# 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:**

1. It is observed that all employees have access to internally stored data. This allows for all employees to access PII and SPII of all their clients. This is in poor consideration of user data and asset confidentiality. Necessary measures like access controls, encryption etc. can be implemented to ensure that user data is protected to prevent fraudulent activities like identity theft, debit scams etc.

It is also crucial to implement user access policies to protect sensitive information and ensure compliance with internal standards and external regulations.

1. Encryption is one the most effective tools that can be used to protect sensitive data. By implementing this feature/tool we can protect sensitive information like customers’ credit card information. By storing this data in the company’s database the members of this organization are jointly responsible for the safekeeping of this data. Encrypting the data ensures that unauthorized access and misuse can be kept at bay.
2. It is expected that within a small business, the IT field will handle the above core responsibilities. However, this clashes with some important security principles like separation of duties and least privilege. These principles are implemented to prevent misuse of assets, fraud etc.

Considering that the company is growing in size it would be advisable to split or expand the IT department to include other sectors such as a dedicated cybersecurity team, a network administration team, and a helpdesk support team to inculcate separation of duties and least privilege to ensure more secure systems with a more minimized risk of unauthorized use or fraud.

1. Although legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear. Legacy systems are those systems in which the software or hardware is too old for it to interact with newer systems. Typically it's the cyber field's responsibility to ensure that confidential data and assets are wiped out securely and properly disposed of.

A proper schedule must be implemented on how to deal with these systems in terms of disposal and maintenance.

1. Part of an efficient security system (as per OWASP security principles) is to ensure a safe failure.

A disaster recovery plan ensures that when a threat occurs, it is contained, responded to and the system is returned to its initial working state (to also ensure business continuity, and maintain the company’s reputation).

1. Although a few walls have been built against cyberattacks by means of implementing firewalls and antivirus software, Intrusion Detection systems are also highly recommended.

ID’s allow detection of an attempted security breach. Based on this it is possible for us to investigate the incident, assess the situation and report it. Necessary actions can be taken to respond to the threat that was posed.

1. It is comparatively easy for an attacker to decrypt a user’s password if it is simple. To avoid such scenarios it’s important to implement password policies and have an effective management system.

Enforce stricter password policies that meet the current minimum password policies. Use a password management tool that enforces password policies and allows users to reset or recover their passwords independently. This reduces the burden on the IT department and minimizes downtime for users.

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 (optional):**

Stakeholders are recommended to adhere to the password policies to create stronger passwords. This ensures that the user’s private or confidential data and assets are better protected.

In addition to that, enabling users to reset and recover their passwords on their own allow for users to experience minimum downtime.

—------------------------------------------------------------------------------------