Controls and compliance checklist

Select "yes" or "no" to answer the question: *Does Botium Toys currently have this control in place?*

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.)

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
☐	☑	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

- [ ]   [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.

Recommendations: The IT manager at Botium Toys should focus on enhancing security and compliance by implementing critical measures. First and foremost, the organization should enforce the principle of least privilege access control, limiting data access to employees who require it for their roles. Disaster recovery plans and robust password policies should be put in place to ensure business continuity and strengthen data protection. Additionally, separation of duties, network security enhancements, intrusion detection systems, regular data backups, encryption for sensitive information, and the introduction of a password management system are essential steps to bolster cybersecurity.

To meet compliance standards such as PCI DSS, GDPR, and SOC, Botium Toys must review and align its practices accordingly. This includes ensuring the confidentiality of customer data through encryption, promptly notifying EU customers in case of data breaches, and properly classifying and documenting data. Lastly, regular employee training and awareness programs should be conducted to ensure a strong cybersecurity culture within the organization. These measures collectively will help mitigate risks, protect sensitive information, and maintain compliance with industry standards.