Controls and compliance checklist

Security Audit checklist review.

Does Botium Toys currently have this control in place?

Controls assessment checklist

Yes	No	Control
☐	X	Least Privilege
☐	X	Disaster recovery plans
☐	X	Password policies
☐	X	Separation of duties
✔	☐	Firewall
☐	X	Intrusion detection system (IDS)
☐	X	Backups
✔	☐	Antivirus software

☐	X	Manual monitoring, maintenance, and intervention for legacy systems
☐	X	Encryption
☐	X	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
☐	X	Only authorized users have access to customers' credit card information.
☐	X	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
☐	X	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
☐	X	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	X	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.
☐	X	Ensure data is properly classified and inventoried.
☐	X	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
☐	X	User access policies are established.
☐	X	Sensitive data (PII/SPII) is confidential/private.
☐	X	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☐	X	Data is available to individuals authorized to access it.

Recommendations (optional): Customers' information such as PII/SPII is completely exposed. Even though Botium Toys has password policies, most passwords do not meet minimum requirements. The company does not adhere to any of the PCI DSS standards and doesn't protect user data. There is no separation of duties within the company, which

can lead to employees misusing the system or data. Botium Toys is exposed to data breaches, fines, customer complaints and loss of reputation which would potentially affect business continuity.