

# Controls and compliance checklist

## Controls assessment checklist

Yes	No	Control
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Least Privilege <ul style="list-style-type: none"><li>all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.</li></ul>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Disaster recovery plans <ul style="list-style-type: none"><li>There are no disaster recovery plans currently in place.</li></ul>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Password policies <ul style="list-style-type: none"><li>Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.</li></ul>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Separation of duties <ul style="list-style-type: none"><li>Access controls pertaining to least privilege and separation of duties have not been implemented.</li></ul>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Firewall <ul style="list-style-type: none"><li>The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.</li></ul>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Intrusion detection system (IDS) The IT department has not installed an intrusion detection system (IDS).
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Backups <ul style="list-style-type: none"><li>the company does not have backups of critical data.</li></ul>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Antivirus software <ul style="list-style-type: none"><li>Antivirus software is installed and monitored regularly by the</li></ul>

department.

- |                                     |                                     |  |
|-------------------------------------|-------------------------------------|--|
| <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Manual monitoring, maintenance, and intervention for legacy systems <ul style="list-style-type: none"><li>• While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.</li></ul> |
| <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Encryption <ul style="list-style-type: none"><li>• No encryption for customer credit card information</li></ul>  |
| <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Password management system <ul style="list-style-type: none"><li>• There is no centralized password management system that enforces the password policy's minimum requirements.</li></ul>  |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Locks (offices, storefront, warehouse) <ul style="list-style-type: none"><li>• The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks.</li></ul>                                      |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Closed-circuit television (CCTV) surveillance <ul style="list-style-type: none"><li>• Company has up to date CCTV surveillance.</li></ul>  |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Fire detection/prevention (fire alarm, sprinkler system, etc.) <ul style="list-style-type: none"><li>• functioning fire detection and prevention systems.</li></ul>  |

---

## Compliance checklist

### Payment Card Industry Data Security Standard (PCI DSS)

<b>Yes</b>	<b>No</b>	<b>Best practice</b>
------------	-----------	----------------------

- |                          |                                     |   |
|--------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Only authorized users have access to customers' credit card information. <ul style="list-style-type: none"> <li>• Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.</li> </ul>                            |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. <ul style="list-style-type: none"> <li>• Lack of encryption puts the credit card information at risk of being stolen.</li> </ul>   |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Implement data encryption procedures to better secure credit card transaction touchpoints and data. <ul style="list-style-type: none"> <li>• Encryption is not currently used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.</li> </ul> |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Adopt secure password management policies.<br>There is no centralized password management system that enforces the password policy's minimum requirements,  |

### General Data Protection Regulation (GDPR)

- | Yes                                 | No                       | Best practice  |
|-------------------------------------|--------------------------|--|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | E.U. customers' data is kept private/secured. <ul style="list-style-type: none"> <li>• Privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain E.U customers' data.</li> </ul> |

- |                                     |                                     |  |
|-------------------------------------|-------------------------------------|--|
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. <ul style="list-style-type: none"> <li>• The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach.</li> </ul> |
| <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Ensure data is properly classified and inventoried.  |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | 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   |
|-------------------------------------|-------------------------------------|---|
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | User access policies are established.   |
| <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Sensitive data (PII/SPII) is confidential/private.  |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Data integrity ensures the data is consistent, complete, accurate, and has been validated. <ul style="list-style-type: none"> <li>• The IT department has ensured availability and integrated controls to ensure data integrity.</li> </ul> |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | Data is available to individuals authorized to access it.   |
- 

### **Recommendations:**

1. Minimize employee access to internal stored data
  - a. Current and former employees can cause extremely high damage to company data, each employee should only have access to data they need.
2. Develop a disaster recovery plan
  - a. Identify and collect information on all hardware, software applications and data.
  - b. Data backup( develop a data backup plan as a corrective measure)

3. Encrypt credit card information
  - a. Stolen customer information is a high risk that can damage a company's reputation as well as reduce its value significantly.
  - b. Encryption will ensure that valuable customer data remains confidential.
4. Separate access/duties
  - a. Entire company data access should not be in the hands of 1 or 2 people, there should be a sizable amount of people who each have their own level of access to minimize internal security risks.
5. Actively use an IDS(Intrusion Detection System)
  - a. The company is at risk without an IDS in place, in case of an attack, an IDS will detect it and alert the cyber security team to take appropriate action efficiently to minimize damage.
6. Minimize legacy system use
  - a. The company should stop using old software/systems as they can be easily infiltrated by a threat actor.
  - b. If legacy systems are mandatory, there should be a clear schedule in place to actively monitor and intervene in case of an attack.
7. Create a password management system
  - a. This will enforce the data security of the company and also improve employee productivity as it will reduce the number of times the employees have to reset their password.
8. Classify existing data
  - a. The company should immediately identify the value of specific company data and implement security measures to protect them.
9. Protect sensitive data
  - a. All Botium Toys' employees have access to sensitive customer data, this should be changed accordingly.