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.

Based on the controls and compliance assessment, it's clear that Botium Toys needs to take immediate action to improve its security posture and ensure compliance with relevant standards. Here are the key recommendations:

1. **Implement Role-Based Access Control (RBAC):**
    - **Risk:** Lack of least privilege and separation of duties increases the likelihood of unauthorized access to sensitive data.
    - **Action:** Establish RBAC to ensure that employees only have access to the data necessary for their roles.
2. **Develop and Implement Disaster Recovery and Backup Plans:**
    - **Risk:** Absence of disaster recovery plans and backups could lead to significant data loss and prolonged downtime in the event of an incident.
    - **Action:** Create a comprehensive disaster recovery plan, including regular backups of critical data with off-site storage.
3. **Enhance Password Management and Security:**
    - **Risk:** Weak password policies and the lack of a centralized password management system increase the risk of unauthorized access.
    - **Action:** Strengthen password complexity requirements and implement a centralized password management system to enforce these policies.
4. **Deploy an Intrusion Detection System (IDS):**

- **Risk:** Without an IDS, there is no mechanism to detect or respond to potential intrusions, leaving the company vulnerable to undetected attacks.
- **Action:** Deploy an IDS to monitor network traffic for suspicious activity and potential breaches.

5. **Implement Data Encryption:**
   - **Risk:** Storing and transmitting unencrypted customer credit card information is a significant compliance violation and security risk.
   - **Action:** Encrypt all sensitive data, particularly payment card information, both at rest and in transit.
6. **Regularly Maintain and Monitor Legacy Systems:**
   - **Risk:** Irregular maintenance of legacy systems could lead to system failures and vulnerabilities.
   - **Action:** Establish a regular maintenance schedule and define clear intervention methods for legacy systems to ensure their reliability.
7. **Review and Improve Compliance with PCI DSS and GDPR:**
   - **Risk:** Non-compliance with PCI DSS and GDPR could result in heavy fines and damage to the company's reputation.
   - **Action:** Conduct a full compliance audit to identify and address any gaps, particularly in the areas of data encryption, access control, and data privacy.
8. **Classify and Inventory Data:**
   - **Risk:** Lack of proper data classification and inventory makes it difficult to protect sensitive data and comply with regulatory requirements.
   - **Action:** Implement a data classification policy to ensure that all data is properly categorized and protected according to its sensitivity.