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.)

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 for Botium Toys:

1. **Implement Access Controls:**
   - Restrict access to internally stored data, especially cardholder data and customers' PII/SPII, based on the principle of least privilege.
   - Enforce separation of duties to ensure that employees only have access to the data necessary for their roles.

2. **Encrypt Sensitive Data:**
   - Utilize encryption mechanisms to ensure the confidentiality of customers' credit card information throughout its lifecycle, including when accepted, processed, transmitted, and stored locally.

3. **Deploy Intrusion Detection System (IDS):**
   - Install and configure an intrusion detection system (IDS) to monitor the network for suspicious activities and potential security breaches.
   -

4. **Develop Disaster Recovery Plans:**
   - Establish comprehensive disaster recovery plans to mitigate the impact of unexpected events and ensure business continuity.
   - Regularly backup critical data and test the recovery process to verify its effectiveness.

5. **Enhance Password Policy and Management:**
   - Update the password policy to align with current industry standards, including minimum password complexity requirements.
   - Implement a centralized password management system to enforce the password policy consistently and efficiently, reducing the need for IT intervention in password-related issues.

6. **Establish Regular Monitoring and Maintenance:**
    - Implement a schedule for monitoring and maintaining legacy systems to ensure their security and reliability.
    - Clearly define intervention methods and responsibilities for maintaining legacy systems.

7. **Continuously Train Employees:**
    - Provide regular security awareness training to all employees, emphasizing the importance of data protection, compliance, and best practices.

8. **Regularly Review and Update Security Measures:**
    - Conduct regular security assessments and audits to identify vulnerabilities and gaps in security measures.
    - Continuously update security controls and practices to adapt to evolving threats and compliance requirements.
9. **Document and Enforce Privacy Policies:**
    - Ensure that privacy policies, procedures, and processes are well-documented and enforced among IT department members and other employees to maintain data integrity and compliance.
    - Monitor Physical Security Measures: