Controls and compliance checklist

Does Botium Toys currently have this control in place?

Controls assessment checklist

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

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

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

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	n	E.U. customers’ data is kept private/secured.
y		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
y		Ensure data is properly classified and inventoried.
y		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
	n	User access policies are established.
y		Sensitive data (PII/SPII) is confidential/private.
y		Data integrity ensures the data is consistent, complete, accurate, and has been validated.
y		Data is available to individuals authorized to access it.

Recommendations:

The Botium Toys IT department is advised to implement the following preventative administrative controls:

- Least Privilege and Access Control Policies to help minimize risks related to insider threats or compromised accounts, as well as to support confidentiality and integrity by specifying which groups can access or modify data.
- Password Policies that align with current minimum requirements to decrease the likelihood of account compromise through brute force or dictionary attacks.
- Account Management Policies for overseeing account lifecycle in order to reduce the attack surface and mitigate risks stemming from former employees and default accounts.
- Separation of Duties to lower the potential impact of insider threats or compromised accounts.
- Development of a disaster recovery plan to maintain business continuity and ensure timely access to data backups.

Botium Toys is also advised to consider the following detective technical controls:

- IDS/IPS Intrusion Detection/Prevention Software to monitor and identify anomalous traffic patterns that may indicate security threats.
- Implementation of a deterrent technical control such as data encryption to protect customer credit card information processed and stored in internal systems.
- Password Management Systems to address password fatigue and reduce IT ticket submissions, enabling more effective monitoring and maintenance, including the replacement of legacy systems with up-to-date alternatives.

For physical deterrence, the following physical controls are recommended:

- Signage indicating alarm systems and service providers at all entryways and exits, accompanied by adequate lighting to ensure visibility and help reduce security risks.