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): Based on the scope, goals and risk assessment report, there are few recommendations that can be taken care of to increase the organizations security. The recommendations are as follows:

NO	ISSUES	RECOMMENDATION
1.	All Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.	Organizations should not let everyone to get access as it will expose to internal threat that can cost to customer's data. Organization should have apply OWASP Principle of least priviledge so that the workers just only have information regarding their jobscope only in order to minimize the risk of data breach.

2.	Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmited, and stored locally in the company's internal database.	Organization does not follow CIA triad model as there are abandoning the using of encryption of the data. The data involves is customer's financial data, credit card number etc. This is considered as SPII. If the data in the database got to be access by threat actors, it will cause the organization into big trouble as it will affect organization reputation and financial. However, organization had done a great work by stored the data inside the internal network.
3.	The IT department has not installed an intrusion detection system (IDS).	IDS is one of the important aspect technical control. Organization need to install IDS as it one of the tools that can help to detect anomaly that happen to ensure that the organization is ready when breaching is happen and to mitigate the risk faster.
4.	There are no disaster recovery plans currently in place, and the company does not have backups of critical data.	Organization should setup disaster recovery plan if something happen and they also need to have backup to their critical data. It is important for the business continuity if incident happen.
5.	Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special (characters).	Organization should revise and applying strict policies regarding password. This is to ensure, that the data is only access by the authorize personnel only. The also can apply Multi Faction Authentication by using biometrics in order to prove the personnel who tyring to access the data is the right personnel not the threat actors.
6.	While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.	Organization also need to apply OWASP Principle of Separation Duties so that the the organization can work effectively thus minimize the security risk.