Untitled

Controls and compliance checklist

To complete the controls assessment checklist, refer to theinformation provided in the *scope, goals,and risk assessment report*. For more details about each control,including the type and purpose, refer to the *controlcategories* document.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently have this controlin place?*

Controls assessment checklist

Yes	No	Control
	x	Least Privilege
	x needs plan implemented	Disaster recovery plans
x needs updated		Password policies
	x	Separation of duties
x		Firewall
	x needs to get	Intrusion detection system (IDS)
	x needs a policy implemented to be sure to back up important data every so often	Backups
x		Antivirus software
x maybe change to something more up to date		Manual monitoring, maintenance, and intervention for legacy systems
	x start encryption process and include in policy all data needs to be encrypted to keep customers info and company data safe	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.)

To complete the compliance checklist, refer to the informationprovided in the *scope, goals,and risk assessment report*. For more details about each complianceregulation, review the *controls,frameworks, and compliance* reading.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to thiscompliance best practice?*

Compliance checklist

PaymentCard Industry Data Security Standard (PCI DSS)

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

GeneralData 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 they need to as well as encrypt	Ensure data is properly classified and inventoried.
	x they need to	Enforce privacy policies, procedures, and processes to properly document and maintain data.

Systemand Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice
	x access control needs implemented as well as a policy made	User access policies are established.
	x when they encrpt data it will be safe	Sensitive data (PII/SPII) is confidential/private.
x		Data integrity ensures the data is consistent, complete, accurate, and has been validated.

X nut also availavle to those who are not authorix		Data is available to individuals authorized to access it.

This section is *optional* and can be used to provide asummary of recommendations to the IT manager regarding which controls and/orcompliance best practices Botium Toys needs to implement, based on the riskposed if not implemented in a timely manner.

Recommendations (optional): Inthis section, provide recommendations, related to controls and/or complianceneeds, that your IT manager could communicate to stakeholders to reduce risksto assets and improve Botium Toys' security posture.