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)

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:

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.

The following actions are the top priority for the IT manager to communicate to stakeholders to reduce the risk score of 8 and improve the security posture:

1. **Implement Foundational Access Controls:** Immediately deploy Least Privilege and Separation of Duties across all systems, restricting access to sensitive data (e.g. PII/SPII) only to authorized personnel.
2. **Enforce Strong Password Management:** Implement a centralized Password Management System that rigorously enforces a modern Password Policy (e.g., minimum 12 characters, complex mix of character types).
3. **Ensure Business Continuity:** Develop and implement formal Disaster Recovery Plans and establish regular, verifiable Backups of all critical data.

4. **Data Protection & Confidentiality:** Immediately deploy Encryption controls to protect customers' credit card information while it is accepted, processed, transmitted, and stored.
5. **Perimeter Monitoring:** Install an **Intrusion Detection System (IDS)** to actively monitor the internal network and alert the IT team to suspicious traffic and potential breaches.
6. **Asset Classification:** Dedicate resources to fully classify and inventory all existing assets (including systems and data) to properly identify remaining risks and ensure full compliance.