Botium Toys:

Controls and compliance checklist

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.

- We are not operating under the principle of least privilege with regards to separation of duties pertaining to access management. Please investigate costs and implementation methodologies for utilizing a new password management system company-wide. This system should allow for customization of user permissions that can be reclassified by group, department, and administrative and support roles throughout the organization and should include strict monitoring of credential usage logging. (Bonus: if possible, utilize a system that can include HR oversight, and also allows user permissions and login credentials to be set during onboarding intake)
- We need an intrusion detection system immediately. Please reach out to ADT, Vivint, or Brinks to schedule a quote for installation of services and equipment.
- We will be meeting this Thursday at 1pm following lunch hour in conference room A to discuss, develop and deploy a disaster recovery plan for any breaches. Currently we do not have either cloud backups or local backups to

internal data, which is already currently deeply high-risk due to the lack of password security policy, and allows for a mildly competent threat actor to breach and remove our customer SPII very quickly. Please prepare your strategies on how to bolster our crisis response as a one-page brief, and be prepared to present.

- To entirely remove the barrier that 24/7 monitoring of our legacy systems presents, we will be migrating all legacy functionality in the coming weeks and creating data backups to our AWS servers, after we complete negotiating our enterprise services contract with them. This will allow us to maintain data integrity through a third party with incredibly secure APIs, covering a pinch point in the data transfer which was a security gap prior to cloud migration (because we were transferring all data by hand internally from file folder to file folder). Migrating to cloud services will also allow greater availability of data without having to manually walk a file from one office to another, saving time and optimizing efficiency through a shift of our current office paradigm to more online sharing and collaboration.