Botium Toys – Controls and Compliance Checklist

Controls Assessment Checklist

Type an X in the “Yes” or “No” column to answer the question: Does Botium Toys currently have this control in place?

Yes	No	Control	Explanation
	X	Least Privilege	All employees have access to customer data; privileges need to be restricted to reduce breach risk.
	X	Disaster recovery plans	No disaster recovery plans exist; these are required for business continuity.
	X	Password policies	Password requirements are minimal and do not meet modern security standards.
	X	Separation of duties	Not implemented; increases risk of fraud and unauthorized access.
X		Firewall	A firewall is in place and blocks traffic based on defined security rules.
	X	Intrusion detection system (IDS)	No IDS is installed to detect potential intrusions.
	X	Backups	No backups of critical data are

			currently maintained.
X		Antivirus software	Antivirus software is installed and regularly monitored.
X		Manual monitoring of legacy systems	Legacy systems are monitored, but not on a regular or documented schedule.
	X	Encryption	Encryption is not used to protect sensitive or cardholder data.
	X	Password management system	No centralized password management system is in place.
X		Locks	Physical locks secure offices, storefront, and warehouse.
X		CCTV surveillance	CCTV systems are installed and functioning.
X		Fire detection/prevention	Fire alarms and prevention systems are operational.

Compliance Checklist

Type an X in the “Yes” or “No” column to answer the question: Does Botium Toys currently adhere to this compliance best practice?

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best Practice	Explanation
	X	Authorized access to credit card data only	All employees can access cardholder data.
	X	Secure storage and transmission of card data	Data is not encrypted and access is unrestricted.
	X	Encryption of cardholder data	Encryption is not implemented.
	X	Secure password management	Password policies are weak and no password manager exists.

General Data Protection Regulation (GDPR)

Yes	No	Best Practice	Explanation
	X	EU customer data is private and secure	Encryption is not used to protect sensitive data.
X		72-hour breach notification plan	A breach notification plan exists and meets GDPR timelines.
	X	Data classification and inventory	Assets are inventoried but not classified.
X		Privacy policies enforced	Privacy policies and procedures are documented and enforced.

System and Organization Controls (SOC 1 / SOC 2)

Yes	No	Best Practice	Explanation
	X	User access policies established	Least privilege and separation of duties are not implemented.
	X	Sensitive data confidentiality	PII/SPII is not encrypted.
X		Data integrity controls	Controls exist to ensure data integrity.
X		Data availability for authorized users	Data is available, but access authorization is too broad.

Recommendations (Optional)

Botium Toys should prioritize implementing least privilege, separation of duties, encryption, a centralized password management system, regular backups, disaster recovery planning, and an intrusion detection system. Asset classification should be completed to better align controls with compliance requirements and reduce overall organizational risk.