# 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** |
|  | X | Least Privilege |
|  | X | Disaster recovery plans |
|  | X | Password policies |
|  | X | Separation of duties |
| X |  | Firewall |
|  | X | Intrusion detection system (IDS) |
|  | X | Backups |
| X |  | Antivirus software |
|  | X | Manual monitoring, maintenance, and intervention for legacy systems |
|  | X | Encryption |
|  | X | Password management system |
| X |  | Locks (offices, storefront, warehouse) |
| X |  | Closed-circuit television (CCTV) surveillance |
| X |  | 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#heading=h.evidx83t54sc). 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, type an X in the “yes” or “no” column 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** |
|  | X | Only authorized users have access to customers’ credit card information. |
|  | X | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
|  | X | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
|  | X | Adopt secure password management policies. |

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  | X | E.U. customers’ data is kept private/secured. |
| X |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
|  | X | Ensure data is properly classified and inventoried. |
| X |  | 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** |
|  | X | User access policies are established. |
|  | X | Sensitive data (PII/SPII) is confidential/private. |
| X |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
|  | X | 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.

There are several potential risk issues in the current audit results. I recommend getting fixed as quickly as possible to avoid any potential harm or legal issues in the future. The first changes I recommend is to make sure all data and information is classified and stored properly and then establish a principle of Least Privilege system within the organization as not everyone in the company needs to have access to the Internally stored data or need to be able to access to cardholder data and/or customers PII/SPII information. Only those who have been specifically hired to work with that information should have the privileges needed to do their job and nothing more, to help prevent any exploits threat actors could use to gain access to any private information or accidental leakage of the information as well.

The second change I recommend making is establishing both a stronger Password Policy as the currently one is too weak and is an easy target for a Threat Actor to take advantage of but I also recommend establishing a password management system to have more control of which users have access to the systems, but also grants the ability to quickly disable a user if the employee is either fired, quits their job from the company or even goes away on holidays having a password management system would allow for quick disabling of user account so threat actors cannot use the account as a method of accessing the system why the user is away.

The third change I recommend is to establish an encryption system to better ensure the safety and confidentiality of customers credit card information, as well as install an Intrusion Detection System to help monitor and catch any unauthorized use of the customer credit cards as well. which will also help the company to be much more compliant to the General Data Protection Regulations act (GDPR) as well to help satisfy PCI DSS regulations,

The fourth and final change I recommend is improving the way the Legacy systems are being monitored and maintained by establishing a regular schedule to perform the required tasks and interventions as well as making the methods much clearer and easier to follow for anyone is currently assigned to the role and for future hires, this includes backing up the systems. I recommend there being 2 different backups in place one scheduled to be done once a week and another back up to be done once a month and kept in a safe as possible storage location so that if a security incident happens once the issues have been resolved it will help the security teams to recover after the incident by rolling back the company system back to a date prior to the incident to hopefully help mitigate how much is lost and quickly help get the company back in to proper functioning order.