# 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 |
|  |  | Disaster recovery plans |
|  |  | Password policies |
|  |  | Separation of duties |
|  |  | Firewall |
|  |  | Intrusion detection system (IDS) |
|  |  | Backups |
|  |  | Antivirus software |
|  |  | Manual monitoring, maintenance, and intervention for legacy systems |
|  |  | Encryption |
|  |  | Password management system |
|  |  | Locks (offices, storefront, warehouse) |
|  |  | Closed-circuit television (CCTV) surveillance |
|  |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) |

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. |
|  |  | Credit card information 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 notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
|  |  | Ensure data is properly classified and inventoried. |
|  |  | 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** |
| --- | --- | --- |
|  |  | 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 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.

**Summary**

Botium Toys' needs multiple controls to improve its security and safeguard sensitive data. This includes implementing Least Privilege, disaster recovery plans, password policies, separation of duties, an IDS (Intrusion Detection System), ongoing legacy system management, encryption, and a password management system.

In addition, compliance gaps demand immediate action. Least privilege, separation of duties, and encryption are priority controls. Additionally, proper asset classification will reveal further controls necessary to bolster security and shield sensitive information.

**Recommended Controls to Implement**

* Least privilege - Unrestricted access to customer data puts us at risk of a breach. It's crucial to limit employee privileges based on their specific roles and responsibilities.
* Disaster recovery plans - The absence of disaster recovery plans is a critical gap in our security posture. These need to be implemented to ensure business continuity.
* Password policies - Employee password requirements are minimal, a threat actor can easily infiltrate our systems through employee devices and steal customer data, disrupt operations, or even cause financial damage.
* Separation of duties - the current practice of the CEO handling both daily operations and payroll management presents a potential risk for fraud or inappropriate access to sensitive data. Implementing separation of duties will mitigate this risk.
* Intrusion detection system (IDS) - The IT department needs an IDS in place to help identify possible intrusions by threat actors.
* Backups - The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.
* Manual monitoring, maintenance, and intervention for legacy systems - The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is not a regular schedule in place for this task and procedures/ policies related to intervention are unclear. By implementing a regular maintenance schedule with clear procedures for intervention, we can significantly improve the security and stability of our legacy systems.
* Encryption - Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.
* Password management system - There is no password management system currently in place; implementing this control would improve IT department/other employee productivity in the case of password issues.

**(PCI DSS) Compliance flags**

* Currently, all employees have access to the company’s internal data.
* Credit card information is not encrypted and all employees currently have access to internal data, including customers’ credit card information.
* The company does not currently use encryption to better ensure the confidentiality of customers’ financial information.
* Password policies are nominal and no password management system is currently in place.

**(GDPR) Compliance flags**

* The company does not currently use encryption to better ensure the confidentiality of customers’ financial information.
* Current assets have been inventoried/listed, but not classified.

**(SOC type 1, SOC type 2) Compliance flags**

* Controls of Least Privilege and separation of duties are not currently in place; all employees have access to internally stored data.
* Encryption is not currently used to better ensure the confidentiality of PII/SPII.
* While data is available to all employees, authorization needs to be limited to only the individuals who need access to it to do their jobs.