Controls Checklist Assessment

Control	In Place?
Least Privilege	No
Disaster recovery plans	No
Password policies	No
Separation of duties	No
Firewall	Yes
Intrusion detection system (IDS)	No
Backups	No
Antivirus software	Yes
Manual monitoring, maintenance, and intervention for legacy systems	No
Encryption	No
Password management system	No
Locks (offices, storefront, warehouse)	Yes
Closed-circuit television (CCTV)	Yes
Fire detection/prevention (fire alarm, sprinkler system, etc.)	Yes

Compliance Checklist Assessment

Payment Card Industry Data Security Standard (PCI DSS):

Best Practice	Adheres?
Only authorized users have access to customers' credit card information.	No
Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	No
Implement data encryption procedures to better secure credit card transaction touchpoints and data.	No
Adopt secure password management policies.	No

General Data Protection Regulation (GDPR):

Best Practice	Adheres?
E.U. customers' data is kept private/secured.	Yes
There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	Yes
Ensure data is properly classified and inventoried.	No
Enforce privacy policies, procedures, and processes to properly document and maintain data.	Yes

System and Organizations Controls (SOC type 1, SOC type 2):

Best Practice	Adheres?
User access policies are established.	No
Sensitive data (PII/SPII) is confidential/private.	No
Data integrity ensures the data is consistent, complete, accurate, and has been validated.	Yes
Data is available to individuals authorized to access it.	Yes

Recommendations

To reduce risks and improve Botium Toys' security posture, the following actions are recommended:

1. **Implement Access Controls**:
    - Enforce least privilege and separation of duties to minimize risk.
    - Establish robust user access policies.
2. **Enhance Data Security**:
    - Encrypt sensitive customer and payment data.
    - Adopt secure password management practices and systems.
3. **Develop Disaster Recovery Plans**:
    - Establish and regularly test disaster recovery and backup solutions to ensure business continuity.

4. **Install an Intrusion Detection System (IDS)**:
    - Implement IDS to monitor and alert on anomalous activity.
5. **Ensure Compliance with PCI DSS**:
    - Secure the storage, processing, and transmission of credit card data.
    - Limit access to cardholder information.
6. **Enhance GDPR Compliance**:
    - Properly classify and inventory data.
    - Review and strengthen privacy policies and procedures.
7. **Schedule Legacy System Maintenance**:
    - Create a regular schedule for maintaining and monitoring end-of-life systems to mitigate risks.