# 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** | **Explanation** |
| --- | --- | --- | --- |
|  |  | Least Privilege | Currently, all employees have access to customer data;  Privileges needs to be reviewed and limited to reduce risk of breach and ensure safety of customers data |
|  |  | Disaster recovery plans | There are no disaster recovery plans in place. To ensure business continuity those need to be implemented |
|  |  | Password policies | Password policies are minimal. To reduce risk of breach and ensure safety, those need to be updated. |
|  |  | Separation of duties | Needs to be implemented to reduce any possibility of fraud or access to critical data |
|  |  | Firewall | Existing firewall blocks traffic according to set of security rules |
|  |  | Intrusion detection system (IDS) | To help identify possible intrusions by threat actors the IDS needs to be implemented |
|  |  | Backups | Currently there are no backups, those need to be implemented, maintained and secured to ensure business continuity |
|  |  | Antivirus software | Antivirus software is installed and monitored by IT department |
|  |  | Manual monitoring, maintenance, and intervention for legacy systems | There should be a regular schedule in place. The tasks and procedures/policies related to intervention are unclear, this makes those systems at risk in a breach |
|  |  | Encryption | Encryption is not currently used; It makes customers’ data at risk in possible breach. Those should be placed to ensure confidentiality of sensitive information |
|  |  | Password management system | Password management system is currently not in place, it would ensure business continuity in case of password related issues |
|  |  | Locks (offices, storefront, warehouse) | The store physical location, which contains the company’s main office, storefront and warehouse of products ha sufficient locks |
|  |  | Closed-circuit television (CCTV) surveillance | CCTV is installed at store’s physical location |
|  |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) | Company’s physical location has functioning Fire detection and prevention systems |

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** | **Explanation** |
| --- | --- | --- | --- |
|  |  | Only authorized users have access to customers’ credit card information. | Currently all employees have access to company’s internal data |
|  |  | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. | Credit card information is at risk. Currently it is not encrypted and all employees have access to all internal data this includes Credit card information |
|  |  | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | There's no encryption of data currently. To ensure confidentiality use data encryption. |
|  |  | Adopt secure password management policies. | Password policies that are currently set are not enforced and theres no password management system. |

General Data Protection Regulation (GDPR)

| **Yes** | **No** | **Best practice** | **Explanation** |
| --- | --- | --- | --- |
|  |  | E.U. customers’ data is kept private/secured. | Botium Toys currently does not use any form of encryption to ensure confidentiality of customers information |
|  |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. | There is a plan to notify E.U. customers within 72 hours of data breach |
|  |  | Ensure data is properly classified and inventoried. | Current assets have been inventoried but have not been classified |
|  |  | Enforce privacy policies, procedures, and processes to properly document and maintain data. | Privacy policies, procedures, and  processes have been developed  and enforced among IT team  members and other employees, as  needed. |

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

| **Yes** | **No** | **Best practice** | **Explanation** |
| --- | --- | --- | --- |
|  |  | User access policies are established. | Currently, all employees have access to all internal data. Least privilege should be implemented to ensure safety of customers data in case of a breach |
|  |  | Sensitive data (PII/SPII) is confidential/private. | Encryption is currently not used. In consequence of this customers data is not protected in case of breach |
|  |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | Data integrity is in place |
|  |  | Data is available to individuals authorized to access it. | All employees have access to all the data. It should be limited to only those employees who need access to it to do their job |

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.

* Only authorized Botium Toys employees should have access to internally stored data. Cardholder data and customers PII/SPII should be accessed by those who need it for work.
* Encryption should be used to ensure confidentiality of customers’ credit card information that is accepted, processed, transmitted, and stored locally in the company’s internal database.
* Access controls pertaining to least privilege and separation of duties should be implemented (e.g., only people who need PII of customers to work should have access to those)
* There should be a recovery plan created in case of data loss. Backups of critical data should be created, maintained and stored properly.
* Better password policies should be forced upon all employees.
* Centralized password management system should be implemented to increase productivity