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.

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.

Security Controls Implementation Plan for Botium Toys

1. Least Privilege:

- Implement the principle of least privilege by granting users only the minimum level of access necessary to perform their job duties.
- Regularly review user permissions and revoke any unnecessary access.

2. Disaster Recovery:

- Develop and implement a comprehensive disaster recovery plan that includes procedures for backing up data, recovering systems, and restoring operations in the event of a disaster.
- Test the disaster recovery plan regularly.

3. Password Policies:

- Implement strong password policies that require users to use complex passwords and change them regularly.
- Enforce password expiration and lockout policies.

4. Separation of Duties:

- Implement separation of duties to prevent any one individual from having complete control over critical processes or systems.
- For example, separate the duties of authorizing payments from the duties of processing payments.

5. Intrusion Detection System:

- Deploy an intrusion detection system (IDS) to monitor network traffic for suspicious activity.
- Configure the IDS to generate alerts when suspicious activity is detected.

6. Backups:

- Regularly back up all critical data to a secure offsite location.
- Test the backups regularly to ensure that they can be restored successfully.

7. Manual Maintenance and Intervention for Legacy Systems:

- Implement manual maintenance and intervention procedures for legacy systems that are not supported by the manufacturer.
- This includes regularly patching the systems and monitoring them for security vulnerabilities.

8. Encryption:

- Encrypt all sensitive data at rest and in transit.
- Use strong encryption algorithms and keys.

9. Password Management System:

- Implement a password management system to securely store and manage user passwords.
- The system should allow users to create strong passwords and store them securely.

10. Access Policies:

- Implement access policies to control who can access sensitive information.
- The policies should be based on the principle of least privilege.

11. Data Integrity:

- Implement data integrity controls to ensure that data is accurate, complete, and consistent.
- The controls should include data validation and verification procedures.