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): 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.

Based on the controls assessment and compliance checklist, the following actions are recommended for the IT manager to reduce risks to critical assets and improve the overall security posture of **Botium Toys**:

1. **Implement least privilege access controls**
   Limiting user access strictly to what is necessary for their role reduces the risk of unauthorized access and insider threats.

2. **Develop and implement a disaster recovery plan**
   There is currently no plan to ensure business continuity. It is urgent to establish policies

and procedures for backing up and restoring critical data.

3. **Install an Intrusion Detection System (IDS)**
   The absence of an IDS poses a high risk of undetected unauthorized access or anomalous network activity. Implementing an IDS will allow proactive threat detection and response.

4. **Establish a password management system**
   Without a centralized system, current password policies are weak and inconsistently enforced, affecting both productivity and security.

5. **Encrypt credit card information**
   Encryption is currently not used to protect financial data, which is a violation of PCI DSS standards and a major risk for sensitive data exposure.

6. **Strengthen data classification and protection for personal information (PII/SPII)**
   To comply with **GDPR**, it is critical to inventory, classify, and protect data belonging to EU citizens and have an incident response plan in place that ensures notification within 72 hours.

7. **Formalize access control and separation of duties policies**
   Clear policies must be established and enforced to manage access to systems and data, and to ensure proper separation of critical duties to prevent abuse or errors.

8. **Schedule regular maintenance for legacy systems**
   The lack of planned monitoring for unsupported systems increases exposure to vulnerabilities. A maintenance schedule with specific intervention procedures should be defined.

9. **Adopt a comprehensive approach to data privacy and security**
   Enforcing consistent privacy policies and procedures aligned with SOC 2 and GDPR ensures the long-term confidentiality, integrity, and availability of organizational data.

These recommendations should be communicated to key stakeholders to prioritize resources and ensure compliance with applicable regulatory frameworks.