Controls and compliance checklist

To complete the controls assessment checklist, refier to the infiormation provided in the [scope, goals, and risk assessment report](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview#heading%3Dh.evidx83t54sc). For more details about each control, including the type and purpose, refier 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 |
|  |  | Disaster recovery plans |
|  |  | Password policies |
|  |  | Separation ofi duties |
|  |  | Firewall |
|  |  | Intrusion detection system (IDS) |
|  |  | Backups |
|  |  | Antivirus software |
|  |  | Manual monitoring, maintenance, and intervention fior legacy systems |
|  |  | Encryption |
|  |  | Password management system |
|  |  | Locks (offices, storefiront, warehouse) |
|  |  | Closed-circuit television (CCTV) surveillance |

 Fire detection/prevention (fire alarm, sprinkler system, etc.)

To complete the compliance checklist, refier to the infiormation provided in the [scope,](https://docs.google.com/document/d/1s2u_RuhRAI40JSh-eZHvaFsV1ZMxcNSWXifHDTOsgFc/template/preview) [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, firameworks, 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 infiormation. |
|  |  | Credit card infiormation 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. |

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  |  | E.U. customers’ data is kept private/secured. |
|  |  | There is a plan in place to notifiy E.U. customers within 72 hours ifi their data is compromised/there is a breach. |
|  |  | Ensure data is properly classified and inventoried. |

 Enfiorce 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 ofi recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed ifi 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.

Recommendations:

It is extremely necessary that the security recommendations be implemented in the company, as they need to comply with the GDPR. Additionally, carefiul handling ofi customer data stored in the company is essential, as this is sensitive infiormation and is vulnerable to attacks.

From this audit, the risks associated with the assets were assessed, and the average risk level is high, because the IT team does not have adequate control over the assets

and there is also no management ofi sensitive data. The implementation ofi backups and disaster recovery plans is necessary in case an attack occurs.

The primary recommendations would be:

* Password encryption
* Employee access control to customers’ sensitive data (privilege control)
* Separation ofi duties
* Employees must sign an agreement regarding the company’s security policies

With these recommendations, the company will be prepared and in compliance with the GDPR.