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.

Summary of Recommendations

To enhance Botium Toys' security and regulatory compliance, the following key actions are recommended:

1. Access Control: Limit employee privileges, ensure only authorized users can access sensitive data, and implement separation of duties.
2. Data Encryption: Protect sensitive data with robust encryption standards, both in transit and at rest.
3. Password Management: Update password policies and implement a centralized password management system.
4. Security Systems: Install intrusion detection systems (IDS) and conduct continuous monitoring with updated antivirus software.
5. Disaster Recovery and Backups: Develop a disaster recovery plan and configure automated backups for critical data.
6. Regulatory Compliance: Align privacy and security policies with international standards, such as GDPR.
7. Physical Security: Strengthen physical controls, such as locks and CCTV surveillance, at company facilities.
8. System Maintenance: Establish a regular schedule for monitoring and updating legacy systems and plan for their modernization.

Recommendations:

Review and Update Access Control Policies:

   - Ensure that only authorized personnel have access to sensitive customer data, including credit card information and PII/SPII. Implement "least privilege" access and separation of duties to reduce the potential for unauthorized access or misuse.

2. Implement Strong Encryption Practices:
   - Establish data encryption procedures for credit card information and sensitive customer data. This will help secure credit card transaction touchpoints and data both in transit and at rest.
3. Improve Password Management:
   - Update password policies to meet current security standards (e.g., minimum complexity requirements). Implement a centralized password management system to enforce these standards and enhance productivity.
4. Install and Maintain Key Security Systems:
   - Implement an intrusion detection system (IDS) and ensure continuous monitoring of all IT systems. Regularly update antivirus software to detect and mitigate threats.
5. Establish Disaster Recovery and Backup Procedures:
   - Develop a formal disaster recovery plan and ensure regular backups of critical data are performed. This will help prevent data loss in the event of an incident.
6. Ensure Compliance with Relevant Regulations:
   - Review and align privacy and security policies with U.S. and international regulations, such as GDPR, to ensure compliance and mitigate legal risks.
7. Enhance Physical Security:

- Strengthen the physical security of company facilities, including offices, storefronts, and warehouses. Implement strong locks, updated CCTV surveillance, and fire detection and prevention systems.

8. Upgrade and Maintain Legacy Systems:
   - Regularly monitor and update legacy systems. Establish a clear schedule for maintenance and implement a plan to eventually phase out outdated systems.