# 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 | Explanation |
|---|---|---|---|
| ☐ | ☑ | Least Privilege | *Currently, all employees have access to personal and sensitive information of customers; privileges need to be implemented to avoid the handling of data by unauthorized users.* |
| ☐ | ☑ | Disaster recovery plans | *Currently, there are no disaster recovery plans in place; this should be implemented to provide business continuity in case an incident occurs.* |
| ☐ | ☑ | Password policies | *Password policies exist, but it's nominal and do not require complexity; passwords should be strong and complex by requiring a combination of at least eight characters, at least one number, and one special character.* |
| ☐ | ☑ | Separation of duties | *Currently, separation of duties is not implemented; This should be implemented to reduce risk and prevent malicious insider or compromised accounts.* |
| ☑ | ☐ | Firewall | *Firewall implemented and blocks traffic based on an appropriately defined set of security rules.* |
| ☐ | ☑ | Intrusion detection system (IDS) | *Currently, IDS is not implemented; it should be implemented to monitor suspicious activities within the network to prevent a security breach.* |
| ☐ | ☑ | Backups | *Currently, they don’t have backups in place;/ this is important and should be implemented, as this* |

| | | | |
|---|---|---|---|
| | | | *will continue the operation of an organization if an incident occurs.* |
| ☑ | ☐ | Antivirus software | *Antivirus is implemented and regularly monitored by the IT department.* |
| ☐ | ☑ | Manual monitoring, maintenance, and intervention for legacy systems | *Currently, legacy systems are monitored and maintained, but they don't have a regular schedule for these tasks, and intervention methods are unclear; legacy systems must be monitored and maintained up-to-date to prevent threats and vulnerabilities. Intervention needs to be in place in order to mitigate risks.* |
| ☐ | ☑ | Encryption | *Currently, encryption is not implemented; this should be in place to ensure the confidentiality of customers' personal and sensitive information.* |
| ☐ | ☑ | Password management system | *Currently, they don't have one main system to manage all passwords that also makes sure people follow the rules for creating strong passwords; this needs to be implemented to ensure security protection, save time, and improves productivity, and reduce human errors and password fatigue.* |
| ☑ | ☐ | Locks (offices, storefront, warehouse) | *The store's physical location and warehouse of products have sufficient locks to prevent unauthorized personnel or individuals from physically accessing assets.* |
| ☑ | ☐ | Closed-circuit television (CCTV) surveillance | *They have up-to-date CCTV surveillance.* |
| ☑ | ☐ | Fire detection/prevention (fire alarm, sprinkler system, etc.) | *They have a fire detection and prevention system that can prevent damage to physical assets.* |

---

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 | Explanation |
|---|---|---|---|
| ☐ | ☑ | Only authorized users have access to customers' credit card information. | *Currently, all employees have access to personal and sensitive information or data of customers* |
| ☐ | ☑ | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. | *Currently, encryption is not implemented, so the credit card information that is stored locally in their database is not secured.* |
| ☐ | ☑ | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | *They have not implemented encryption to secure their customers' credit card information.* |
| ☐ | ☑ | Adopt secure password management policies. | *Password policy requirements are nominal and not in line with the current minimum password complexity requirements.* |

General Data Protection Regulation (GDPR)

| Yes | No | Best practice | Explanation |
|---|---|---|---|
| ☐ | ☑ | E.U. customers' data is kept private/secured. | *Since encryption is not implemented, and all employees can access personal and sensitive information, the customer's data is not secured.* |
| ☑ | ☐ | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. | *They established a plan to notify E.U. customers within 72 hours if a security breach occurs.* |
| ☐ | ☑ | Ensure data is properly | *Current assets are listed but not classified* |

| | | | |
|---|---|---|---|
| | | classified and inventoried. | |
| ☑ | ☐ | Enforce privacy policies, procedures, and processes to properly document and maintain data. | *Privacy policies, procedures, and processes are established and enforced among the IT Department and employees to properly document and maintain data.* |

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

| Yes | No | Best practice | Explanation |
|---|---|---|---|
| ☐ | ☑ | User access policies are established. | *Access controls and separation of duties are not implemented* |
| ☐ | ☑ | Sensitive data (PII/SPII) is confidential/private. | *Encryption is not implemented, so sensitive data is not secured.* |
| ☑ | ☐ | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | *The IT Department ensured the availability and implemented integrated controls to ensure data integrity.* |
| ☐ | ☑ | Data is available to individuals authorized to access it. | *All employees have access to internal data that has personal and sensitive information.* |

---

**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.

*To strengthen its security posture and protect critical assets, Botium Toys' needs to implement key controls across its systems and processes. This includes ensuring least privilege and separation of duties so employees have access only to what they need, establishing disaster recovery plans and backups to maintain operations during disruptions, and implementing strong password policies and a centralized password management system to reduce security risks and password fatigue. Additional protections, such as encryption, intrusion detection, and proper monitoring of legacy systems, will safeguard sensitive data and detect threats early.*

*To maintain regulatory compliance, Botium Toys' must ensure that credit card information and other sensitive customer data are securely stored, processed, and encrypted, and that only authorized users have access. For GDPR and data privacy, EU customer data must be protected, and all sensitive data should be properly classified and inventoried. Finally, clear user access policies and controls must be in place to ensure data is confidential yet available to authorized personnel. Implementing these measures will reduce the risk of breaches, improve productivity, and help the company avoid potential fines or violations.*