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.

Yes	No	Best practice
☐	☑	User access policies are established.
☑	☐	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 Data Encryption:** Start encrypting sensitive data, especially credit card information and PII/SPII, both in transit and at rest. This will help protect customer data from unauthorized access.
2. **Access Controls:** Implement least privilege and separation of duties access controls. Only grant employees access to the data and systems on a “need to know basis”
3. **Intrusion Detection System(IDS):** Install and configure an intrusion detection system to monitor network traffic and detect potential threats and breaches in real time.
4. **Disaster Recovery and Back Plan:** Develop and regularly test a disaster recovery plan to ensure business continuity in case of data loss or system failures. Implement regular data backups to prevent data loss.
5. **Password Policy Enforcement:** Strengthen the password policy by requiring longer passwords with a combination of letters, numbers, and special characters.
6. **Regular Legacy System Maintenance:** Establish a regular schedule for monitoring and maintaining legacy systems to ensure they are up-to-date and secure.

7. **Access Monitoring and Logging:** Implement comprehensive access monitoring and logging to track user activity and detect any unusual or unauthorized access.
8. **User Access policies:** Develop and enforce user access policies to define who can access what data and systems.
9. **Data Classification and Inventory:** Implement a system of properly classifying and inventorying data assets. This will help in prioritizing security measures based on data sensitivity.
10. **Incident Response Plan:** Develop a comprehensive incident response plan that outlines steps to take in the event of a security break, including notifying affected parties and stakeholders.
11. **Compliance:** Ensure compliance with data protection regulations, especially for E.U. customers. Adopt GDPR, and/or ISO 27000 frameworks.
12. **Physical Security:** Maintain physical security measures like locks, CCTV surveillance, and fire detection/prevention systems at the company's physical location to protect against physical threats.
13. **Regular Security Audits:** Conduct regular security audits and assessments to identify vulnerabilities and areas of improvement.

These recommendations should help Botium Toys improve its security posture and reduce risks to its assets and customer data.