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: The following recommendations include several administrative and technical controls that should be implemented in order to protect Botium Toys from potential cybersecurity threats and to become compliant with NIST CSF benchmarks.

- Implement a system with group policy rules for all users in the organization to ensure that individual users only have access to the data that is required to perform their work duties. This system should be configured to require passwords for all users to be secure (at least eight characters, a combination of letters and at least one number, and special characters). Additionally, a group policy setting should be put in place to require passwords to be changed on a quarterly basis.
- Implement data encryption on all PII (i.e. employee/customer private info and credit card information) in all phases (in transit, in use, and at rest). This is not only an overall secure practice, but will make the organization compliant to conduct commerce in the EU.
- Develop, implement, and maintain an effective disaster recovery plan including backup servers for business operation.
- Implement and maintain IDS and IPS in order to prevent potential cyber attack.
- Ensure segmentation is implemented across the organization's network to prevent lateral movement in the event a threat actor gains access to the network.