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, type an X in the "yes" or "no" column to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control
	X	Least Privilege
	X	Disaster recovery plans
X		Password policies
	X	Separation of duties
X		Firewall
	X	Intrusion detection system (IDS)
	X	Backups
X		Antivirus software
	X	Manual monitoring, maintenance, and intervention for legacy systems
	X	Encryption
	X	Password management system
X		Locks (offices, storefront, warehouse)
X		Closed-circuit television (CCTV) surveillance
X		Fire detection/prevention (fire alarm, sprinkler system, etc.)

Commented [Ej1]: *Employee password requirements are minimal, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network*

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, type an X in the "yes" or "no" column 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.
	X	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
	X	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
	X	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
X		E.U. customers' data is kept private/secured.
X		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
X		Ensure data is properly classified and inventoried.
X		Enforce privacy policies, procedures, and processes to properly document and maintain data.

Commented [Ej2]: *The company does not currently use encryption to better ensure the confidentiality of customers' financial information.*

Commented [Ej3]: *Current assets have been inventoried/listed, but not classified*

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

Yes	No	Best practice
	X	User access policies are established.
	X	Sensitive data (PII/SPII) is confidential/private.
X		Data integrity ensures the data is consistent, complete, accurate, and has been validated.
	X	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): 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.

Recommendation:

Per our findings below is a break down of each segment which gives suggestions that need to be implemented to mitigate future risk.

Risk Score: Medium

1 2 3 4 5 6 7 **8** 9 10

Administrative/Managerial Controls

Implementation of least privilege and separation of duties is a must to ensure the reduction of risk and overall impact of malicious insider or compromised accounts.

Suggestion: Create specialized access for those who need to use PII/SPII of customer cardholder data for transaction, while restricting the access of that data for all other employees.

Technical Controls

Implementation of (IDS) Intrusion detection system to detect and prevent anomalous traffic that matches a signature or rule.

Implement encryption to provide confidentiality to sensitive information.

Implementation of backups to restore/recover from an event.

Implement password management to reduce password fatigue

Continuous manual monitoring maintenance and intervention to identify and manage threats, risks, or vulnerabilities to out of data systems.

Suggestion: Implement a plan to create a system for these technical controls in order to be able to prevent, detect, and correct moving forward. (Create a regular schedule for tasks and intervention methods for optimal organization of legacy systems).

As for the following we have indicated that these implementations are being used properly:

Firewall

Antivirus Software

Commented [Ej4]: *Multiple controls need to be implemented to improve Botium Toys' security posture and better ensure the confidentiality of sensitive information, including: Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS, ongoing legacy system management, encryption, and a password management system.*

To address gaps in compliance, Botium Toys needs to implement controls such as Least Privilege, separation of duties, and encryption. The company also needs to properly classify assets, to identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.

Plan implemented to notify E.U customers in 72 hours

Password Policy

Stores physical locations have sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.