Controls and compliance checklist

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.)

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 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:

- As all the employees have access to internally stored data which also includes PII/SPII, it makes the company more vulnerable from the inside from possible future disgruntled employees, so there is a need for a Least Privilege system.
- We also need Disaster recovery plans in case an attack happens, we should be ready to stop the disaster but at the same time be able to reconstruct from the damages done to keep the continuity in business.
- Password policies are good but stricter/firm policies would be better as they would decrease our chances of getting attacked significantly. Examples could be: increasing the required number of characters in the password, having Two-factor authentication, etc.
- An IDS system is needed for quick action against any intrusion to keep the damages to the minimum.
- Being compliant with U.S. and international regulations and standards is crucial for the company to thrive and not face any financial penalties resulting in reputational damage.
- The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is not a regular schedule in place for this task and procedures/policies related to intervention are unclear, which could place these systems at risk of a breach.