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.

Recommendation to Botium Toys Stakeholders Based on Security Audit Findings

1. **Access Controls and Data Privacy**

- Implement Role-Based Access Controls (RBAC): Limit access to sensitive data such as cardholder information and Personally Identifiable Information (PII/SPII) to only those employees who require it for their roles.

- Encryption: Immediately begin encrypting all stored and transmitted credit card information using industry-standard encryption protocols to ensure confidentiality and compliance with Payment Card Industry Data Security Standard (PCI DSS) requirements.

2. **Least Privilege and Separation of Duties**

- **Least Privilege Principle**: Enforce least privilege access by ensuring that employees have the minimum level of access necessary to perform their job functions.

- **Separation of Duties**: Establish clear separation of duties to prevent conflicts of interest and reduce the risk of fraud and errors.

3. **Security Infrastructure Enhancements**

- **Intrusion Detection System (IDS)**: Install an IDS to monitor network traffic for suspicious activities and potential threats, enhancing overall security posture.

- **Password Policy and Management**: Update the password policy to align with modern security standards (minimum of eight characters, a mix of letters, numbers, and special characters). Implement a centralized password management system to enforce these policies and streamline password recovery processes.

4. **Disaster Recovery and Data Backups**

- **Disaster Recovery Plan (DRP)**: Develop and implement a comprehensive disaster recovery plan to ensure business continuity in the event of a critical incident. This should include regular backups of critical data and a clear process for data restoration.

5. **Regulatory Compliance and Notification Procedures**

- **GDPR Compliance**: Ensure compliance with General Data Protection Regulation (GDPR) by maintaining the ability to notify E.U. customers within 72 hours of a security

breach. Regularly review and update privacy policies and procedures to align with current regulations.

6. **Physical and IT Security Maintenance**

- **Regular Maintenance Schedule**: Establish a regular maintenance schedule for both legacy systems and IT infrastructure to ensure they are up-to-date and secure. Clearly define intervention methods for addressing issues.

- **Physical Security**: Continue maintaining the physical security measures (locks, CCTV, fire detection, and prevention systems) at the store's physical location to protect assets and personnel.

By addressing these recommendations, Botium Toys will enhance its security posture, protect sensitive customer information, and ensure compliance with relevant regulations. This proactive approach will mitigate risks, safeguard the company's reputation, and foster trust among customers and stakeholders.