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	Explanation
☐	☑	Least Privilege	(All employees have access to customer data; limit privilege to reduce risk of breach)
☐	☑	Disaster recovery plans	(No disaster recovery plan in place; must be implemented to ensure business continuity)
☑	☐	Password policies	(Requirements are minimal and not inline with complexity requirements to reduce likelihood of compromise)
☐	☑	Separation of duties	(Needs to be implemented to reduce risk and overall impact of malicious insider or compromised accounts)
☑	☐	Firewall	(Firewall is in place that blocks traffic based on an appropriately defined set of security rules)
☐	☑	Intrusion detection system (IDS)	(Must install a IDS to detect and prevent intrusions by possible threat actors)
☐	☑	Backups	(Company does not have backups of critical data to restore/recover from an event)
☑	☐	Antivirus software	(Antivirus is installed and monitored regularly by the IT department)
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	(Asset report notes states that legacy systems are

monitored and maintained, but there is no regular schedule in place for these tasks and intervention methods are unclear)

- ☐ ☑ Encryption (Encryption is not currently being used. Implementing encryption will ensure confidentiality of customer data)
- ☐ ☑ Password management system (There is no password management system currently in place. Implementing this will improve productivity within the IT department to recover or reset a password)
- ☑ ☐ Locks (offices, storefront, warehouse) (Sufficient locks are in place)
- ☑ ☐ Closed-circuit television (CCTV) surveillance (CCTV is up to date and functioning)
- ☑ ☐ Fire detection/prevention (fire alarm, sprinkler system, etc.) (Fire detection/prevention systems are fully functional)

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 have access to company's internal data)
☐	☑	Credit card information is stored, accepted, processed, and

transmitted internally, in a secure environment. (Credit card information is not Encrypted and all employees have access to customer data)

☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data. (Company has not implemented data encryption to help secure all customer's financial data)
☐	☑	Adopt secure password management policies. (Password policies are nominal and no password management system is in place)

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	☑	E.U. customers' data is kept private/secured. (Company has not implemented data encryption to help secure all customer's financial data)
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. (The IT department has established a plan to notify E.U customers within 72 hours if their data is compromised/there is a breach)
☐	☑	Ensure data is properly classified and inventoried. (Data has been inventoried but not classified)
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data. (Privacy policies, procedures, and processes to properly document and maintain data have been enforced among IT department)

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice

- ☐ ☑ User access policies are established. (All employees have access to internally stored data. Controls of least privilege and Separation of Duties have not been implemented.
- ☐ ☑ Sensitive data (PII/SPII) is confidential/private. (Company not using encryption to protect sensitive data (PII/SPII) and maintain confidentiality)
- ☑ ☐ Data integrity ensures the data is consistent, complete, accurate, and has been validated. (Data integrity is in place)
- ☐ ☑ Data is available to individuals authorized to access it. (All employees have access, but authorization needs to be limited to only those employees who require full access)

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.

Multiple controls must be implemented to strengthen BotiumToys security posture. The company must also take necessary steps to ensure the confidentiality of sensitive information by implementing least privilege, disaster recovery plans, separation of duties, an IDS, an ongoing legacy system, encryption, and a password management system.