# Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each control, including the type and purpose, refer to the control categories 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<br>*"Access controls pertaining to least privilege and separation of duties have not been implemented."* |
| ☐ | ☑ | Disaster recovery plans<br>*"There are no disaster recovery plans currently in place."* |
| ☑ | ☐ | Password policies<br>*"Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters)."*<br>*The company still should implement a stronger password policy to enforce password complexity.* |
| ☐ | ☑ | Separation of duties<br>*"Access controls pertaining to least privilege and separation of duties have not been implemented."* |
| ☑ | ☐ | Firewall<br>*"The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules."* |
| ☐ | ☑ | Intrusion detection system (IDS)<br>*"The IT department has not installed an intrusion detection system* |

*(IDS)."*

☐ ☑ Backups
*"The company does not have backups of critical data."*

☑ ☐ Antivirus software
*"Antivirus software is installed and monitored regularly by the IT department."*

☐ ☑ Manual monitoring, maintenance, and intervention for legacy systems
*"While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear."*

☐ ☑ Encryption
*"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."*

☐ ☑ Password management system
*"There is no centralized password management system that enforces the password policy's minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password."*

☑ ☐ Locks (offices, storefront, warehouse)
*"The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems."*

☑ ☐ Closed-circuit television (CCTV) surveillance
*"The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems."*

☑ ☐ Fire detection/prevention (fire alarm, sprinkler system, etc.)
*"The store's physical location, which includes Botium Toys' main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems."*

---

To complete the compliance checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each compliance regulation, review the 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.<br>*"Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers’ PII/SPII."* |
| ☐ | ☑ | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.<br>*"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."* |
| ☐ | ☑ | Implement data encryption procedures to better secure credit card transaction touchpoints and data.<br>*"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."* |
| ☐ | ☑ | Adopt secure password management policies.<br>*"Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters)."* |

General Data Protection Regulation (GDPR)

| Yes | No | Best practice |
|---|---|---|
| ☐ | ☑ | E.U. customers' data is kept private/secured.<br>*"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."* |
| ☑ | ☐ | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.<br>The company<br>*"The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach."* |
| ☐ | ☑ | Ensure data is properly classified and inventoried.<br>*"Storefront products available for retail sale on site and online; stored in the company's adjoining warehouse"*<br>*"Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management"*<br>*Does not show evidence of classification.* |
| ☑ | ☐ | Enforce privacy policies, procedures, and processes to properly document and maintain data.<br>*"privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, 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.<br>*"Access controls pertaining to least privilege and separation of duties have not been implemented."* |
| ☐ | ☑ | Sensitive data (PII/SPII) is confidential/private.<br>*"Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII."* |

| | | |
|---|---|---|
| ☑ | ☐ | Data integrity ensures the data is consistent, complete, accurate, and has been validated.<br>*"The IT department has ensured availability and integrated controls to ensure data integrity."* |
| ☐ | ☑ | Data is available to individuals authorized to access it.<br>*"Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII."* |

---

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.