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
	X	Least Privilege-	(Currently there is no principle of least privilege being *used at Botium Toys. Currently all employees have access to Sensitive customer data like their PII, and SPII.)*
	X	Disaster recovery plans-	(*Currently there are no disaster recovery plans in place at Botium Toys. The company does not have backups of sensitive, and critical data.*
	X	Password policies-	(*There is a password policy currently but it is rather weak, and they have no centralized password management system to monitor and implement better password policies.)*
	X	Separation of duties-	(*Currently there is no separation of duties at Botium Toys. Much like leat privilege they need to implement separation of duties.)*
X		Firewall-	*(Botium Toys IT department has implemented a firewall that blocks traffic based on the security rules set in place by the IT department.)*
	X	Intrusion detection system (IDS)-	*(Currently there is no IDS system in place. They should also implement this so they can detect any anomalies within the network traffic.*
	X	Backups-	*(Currently there are no backups stored of critical data in the database.)*
X		Antivirus software-	*(Yes the IT department has antivirus software installed, and they also monitor it regularly)*

	X	Manual monitoring, maintenance, and intervention for legacy systems-*(The asset list does show that they do monitor and maintain the legacy system, There is no regular schedule in place for these tasks. Could make this liable for a breach.)*
	X	Encryption-*(Currently there is no encryption in place. We will need to implement encryption so that customer data is safe, and secure incase of a breach. Information right now is just stored in the internal database.)*
	X	Password management system-*(There is no password management system in place that enforces password policies minimum requirements. We need to implement this so it doesn't affect productivity.)*
X		Locks (offices, storefront, warehouse)-*(Yes Botium Toys physical locations has up to date locks on there main offices, and store front locations.)*
X		Closed-circuit television (CCTV) surveillance-*(Yes they have up to date closed circuit television (CCTV) at there physical locations.)*
X		Fire detection/prevention (fire alarm, sprinkler system, etc.)-*(Yes they have functioning fire detection and prevention systems.)*

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
	X	Only authorized users have access to customers' credit card information.*(No currently all employees at Botium Toys have access to credit card information)*
	X	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.*(No currently credit card information is stored, accepted, processed, and transmitted in the companies internal database.)*
	X	Implement data encryption procedures to better secure credit card transaction touchpoints and data.*(Botium Toys currently has no data encryption procedures in place to protect credit card transaction touchpoints, or data.)*
	X	Adopt secure password management policies.*(Currently Botium Toys has a very weak password policy and no centralized management system to monitor and make sure the passwords meet the minimum requirement.)*

General Data Protection Regulation (GDPR)

Yes	No	Best practice
	X	E.U. customers' data is kept private/secured.*(Currently there is no encryption to ensure that E.U. customers data is private and secure)*

X		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. *(Yes Botium Toys IT department has implemented a plan to notify the customers is there has been a breach.)*
	X	Ensure data is properly classified and inventoried. *(No Botium Toys does not have their assets classified, but they do have them listed)*
X		Enforce privacy policies, procedures, and processes to properly document and maintain data. *(Yes the IT department has developed privacy policies, and procedures, and are enforced by the IT department.)*

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

Yes	No	Best practice
	X	User access policies are established. *(No there is no separation of duties at Botium Toys. So there is no user access policy established.)*
	X	Sensitive data (PII/SPII) is confidential/private. *(No every employee has access the PII/SPII because there is no encryption and all employees have access to the company internal database.)*
X		Data integrity ensures the data is consistent, complete, accurate, and has been validated. *(Yes data integrity is in place)*
	X	Data is available to individuals authorized to access it. *(No, every employee has access to critical data. There is no separation of duties or least privilege)*

Recommendations: Currently I have a lot of updates I think Botium Toys should implement to better improve their security posture. I think one of the first controls they

need to implement is separation of duties, and least privilege. This will help by only having the right employees or individuals being able to access certain data. Then they should probably add some disaster recovery plans, just in case Botium Toys loses sensitive data we can get it back, then a better password management system that will be monitored regularly, with a better password policy enforced. Then we should implement an intrusion detection system (IDS) to detect or to prevent certain anomalies in the network traffic with a certain signature. They should also input encryption to ensure their customers confidentiality or there PII, or SPII