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:

Recommendation for Enhanced Security and Compliance

To strengthen Botium Toys' security posture and ensure compliance with industry standards, the following recommendations should be implemented:

1. **Access Control and Privilege Management:**

- Formalize and enforce user access policies that adhere to the principle of least privilege. Ensure that access permissions are granted based on job roles and responsibilities, minimizing the risk of unauthorized access.

2. **Data Confidentiality and Encryption:**
    - Enhance security controls to protect Personally Identifiable Information (PII) and Sensitive Personal Identifiable Information (SPII). Implement encryption protocols for data at rest and in transit to safeguard sensitive information from unauthorized disclosure.
3. **Integrity and Validation of Data:**
    - Implement data integrity controls to ensure that all information is accurate, complete, and validated regularly. Utilize data validation techniques and audit trails to maintain data integrity across systems.
4. **Data Availability and Authorized Access:**
    - Ensure that data is accessible only to authorized individuals as per established access control policies. Implement role-based access controls (RBAC), continuous monitoring of access logs, and regular reviews of access permissions.
5. **Disaster Recovery and Business Continuity:**
    - Develop comprehensive disaster recovery plans to ensure continuity of operations in the event of a disruption or security incident. Test and update these plans regularly to maintain effectiveness.
6. **Password Management:**
    - Strengthen password policies to include requirements for complexity, regular rotation, and the use of a centralized password management system. This will enhance security and reduce the risk of unauthorized access due to weak passwords.
7. **Intrusion Detection and Monitoring:**

- Implement intrusion detection systems (IDS) to proactively monitor network traffic and detect potential security breaches or anomalies. This will enable timely response and mitigation of security incidents.

8. **Compliance with Regulatory Standards:**
    - Ensure compliance with regulatory standards such as PCI DSS and GDPR by adopting best practices for data protection, privacy policies, and breach notification procedures.

Implementing these recommendations will enhance Botium Toys' ability to protect critical assets, mitigate security risks, and maintain compliance with industry regulations. These measures not only strengthen the organization's security posture but also build trust with customers and stakeholders.