# 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**

|  |
| --- |
| **Control** |
| Least Privilege **NO** |
| Disaster recovery plans **NO** |
| Password policies **NO** |
| Separation of duties **NO** |
| Firewall **YES** |
| Intrusion detection system (IDS) **NO** |
| Backups **NO** |
| Antivirus software **YES** |
| Manual monitoring, maintenance, and intervention for legacy systems **NO** |
| Encryption **NO** |
| Password management system **NO** |
| Locks (offices, storefront, warehouse) **YES** |
| Closed-circuit television (CCTV) surveillance **YES** |
| Fire detection/prevention (fire alarm, sprinkler system, etc.) **YES** |

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)***

|  |
| --- |
| **Best practice** |
| Only authorized users have access to customers’ credit card information. **NO** |
| Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. **NO** |
| Implement data encryption procedures to better secure credit card transaction touchpoints and data. **NO** |
| Adopt secure password management policies. **NO** |

***General Data Protection Regulation (GDPR)***

|  |
| --- |
| **Best practice** |
| E.U. customers’ data is kept private/secured. **NO** |
| There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. **YES** |
| Ensure data is properly classified and inventoried. **NO** |
| Enforce privacy policies, procedures, and processes to properly document and maintain data. **YES** |

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

|  |
| --- |
| **Best practice** |
| User access policies are established. **NO** |
| Sensitive data (PII/SPII) is confidential/private. **NO** |
| Data integrity ensures the data is consistent, complete, accurate, and has been validated. **YES** |
| Data is available to individuals authorized to access it. **YES** |

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):**

1. **Implement Least Privilege Access Control** – Employees should only have access to data necessary for their job roles to reduce insider threats.
2. **Develop and Implement a Disaster Recovery Plan** – There are no backups of critical data, which means the business is at high risk of data loss.
3. **Adopt Strong Password Policies and a Password Management System** – The current password policy does not meet industry standards, and a centralized password management system should be implemented.
4. **Introduce Data Encryption** – To comply with PCI DSS and GDPR, encryption should be implemented to protect sensitive customer and financial data.
5. **Deploy an Intrusion Detection System (IDS)** – The IT department should install an IDS to detect and respond to cyber threats in real time.
6. **Enforce Separation of Duties** – The company should implement role-based access controls to prevent unauthorized access to sensitive data.
7. **Improve Compliance with PCI DSS and GDPR** – Implement proper data classification, restrict access to credit card information, and ensure compliance with global data security standards.