Controls and compliance checklist

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:

To reduce risk (currently scored at 8/10) and improve compliance and cybersecurity maturity, Botium Toys should prioritize the following:

1. **Implement Least Privilege & Role-Based Access Control**
   Restrict access to sensitive data like credit card and customer info based on role. This aligns with both PCI DSS and SOC compliance requirements.

2. **Deploy Encryption for Sensitive Data**
   Encrypt cardholder and customer data both at rest and in transit to comply with PCI DSS and GDPR.

3. **Install an Intrusion Detection System (IDS)**
   An IDS will help detect abnormal traffic and provide real-time alerts for early threat mitigation.

4. **Develop and Test a Disaster Recovery Plan**
   Create and regularly test a documented disaster recovery plan to ensure business continuity in the event of system failure or breach.

5. **Establish a Secure Password Management System**
   Implement tools like password managers and enforce modern complexity rules and rotation policies.

6. **Set Up Regular Backups**

   Back up critical data on a daily or weekly basis, storing copies off-site or on secure cloud platforms.

7. **Formalize Monitoring of Legacy Systems**

   Schedule manual maintenance for legacy systems and document intervention protocols.

8. **Classify and Inventory All Assets**

   Begin asset identification and classification to strengthen control over sensitive data, fulfilling NIST CSF's Identify function.

9. **Conduct Regular Security Training**

   Make employees aware of their role in protecting customer data and complying with internal and external regulations.

10. **Prepare for External Audits**

    Address SOC 1/2 gaps now to ensure readiness for potential audits from business partners or regulators.