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. |

Summary and Recommendations.

Currently Botium Toys' security posture is weak and susceptible to threat actors. Risk score being an 8/10 due to lack of controls and adherence to compliance best practices.

Recommended to **implement technical and administrative controls** to further secure digital assets. This would include but not be limited to, implementing **encryption** to ensure confidentiality of customer's PII/SPII. **Limiting users' access** to bare minimum information needed to complete work-related tasks. Introduce an **Intrusion Detection System** to monitor any attempts at unauthorized access. On the administrative side, **enforcing password policies** and **implementing a password management system**.

Suggestion to devise a recovery plan in the case of an event to avoid disrupting business continuity. This can involve **creating backups of critical data** and having a **plan or playbook** in place to respond to incidents.

Failure to adhere to recommendations can result in severe financial consequences as well as damage to an organization's reputation.