Controls and compliance checklist

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
X		Firewall
	X	Intrusion detection system (IDS)
	X	Backups
X		Antivirus software
	X	Manual monitoring, maintenance, and intervention for legacy systems
	X	Encryption
	X	Password management system
X		Locks (offices, storefront, warehouse)
X		Closed-circuit television (CCTV) surveillance
X		Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

Does Botium Toys currently adhere to this compliance best practice?

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 accepted, processed, transmitted, and stored 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.
X		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:
A lot of protocols need to be in place to improve Boitium's posture. This will ensure good security practices in terms of their sensitive information confidentiality, separation of duties and encryption.