# 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** |
|  |  | Least Privilege (No) |
|  |  | Disaster recovery plans (No) |
|  |  | Password policies (No) |
|  |  | Separation of duties (No) |
|  |  | Firewall (Yes) |
|  |  | Intrusion detection system (IDS) (No) |
|  |  | Backups (No) |
|  |  | Antivirus software (Yes) |
|  |  | Manual monitoring, maintenance, and intervention for legacy systems (Yes, but not consistent) |
|  |  | Encryption (No) |
|  |  | Password management system (No) |
|  |  | Locks (offices, storefront, warehouse) (Yes) |
|  |  | Closed-circuit television (CCTV) surveillance (Yes) |
|  |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) (Yes) |

To complete the compliance 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). For more details about each compliance regulation, review the [controls, frameworks, and compliance](https://www.coursera.org/learn/foundations-of-cybersecurity/supplement/xu4pr/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. (No) |
|  |  | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. (Yes) |
|  |  | Implement data encryption procedures to better secure credit card transaction touchpoints and data. (No) |
|  |  | Adopt secure password management policies. (No) |

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  |  | E.U. customers’ data is kept private/secured. (No) |
|  |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. (Yes) |
|  |  | Ensure data is properly classified and inventoried. (Yes) |
|  |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. (Yes) |

System and Organizations Controls (SOC type 1, SOC type 2)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  |  | User access policies are established. (Yes) |
|  |  | Sensitive data (PII/SPII) is confidential/private. (No) |
|  |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. (Yes) |
|  |  | Data is available to individuals authorized to access it. (Yes) |

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.

After reviewing Botium Toys’ current security practices, I recommend the following measures to strengthen its security posture:

* Enforce stricter policies regarding employee access to customer Personally Identifiable Information (PII) and Sensitive Personally Identifiable Information (SPII).
* Implement the principles of least privilege and separation of duties to reduce the risk of insider threats.
* Establish stronger password policies and enforce the use of secure password management solutions.
* Develop and maintain policies and safeguards to mitigate potential data loss, including regular backups and a comprehensive disaster recovery plan.
* Secure critical data through encryption, deploy intrusion detection systems (IDS), and consistently monitor legacy systems to help prevent the loss of high-risk assets.