

Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the [scope, goals, and risk assessment report](#).

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 checked="" type="checkbox"/> | <input 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 |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | 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](#).

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. |

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.

1. Since all employees currently have access to users' PII (Personally Identifiable Information) and SPII (Sensitive Personal Identifiable Information), authorization measures should be implemented to ensure that only authorized personnel can access this data.
2. Encryption must be applied to all modes of payment and when storing users' personal data to ensure its security.
3. The IT department should establish measures to guarantee that only authorized users can access sensitive data, and unauthorized users should be effectively blocked.
4. Password policies should be updated to meet the latest complexity standards to enhance data security. Additionally, password management systems should be deployed to ensure all authorized users comply with these policies.