Controls and compliance checklist -Boitum Toys

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.

- [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:

To enhance the security posture and ensure compliance with industry regulations, Botium Toys must prioritize the implementation of critical controls and best practices. One of the most pressing issues is the lack of access control mechanisms, such as enforcing the principle of least privilege and separation of duties. These measures will minimize the risk of unauthorized access to sensitive data, such as customer credit card information and personally identifiable information (PII). Additionally, updating password policies and deploying a centralized password management system will improve both security and operational efficiency by reducing the frequency of password recovery incidents.

Data protection is another key area requiring immediate attention. Encryption should be implemented to secure sensitive data in transit and at rest, particularly credit card information stored and processed internally. Furthermore, a robust disaster recovery plan and regular backups are essential to safeguard the business against potential data loss or system failures. Introducing an intrusion detection system (IDS) will also help identify and mitigate security threats proactively, ensuring the integrity and availability of your network.

Lastly, compliance with regulatory frameworks such as PCI DSS, GDPR, and SOC must be strengthened to avoid potential fines and maintain customer trust. This includes conducting a detailed compliance audit, ensuring data classification and inventory processes are updated, and adopting secure encryption and privacy policies. Investing in these measures will not only protect Botium Toys' assets and reputation but also provide a solid foundation for sustained growth and resilience in an increasingly complex cybersecurity landscape.