Controls and compliance checklist

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control
☐	☑	Least Privilege
☐	☑	Role-Based Access Control (RBAC) implemented
☐	☑	Disaster recovery plans
☐	☑	Password Policy (length, complexity, expiration)
☑	☐	MFA (Multi-Factor-Auth)
☐	☑	Intrusion Detection/Prevention System (IDS/IPS)
☐	☑	Security Information and Event Management (SIEM)
☑	☐	Separation of duties
☑	☐	Firewall
☐	☑	Business Continuity Plan (BCP)
☑	☐	Backups
☐	☑	Security awareness training for employees
☑	☐	Antivirus software
☐	☑	Remote access secured (VPN, MFA)
☑	☐	Manual monitoring, maintenance, and intervention for legacy systems

☐	☑	Encryption
☐	☑	Password management system
☐	☑	Network segmentation in place
☑	☐	Locks (offices, storefront, warehouse)
☑	☐	Closed-circuit television (CCTV) surveillance
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

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.

HIPAA (The Health Insurance Portability and Accountability Act) DOES NOT APPLY

Yes	No	Best practice
☐	☐	PHI (Protected Health Information) access controlled
☐	☐	Audit logs for patient data access
☐	☐	Encryption for stored/transmitted PHI.
☐	☐	Employee HIPAA training records maintained
☐	☐	Breach notification procedures established

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 (optional):

After reviewing the current state of controls and compliance practices at FintexCorp, several critical areas must be addressed to strengthen the organization's cybersecurity posture and align with industry best practices, particularly those outlined in **PCI DSS** and **SOC 2** frameworks.

Key recommendations include:

- **Implementing least privilege and role-based access control (RBAC)**
- **Enforcing multi-factor authentication (MFA)** on all systems
- **Deploying a centralized password management system** and enforcing strong password policies that include complexity, expiration, and reuse prevention.
- **Formalizing and testing a comprehensive Disaster Recovery Plan (DRP)**
- **Establishing a Business Continuity Plan (BCP)**
- **Implementing a Security Information and Event Management (SIEM) solution** for real-time threat detection, log analysis, and incident response.
- **Deploying an Intrusion Detection and Prevention System (IDS/IPS)** to monitor and defend against internal and external threats.
- **Enhancing encryption practices**, ensuring that all sensitive data—including PII and credit card information—is encrypted at rest and in transit, and that tokenization methods are fully irreversible.
- **Conducting a comprehensive data classification and inventory effort** to identify and manage sensitive data in accordance with regulatory requirements.

- **Establishing DDoS protection mechanisms** to safeguard APIs and customer-facing services from availability-based attacks.
- **Removing shared credentials** and implementing individual user accounts with clearly defined permissions for developers and operations teams.

These measures are necessary to reduce FintexCorp's elevated risk exposure (currently scored at 8 out of 10) and to maintain trust among customers, partners, and regulatory bodies.