# 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/1HsIw5HNDbRXzW7pmhPLsK06B7HF-KMifENO_TlccbSU/template/preview) document.

Then, type an X in the “yes” or “no” column to answer the question: *Does Botium Toys currently have this control in place?*

**Controls assessment checklist**

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Control** | **Remarks** |
|  | X | Least Privilege | Every employee can access everything |
|  | X | Disaster recovery plans | Non existent |
|  | X | Password policies | In place but not compliant to the current standard of complexity requirement |
|  | X | Separation of duties | Non existent |
| X |  | Firewall | IT has installed a firewall that blocks traffic based on a predefined set of rules |
|  | X | Intrusion detection system (IDS) | Not installed |
|  | X | Backups | There is no backups being made of critical |
| X |  | Antivirus software | Installed |
| **Yes** | **No** | **Control** | **Remarks** |
|  | X | Manual monitoring, maintenance, and intervention for legacy systems | The monitoring and maintenance is not sufficient for the legacy systems. |
|  | X | Encryption | No encryption is used. |
|  | X | Password management system | Not installed |
| X |  | Locks (offices, storefront, warehouse) | Sufficient according to assessment. No improvements necessary. |
| X |  | Closed-circuit television (CCTV) surveillance | Sufficient according to assessment. No improvements necessary. |
| X |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) | Sufficient according to assessment. No improvements necessary. |

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | **Remarks** |
|  | X | Only authorized users have access to customers’ credit card information. | Principle of least privilege is not used, all employees could access the data |
|  | x | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. | No encryption is used and all employees can access the data. |
|  | X | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | No encryption is currently used |
|  | X | Adopt secure password management policies. | The password policies are nominal and should be improved according to the requirement standarts |

General Data Protection Regulation (GDPR)

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | **Remarks** |
|  | X | E.U. customers’ data is kept private/secured. | No encryption and access to data is manage poorly. |
| X |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. | Compliant |
|  | X | Ensure data is properly classified and inventoried. | Data is listed, but not classified |
| X |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. | Compliant |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Yes** | **No** | **Best practice** | **Remarks** |
|  | X | User access policies are established. | Principle of least privilege should be implemented |
|  | X | Sensitive data (PII/SPII) is confidential/private. | No encryption -> not confidential |
| X |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | Compliant |
|  | X | Data is available to individuals authorized to access it. |  |

This section is 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:**

* Implement a principle of least privilege: The employees should have only the minimum access to data in order to fulfill their tasks.
* Implement a disaster recovery plan for all applicable scenarios.
* Make sure that the password policies follow the current requirements for the
* Separation of duties should be applied: Critical actions should rely on multiple people, each of whom follow the principle of least privilege.
* Ensure that the data is encrypted and stored in database that is not accessible for anyone who is not authorized. This will improve the confidentiality of the PII/SPII data (eg. Card holder data).
* Make sure that the legacy systems have a schedule in place for maintanance and monitoring and make sure that the task and procedures for intervention are clear for the employees involved.
* Implementing a password management system to enforce proper password usage.