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.

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.

Based on the security audit and risk assessment at Botium Toys, several vulnerabilities were identified across access controls, data protection, and compliance readiness. The following mitigation recommendations are intended to reduce risk, improve compliance, and strengthen the organization's overall security posture.

Mitigation Recommendations for Botium Toys Security Risks

- Enforce least privilege access controls to ensure employees can only access the data necessary for their job functions, reducing the risk of unauthorized exposure to sensitive information.

- Implement separation of duties by assigning responsibilities to different individuals, minimizing the risk of insider threats or accidental misuse of system privileges.

- Develop and maintain a disaster recovery plan (DRP) that includes data backup procedures, recovery time objectives (RTO), and testing periodically to ensure resilience in the event of a system failure or breach.

- Establish strong password policies requiring minimum complexity (e.g., 12+ characters, mixed case, symbols, numbers) and regular rotation of them to defend against brute-force and credential stuffing attacks.

- Deploy a centralized password management system to enforce policy compliance, streamline password resets, and reduce helpdesk workload.

- Implement encryption protocols to protect sensitive data, such as payment card information and personally identifiable information (PII), both at rest and in transit, and in compliance with PCI DSS and GDPR.

- Install and configure an intrusion detection system (IDS**)** to monitor network traffic and detect unauthorized or suspicious activity in real time.

- Automate and schedule regular data backups of critical systems, ensuring off-site storage and periodic testing of restore procedures to minimize data loss.

- Create and follow a maintenance schedule for legacy systems, including patch management and defined intervention processes, to reduce vulnerabilities associated with outdated technologies.

- Restrict access to sensitive data, including customer PII and SPII, to authorized personnel only, and audit access regularly to maintain accountability.

- Conduct a full data inventory and classification to better understand what data is stored, where it resides, and the level of protection it requires.

- Update physical security controls regularly, ensuring CCTV systems, door locks, and fire prevention systems remain functional and effective.

- Provide regular cybersecurity awareness training to all employees, covering topics such as phishing prevention, secure data handling, and regulatory responsibilities under GDPR and PCI DSS.