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.

□	☑	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 : Following the recent risk assessment conducted for Botium Toys, several areas of concern regarding the company's security posture have been identified. These gaps pose potential risks to the organization’s data, infrastructure, and operations. The following outlines a series of prioritized recommendations to address these lack of controls and compliance standards to improve Botium Toys’ overall security stance.

The recommendations are categorized based on their severity, from critical to low priority, along with suggested timelines for implementation.

Critical Recommendations (Immediate Action Required)

1. **Encryption**: It is crucial to implement end-to-end encryption for sensitive data both at rest and in transit. Encryption safeguards confidential data from unauthorized access, ensuring privacy and compliance with security standards.
2. **Disaster Recovery Plan** : Develop and implement a comprehensive Disaster Recovery (DR) plan, including clear backup strategies, restoration procedures, and specified RTO (Recovery Time Objective) and RPO (Recovery Point Objective) metrics. This plan will ensure business continuity in case of system failures or unforeseen events.
3. **Intrusion Detection System (IDS):** Deploy an Intrusion Detection System (IDS) to monitor network traffic and identify potential threats. An IDS enables early detection of suspicious activity, providing valuable insight into possible intrusions or cyberattacks.

High Priority Recommendations (Short-Term Action)

1. **Least Privilege Policy:** Establish and enforce a Least Privilege Access Control policy that limits user permissions to only the resources necessary for their job functions. This reduces the attack surface by minimizing the risk of unauthorized access or misuse of critical systems.
2. **Password Management System:** Implement a centralized, secure password management system for creating, storing, and managing strong passwords across the organization. This includes updating the existing password policy to comply with modern password standards (e.g., complexity requirements, expiration, and multi-factor authentication).
3. **Separation of Duties:** Develop and enforce policies that ensure a clear separation of duties across key roles and functions within the organization. No single employee should have excessive control over critical systems or business operations, which could lead to fraud, errors, or misuse of privileges.

Moderate Priority Recommendations (Medium-Term Action)

1. **Backup Policy :** Create and implement a formal backup policy that ensures regular backups of critical data and systems. Backups should be tested periodically to ensure they can be restored quickly and accurately during an emergency or data loss event.
2. **Manual Monitoring, Maintenance, and Intervention for Legacy Systems :** Implement manual monitoring and regular maintenance procedures for legacy systems that may not be compatible with automated security tools. This includes periodic updates, patching, and ensuring that manual intervention procedures are clearly documented.

Low Priority Recommendations (Ongoing Improvement)

1. **Password Policy Update:** Review and update the existing password policy to align with best practices for password security. This includes enforcing password complexity, setting regular password expiration intervals, and considering the implementation of multi-factor authentication (MFA) where applicable.

Security Recommendations Timeline Overview

Recommendation	Severity	Recommended Timeline
Encryption	Critical	1-2 months
Disaster Recovery Plan	Critical	1-2 months
Intrusion Detection System (IDS)	Critical	1-2 months
Least Privilege Policy	High	2-3 months
Password Management System	High	2-3 months
Separation of Duties	High	2-3 months
Backup Policy	Moderate	3-4 months

Manual Monitoring, Maintenance, and Intervention for Legacy Systems	Moderate	3-4 months
Password Policy Update	Low	4-6 months

The implementation of these recommendations will significantly enhance the security posture of Botium Toys, reducing risks associated with data breaches, unauthorized access, and operational disruptions. It is essential that the critical recommendations are addressed immediately, with high-priority actions implemented in the short term, followed by medium and low-priority tasks over the coming months.

A proactive approach to these recommendations will ensure a robust security framework, safeguarding Botium Toys' assets, sensitive data, and reputation.

For further clarification or assistance with any of the recommendations, please feel free to contact **Abdul Ghayour Adib Amiri**, Cybersecurity Analyst, at **ghcyber@gmail.com**.