Botium Toys

Audit: 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.

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, 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.

1. Ensure compliance with US and International regulations and standards
2. Identify all assets in order to manage them
3. Classify all assets in order to determine to impact of the loss to existing assets, including systems on business continuity.
4. Implement controls to access to cardholder data and customer's PII and SPII
5. Use encryption to ensure confidentiality of customers credit card information that is accepted, processed, transmitted and stored locally in the company's internal database.
6. Install Intrusion Detection Systems (IDS)
7. Implement a disaster recovery plan and have backups for the company's critical data.