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.)

* Attention: when indicating yes and no, it means that the type of control exists but is not effective or is obsolete

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 Improve Botium Toys' Security Posture

1. Implement the Principle of Least Privilege:
   - Recommendation: Ensure that only authorized users have access to critical data and systems, including customer credit card information. Regularly review and update access permissions to ensure that only necessary personnel have access to sensitive information.
2. Develop and Implement Secure Password Management Policies:
   - Recommendation: Adopt robust password policies that include complexity requirements, length, and periodic password changes. Consider implementing a centralized password management system to facilitate compliance and reduce password fatigue.
3. Implement Data Encryption Procedures:
   - Recommendation: Encrypt credit card information during storage, processing, and transmission to protect it from unauthorized access. Ensure that sensitive data is encrypted both at rest and in transit.
4. Establish a Disaster Recovery Plan:
   - Recommendation: Develop and implement a disaster recovery plan to ensure business continuity in the event of a security breach or disaster. Regularly test and update the plan as needed.
5. Adopt a Comprehensive Backup Strategy:
   - Recommendation: Perform regular backups of all critical data and store them in a secure location. Verify the integrity of backups and conduct periodic recovery tests to ensure effective data restoration.
6. Implement an Intrusion Detection and Prevention System (IDS/IPS):
   - Recommendation: Install and configure an IDS/IPS to detect and prevent suspicious or malicious traffic on the network. Ensure the system is updated with the latest signatures and detection rules.
7. Ensure Compliance with Privacy and Data Protection Policies:

    - Recommendation: Review and strengthen privacy policies and procedures to ensure compliance with data protection regulations, such as GDPR. Implement processes to properly classify, document, and maintain data.
8. Strengthen Physical and Operational Controls:
    - Recommendation: Ensure that high-risk physical areas (offices, warehouses) are protected with adequate locks, CCTV systems, and fire detection and prevention measures. Implement controls to limit physical access to critical assets.
9. Conduct Continuous Monitoring and Maintenance:
    - Recommendation: Establish continuous monitoring and maintenance processes to identify and manage vulnerabilities in legacy systems and other critical infrastructure. Consider implementing a vulnerability management tool to automate this process.

These recommendations can help mitigate risks to Botium Toys' assets and enhance its overall security posture.