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** (**Note: Not very strong)**
	✓	Separation of duties
✓		Firewall
	✓	Intrusion detection system (IDS)
	✓	Backups
✓		Antivirus software
	✓	Manual monitoring, maintenance, and intervention for legacy systems** (**Note: No regular schedule in place for tasks)**
	✓	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.

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.

Principle of Least Privilege must be adopted, i.e. only giving access to SPII and PII to employees who both have clearance and need access to said information to do their jobs

Proper Password Management & Policy must be adopted. Currently passwords can be anything including 123456, which is insecure. Also, all passwords are stored without being encrypted. -> Adopt a Password Manager. Enforce a password policy minimum 8 characters and include uppercase, lowercase, digits and special characters in the password. If dealing with more sensitive information, enable 2FA using cryptographic keys rather than simply relying on a password.

After adopting the above two things, **Proper Separation of duties** will be easier because employees will only have access to info they need to do their jobs.

Proper Disaster Recovery Plan must be adopted which includes robust backups to an out-of-network data storage, and a regular backup schedule. This includes the CCTV footage, which backups need to be in compliance with regulations.

With proper password management and least privilege, we introduced encryption there. We can continue with the encryption by also **Encrypting Credit Card Transactions.** Failing to do this, means we are not in compliance with PCI DSS.

IDS needs to be implemented as well. Right now even though they have a plan to notify EU customers within 72 hours of a breach, they have no way of knowing there is a breach until say a Ransomware attack happens.

Proper Asset Classification and handling . Many assets are not classified nor is their access controlled. Some assets are legacy systems and those need to be properly decommissioned or if they are still able to be used and within Compliance, a proper maintenance, update and backup schedule needs to be implemented for those devices to ensure that SPII is not compromised due to a vulnerability.