Controls and compliance checklist

Does Botium Toys currently have this control in place?

- *NO*

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.)

Does Botium Toys currently adhere to this compliance best practice?

- *NO*

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 (optional):

Summary of Recommendations to the IT Manager:

1. **Asset Management and Classification**: Implement a comprehensive asset management system to identify, classify, and manage all assets effectively. This includes end-user devices, storefront products, management systems, and data storage.
2. **Access Controls and Encryption**: Enforce access controls, least privilege, and separation of duties to restrict unauthorized access to sensitive data, including cardholder and customer PII/SPII. Implement encryption measures to ensure confidentiality of credit card information stored locally.
3. **Intrusion Detection System (IDS)**: Install and maintain an intrusion detection system to detect and respond to potential security threats in real-time.
4. **Disaster Recovery and Backup**: Develop and implement disaster recovery plans to ensure business continuity in case of data loss or security breaches. Regularly backup critical data to prevent permanent loss.
5. **Password Policy and Management**: Strengthen the password policy to meet current minimum complexity requirements. Implement a centralized password management system to enforce policy compliance and streamline password recovery/reset processes.

6. **Legacy System Maintenance**: Establish a regular schedule for monitoring and maintaining legacy systems to ensure they are secure and functional.
7. **Compliance Adherence**: Ensure compliance with U.S. and international regulations and standards, particularly regarding data privacy and security. This includes GDPR requirements for timely notification of security breaches and maintaining updated privacy policies and procedures.
8. **Employee Training and Awareness**: Provide regular training and awareness programs for employees to educate them about security best practices and their role in maintaining a secure environment.

By implementing these recommendations, Botium Toys can mitigate the identified risks and improve its overall security posture, thereby protecting sensitive data and ensuring regulatory compliance.