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 **(All BT employees have access to internally stored data)**
☐	☑	Disaster recovery plans **(no disaster recovery plan in place)**
☐	☑	Password policies **(it exists, but its requirements are nominal)**
☐	☑	Separation of duties **(have not been implemented)**
☑	☐	Firewall **(Has a firewall in IT department)**
☐	☑	Intrusion detection system (IDS) **(not installed)**
☐	☑	Backups **(no backup for critical data)**
☑	☐	Antivirus software **(installed and monitored regularly)**
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems **(no regular schedule for those tasks)**
☐	☑	Encryption **(not used for customer’s credit card info)**
☐	☑	Password management system **(there is no centralized 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. **(all employees can access customers' PI/PII data)**
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. **(Since all employees can access, it is not secure environment)**
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data. **(Encryption is not currently used to ensure con dentiality of customers' credit card information)**
☐	☑	Adopt secure password management policies. **(its requirements are nominal)**

General Data Protection Regulation (GDPR)

Yes	No	Best practice

☐	☑	E.U. customers' data is kept private/secured. **(all employees can access it)**
☑	☐	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.**(IT department does not know which assets would be at risk.)**
☑	☐	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. **(all BT employees can access all data/ least privilege is not implemented)**
☐	☑	Sensitive data (PII/SPII) is confidential/private. **(all BT employees can access all data/ least privilege is not implemented)**
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☐	☑	Data is available to individuals authorized to access it. **(all BT employees can access all data/ least privilege is not implemented)**

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.

To improve Botium Toys' security posture, multiple controls need to be implemented. These include: enforcing least privilege, developing comprehensive disaster recovery plans, establishing strong password policies, ensuring separation of duties, deploying intrusion detection systems (IDS), maintaining backups for critical data, applying regulations for legacy systems, encrypting sensitive information, and adopting a password management system.

Additionally, to meet compliance requirements, Botium Toys must implement least privilege, access control, duty separation, and encryption. The company should also classify its assets to identify those that are at risk. Overall, Botium Toys needs to strengthen its ability to protect sensitive information and ensure regulatory compliance.