Controls and Compliance Checklist

Controls Assessment

Control	In place?
Asset Inventory and Classification	**No**
Access Controls (Least Privilege, Separation of Duties)	**No**
Encryption of Sensitive Data (e.g. credit card data, PII)	**No**
Firewall	**Yes**
Antivirus/Anti-malware	**Yes**
Intrusion Detection System (IDS)	**No**
Disaster Recovery and Data Backups	**No**
Password Policy (meets best practices)	**No**
Centralized Password Management	**No**
Physical Security (locks, CCTV, fire detection)	**Yes**
Data Integrity Controls	**Yes**
Privacy Policy and Breach Notification Procedures	**Yes**
Regular Legacy System Maintenance Schedule	**No**

Compliance Checklist

Compliance Best Practice	Does Botium Toys currently adhere to this best practice?
PCI DSS (Payment Card Industry Data Security Standard)	**No**
GDPR (General Data Protection Regulation)	**Partial** (Breach notification and privacy policy in place, but lack of access controls and encryption means not fully compliant)
SOC 1/SOC 2 (System and Organization Controls)	**No**

Recommendations (Optional, but Strongly Encouraged)

Top Priorities for Immediate Action:

1. **Implement Asset Inventory and Classification:**
   a. Begin by cataloging all IT assets and classifying data according to sensitivity and business impact.
2. **Enforce Access Controls:**
   a. Apply least privilege and separation of duties to restrict access to sensitive data (cardholder data, PII/SPII).
3. **Enable Encryption for Sensitive Data:**
   a. Encrypt all customer credit card data and PII both at rest and in transit.
4. **Establish Regular Data Backups and a Disaster Recovery Plan:**
   a. Develop and test a disaster recovery plan; schedule regular backups of all critical data.
5. **Upgrade Password Policies and Implement Centralized Management:**
   a. Update password requirements to meet industry standards and deploy a centralized password management system.
6. **Deploy an Intrusion Detection System (IDS):**
   a. Add IDS to monitor for unauthorized access or suspicious activity.
7. **Schedule Regular Legacy System Maintenance:**
   a. Create and enforce a maintenance schedule for legacy systems, including clear intervention procedures.

Compliance Actions:

- **PCI DSS:**
  - Immediately address encryption, access controls, and regular monitoring to meet PCI DSS requirements.
- **GDPR:**
  - Ensure technical and organizational measures for data protection, including access controls and encryption, are in place for all E.U. customer data.
- **SOC 1/SOC 2:**
  - Review and implement relevant controls for financial reporting and data security.

Summary for Stakeholders:

Botium Toys faces significant risks due to gaps in core security controls and incomplete compliance with major regulations. The risk of data breaches, regulatory fines, and business disruption is high. Immediate action is needed to implement missing controls, strengthen compliance, and protect company and customer data as the business grows.