Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the
scope, goals, and risk assessment report. For more details about each control,
including the type and purpose, refer to the control categories document.

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
☐	☑	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.)

To complete the compliance checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each compliance regulation, review the controls, frameworks, and compliance reading.

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.

Yes	No	
☑	☐	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.

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

Recommendations (optional): In this section, provide recommendations, related to controls and/or compliance needs, that your IT manager could communicate to stakeholders to reduce risks to assets and improve Botium Toys' security posture.

Critical Priority (Implement Immediately):

Botium Toys faces high-risk gaps that could result in data breaches, regulatory fines, or business disruption. Implement least privilege and separation of duties access controls now. All employees currently access sensitive customer data including credit card info and PII/SPII. This violates compliance standards and creates security risk.

Encryption must be implemented for customer credit card data. The company stores, processes, and transmits this data without encryption. This puts Botium Toys at serious risk for PCI DSS violations and lawsuits.

High Priority (Implement Within 30-60 Days):

Create disaster recovery plans and backups. No backup system exists right now. Any ransomware attack, hardware failure, or disaster could wipe out the business. This concern grows with e-commerce operations and inventory management systems running.

The password system needs a complete overhaul. Implement a centralized password management system with security requirements: minimum 8 characters and complexity rules. The current policy lacks strength and employees reset passwords often, killing productivity.

Medium Priority (Implement Within 90 Days):

Deploy an IDS to detect intrusions and anomalous traffic. The firewall blocks known threats, but the IT team has no visibility into network activity without detection capabilities.

Set up a regular schedule for legacy system monitoring and maintenance. These systems need human oversight. Without clear procedures, issues will slip through.

Bottom Line:

The risk score of 8/10 stands. Compliance violations (PCI DSS, GDPR, SOC) and missing controls put Botium Toys one incident away from serious financial and reputational damage. Most of these fixes are standard implementations that roll out systematically with proper planning and resource allocation.