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.

Post audit Notes and Recommendations

- Implement Least Privilege Access Controls

Restrict user access to only the data and systems necessary for their roles. This will reduce the potential for internal data breaches and limit the scope of exposure in the event of a compromise.

- Develop and Maintain a Disaster Recovery Plan

Create and routinely test a comprehensive disaster recovery and business continuity plan. This should include regular data backups and clearly defined recovery procedures to ensure minimal disruption during unexpected events.

- Enhance Password Security and Management

Update the current password policy to align with industry standards, including requirements for complexity, length, and expiration. Deploy a centralized password management system to enforce these policies and reduce support load on IT staff.

- Encrypt Sensitive Customer Data

Implement robust encryption protocols for all stored and transmitted credit card information and personally identifiable information (PII/SPII). This step is critical for achieving PCI DSS compliance and protecting customer trust.

- Deploy an Intrusion Detection System (IDS)

Install and monitor an IDS to detect and respond to suspicious activities within the network in real time. This is a key component in preventing, identifying, and mitigating security threats.

- Enforce Separation of Duties

Segregate responsibilities across different roles to prevent fraud and minimize security risks. For example, the individuals managing financial transactions should not also be responsible for reviewing or approving them.

- Ensure Regular Legacy System Maintenance

Establish a documented schedule and clear intervention procedures for legacy system monitoring. This will improve reliability and security of outdated but still operational systems.

- Review and Improve Compliance with PCI DSS and GDPR

Limit access to customer credit card data, secure the environment in which it is stored or processed, and ensure all handling of E.U. customer data complies with GDPR data classification and breach notification requirements.

- Conduct Regular Security Awareness Training

Educate employees about current threats, phishing attacks, and safe data handling practices to build a strong human firewall within the organization.

- Perform Regular Security Audits

Schedule recurring internal and third-party security audits to continually assess and improve the effectiveness of implemented controls.