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

1. Implement Least Privilege Access Control: To minimize the risk of unauthorized access, implement a least privilege policy across all systems. This ensures employees only have access to the data necessary for their roles.

2. Develop and Test a Disaster Recovery Plan: Without a disaster recovery plan, Botium Toys is at risk of significant operational downtime. Implementing this will ensure business continuity in case of a critical incident.

3. Strengthen Encryption and Password Policies: Implement encryption for sensitive data, especially credit card information, and enforce stronger password policies and management systems to protect against unauthorized access and breaches.

4. Deploy an Intrusion Detection System (IDS): An IDS is crucial for detecting and responding to potential threats. This system should be a priority for safeguarding the network against unauthorized intrusions.

5. Regular Backups: Establish a regular backup schedule for critical data to ensure that Botium Toys can quickly recover from data loss incidents.