

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 |
|-------------------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Least Privilege |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Disaster recovery plans |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Password policies |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Separation of duties |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Firewall |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Intrusion detection system (IDS) |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Backups |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Antivirus software |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Manual monitoring, maintenance, and intervention for legacy systems |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Encryption |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Password management system |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Locks (offices, storefront, warehouse) |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | 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 |
|--------------------------|-------------------------------------|--|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Only authorized users have access to customers’ credit card information. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Adopt secure password management policies. |

General Data Protection Regulation (GDPR)

| Yes | No | Best practice |
|-------------------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | E.U. customers’ data is kept private/secured. |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Ensure data is properly classified and inventoried. |

- | | | |
|-------------------------------------|--------------------------|---|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | 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 |
|-------------------------------------|-------------------------------------|--|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | User access policies are established. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Sensitive data (PII/SPII) is confidential/private. |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | 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: I recommend numerous remediations to update security standards within Botium Toys relating to Administrative and Technical controls such as:

- Ensuring least privilege is in place to minimize the impact of threats and threat actors
- Creating a disaster recovery plan to ensure business continuity and reduce overall downtime due to an attack or compromised system
- Establish separation of duties to reduce the effects of a compromised account
- Implement an intrusion detection system to monitor for real-time threat actors and allow for a faster response time to minimize possible damage

- Create a schedule for regular maintenance and monitoring of legacy systems and establish proper intervention methods for those systems
- Use encryption to secure customer's personally identifiable information
- Implement a password management system and standard password policies to improve productivity and ensure both user and customer accounts are secure
- Classify all data and assets to better identify additional controls that may be needed to improve security posture

Compliance within the PCI DSS, GDPR, and SOC types 1 and 2 is not fully implemented which could result in loss of data, damage to assets, large fines, and/or loss of trust with our customers.