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 (Way too weak)
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	Antivirus software
☑	☐	Manual monitoring, maintenance, and intervention for legacy systems (Not regular scheduled)
☐	☑	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. (Every employee has access)
☑	☐	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. (Make policy stronger)

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.

To enhance Botium Toys' security posture and mitigate the identified risks, the following recommendations are provided for the IT manager to communicate to stakeholders. These recommendations focus on implementing critical controls and compliance best practices.

1. **Asset Management and Classification**:
    - **Inventory and Classification**: Establish a comprehensive asset management system to track and classify all assets, including end-user devices, internal network components, and software systems. This will facilitate better asset tracking, risk assessment, and resource allocation.
    - **Regular Audits**: Conduct periodic audits to ensure the asset inventory is up-to-date and accurate.
2. **Access Controls**:
    - **Least Privilege Principle**: Implement access controls based on the principle of least privilege to limit access to sensitive data and systems to only those employees who need it for their job functions.
    - **Separation of Duties**: Enforce separation of duties to reduce the risk of fraud and errors, ensuring that no single individual has control over all aspects of any critical process.
3. **Encryption**:
    - **Data Encryption**: Use strong encryption methods to protect sensitive data, especially customers' credit card information and personally identifiable information (PII/SPII), both in transit and at rest.
4. **Password Policies and Management**:
    - **Strengthen Password Policies**: Update the password policy to meet current best practices, including requirements for complexity, length (minimum of 12 characters), and regular updates.
    - **Centralized Password Management**: Implement a centralized password management system to enforce these policies and streamline password recovery and reset processes.
5. **Intrusion Detection and Response**:
    - **Intrusion Detection System (IDS)**: Install and configure an intrusion detection system to monitor network traffic for suspicious activity and potential security breaches.

    - **Incident Response Plan**: Develop and regularly update an incident response plan to quickly and effectively address security incidents.
6. **Disaster Recovery and Data Backup**:
    - **Disaster Recovery Plan**: Create and implement a comprehensive disaster recovery plan to ensure business continuity in the event of a major incident. This should include regular testing and updates to the plan.
    - **Regular Backups**: Establish a routine schedule for backing up critical data, and ensure that backups are stored securely and are regularly tested for integrity and restoration capability.
7. **Compliance with Regulations**:
    - **Regulatory Compliance**: Ensure full compliance with relevant U.S. and international regulations, such as GDPR for E.U. customers, including timely breach notifications and proper data handling practices.
    - **Privacy Policies**: Strengthen privacy policies and ensure they are rigorously enforced across the organization.
8. **Physical Security**:
    - **Good measures in comparison to other areas of work**