define clear policies for accessing sensitive information, regularly review user access, and revoke permissions for users who no longer need them.

2. Disaster Recovery and Backup Management

- **Develop and Document Disaster Recovery Plans:** Implement a robust disaster recovery plan to ensure business continuity in case of disruptions. Regularly test the recovery process to validate effectiveness.
- **Automate and Secure Backups:** Regularly back up critical data and ensure it is stored securely, with access restricted to authorized personnel.

3. Password and Encryption Policies

- **Adopt Strong Password Policies:** Require complex passwords, and consider using a password management system to securely store and manage credentials.
- **Implement Data Encryption:** Encrypt sensitive data, especially when transmitting credit card information and personal data, to protect it from unauthorized access.

4. Network Security Controls

- **Install and Monitor Firewalls and IDS:** Ensure firewalls are in place to protect internal networks and deploy an Intrusion Detection System (IDS) to monitor and alert on suspicious activities.
- **Deploy Antivirus Software:** Regularly update and maintain antivirus software to detect and prevent malicious software threats.

5. Compliance with Data Protection Regulations

- **GDPR Compliance:** Protect E.U. customer data, and implement a data breach notification plan to inform affected parties within 72 hours. Inventory and classify data to maintain compliance and safeguard privacy.

- **PCI DSS Compliance:** Store, process, and transmit credit card data securely, limiting access to authorized users only. Encrypt transaction touchpoints and improve the overall security of payment environments.

6. Physical and Environmental Security

- **Secure Physical Access with Locks and CCTV:** Restrict physical access to sensitive areas with locks and monitor these areas with CCTV.
- **Install Fire Detection Systems:** Ensure fire alarms and sprinkler systems are operational to protect assets and data from potential fire damage.