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, storefronts, warehouses)
☑	☐	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 Organization 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.

Critical Security Gaps Analysis

The assessment reveals several critical security vulnerabilities that significantly contribute to Botium Toys' high risk score of 8 out of 10.
The most concerning gaps include:

Access Control Deficiencies: The absence of least privilege principles means all employees can access sensitive customer data, creating unnecessary exposure to cardholder information and personally identifiable information. This violates fundamental security principles and compliance requirements.

Data Protection Failures: The lack of encryption for credit card data represents a severe PCI DSS violation that could result in substantial fines and reputational damage. Without proper encryption, sensitive financial data remains vulnerable during storage, processing, and transmission.

Business Continuity Risks: The absence of disaster recovery plans and data backups creates significant business continuity risks. Legacy systems require manual monitoring without established schedules, increasing the likelihood of system failures and data loss .

Password Security Weaknesses: The current password policy fails to meet modern security standards, and the lack of a centralized password management system creates operational inefficiencies and security vulnerabilities .

Recommendations for Immediate Implementation

High Priority (Implement within 30 days)

1. Implement Least Privilege Access Controls: Establish role-based access controls to ensure employees only access data necessary for their job functions
2. Deploy Encryption for Cardholder Data: Implement end-to-end encryption for all credit card information to meet PCI DSS requirements.
3. Establish Data Backup Systems: Implement automated backup solutions for critical data with regular testing procedures
4. Install Intrusion Detection System: Deploy IDS to monitor network traffic and detect potential security threats

Medium Priority (Implement within 60 days)

5. Develop Disaster Recovery Plan: Create comprehensive disaster recovery procedures with defined recovery time objectives

6. Implement Password Management System: Deploy a centralized password management system with strong policy enforcement
7. Establish Separation of Duties: Implement controls to prevent single individuals from having complete control over critical processes
8. Strengthen Password Policies: Update password requirements to meet current industry standards with complexity requirements

Ongoing Priorities

9. Formalize Legacy System Management: Establish regular maintenance schedules and clear intervention procedures for end-of-life systems
10. Implement Data Classification: Develop and implement a comprehensive data classification system to support proper access controls
11. Conduct Regular Security Assessments: Establish quarterly security assessments to identify new vulnerabilities and ensure ongoing compliance

The implementation of these recommendations will significantly improve Botium Toys' security posture, reduce regulatory compliance risks, and protect critical business assets from cyber threats