# Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading=h.evidx83t54sc). For more details about each control, including the type and purpose, refer to the [control categories](https://docs.google.com/document/d/1btezuy_bMKWoK8pd97ZuzdWB9y6au_zfkrpkfVf8ktI/template/preview) 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** |  |
|  | X | Least Privilege |  |
|  | X | Disaster recovery plans |  |
|  | X | Password policies |  |
|  | X | Separation of duties |  |
| X |  | Firewall |  |
|  |  |  |  |
|  | X | Intrusion detection system (IDS) |  |
|  | X | Backups |  |
| X |  | Antivirus software |  |
|  | X | Manual monitoring, maintenance, and intervention for legacy systems |  |
|  | X | Encryption |  |
|  | X | Password management system |  |
| X |  | Locks (offices, storefront, warehouse) |  |
| X |  | Closed-circuit television (CCTV) surveillance |  |
| X |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) |  |

**Compliance checklist**

Type an X in the “yes” or “no” column to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** |  |
|  | X | Only authorized users have access to customers’ credit card information. |  |
|  | X | Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment. |  |
|  | X | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |  |
|  | X | Adopt secure password management policies. |  |

General Data Protection Regulation (GDPR)

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** |  |
|  | X | E.U. customers’ data is kept private/secured. |  |
| X |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |  |
|  | X | Ensure data is properly classified and inventoried. |  |
| X |  | 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** |  |
|  | X | User access policies are established. |  |
|  | X | Sensitive data (PII/SPII) is confidential/private. |  |
| X |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |  |
|  | X | Data is available to individuals authorized to access it. |  |

**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.

*There are many glaring holes in Botium Toys’ security posture. Some of the most critical, but simple to implement the necessary changes include the principle of least privilege, password policies, and data backups. Other critical needs that are not as simple to fix include the introduction of an IDS, a password management system, and disaster recovery plans. There are many other needs at the company, but making these changes undoubtedly moves Botium Toys and their security posture in the right direction.*