Controls and compliance checklist

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

Then, select "yes" or "no" to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

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

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

Then, select "yes" or "no" to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

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

General Data Protection Regulation (GDPR)

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

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

Recommendations (optional): In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.

Implement Data Encryption
Encrypt all sensitive customer data, including credit card and PII, to protect it from unauthorized access and ensure PCI DSS compliance. Encryption should cover all stages of data processing.

Establish Access Controls
Implement least privilege and separation of duties for access to sensitive data. This will reduce the risk of unauthorized data access and ensure compliance with both PCI DSS and SOC standards.

Deploy Intrusion Detection System (IDS)
Install an IDS to monitor network traffic for suspicious activities. An IDS will enhance network security and help the IT team respond swiftly to threats.

Create a Disaster Recovery Plan (DRP)
Develop a comprehensive DRP and backup protocol for critical data. Ensure that regular backups are conducted and securely stored to maintain business continuity in case of a disaster.

Upgrade Password Policies and Management
Strengthen password policies to align with industry standards (e.g., minimum length, complexity, regular updates). Implement a centralized password management system to enforce policies and streamline password resets.

Regular Maintenance for Legacy Systems
Establish a schedule for regular monitoring and maintenance of legacy systems. This will reduce the risk of system failures and improve overall operational efficiency.

Conduct Regular Compliance Audits
Schedule routine audits to ensure ongoing adherence to PCI DSS, GDPR, and SOC requirements. Use these audits to identify potential gaps and keep Botium Toys' security posture aligned with current regulatory standards.