# Controls and compliance checklist

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 | *All employees have access to internal data, including sensitive customer information. Implementing this control will reduce insider risks.* |
| ☐ | ☑ | Disaster recovery plans | *No plans are currently in place, which are essential for business continuity during a breach or disaster.* |
| ☐ | ☑ | Password policies | *There are currently no plans established, and having them is vital for maintaining business continuity in the event of a breach or disaster.* |
| ☐ | ☑ | Separation of duties | *Not yet established; minimizing fraud risks and maintaining operational security is essential.* |
| ☑ | ☐ | Firewall | *A firewall is implemented to restrict traffic according to clearly defined security* |

| | | | |
|---|---|---|---|
| | | | *protocols.* |
| ☐ | ☑ | Intrusion detection system (IDS) | *An IDS is not currently in place. This system is needed to detect and respond to possible intrusions.* |
| ☐ | ☑ | Backups | *The company does not regularly back up important data. This puts business continuity at risk.* |
| ☑ | ☐ | Antivirus software | *Antivirus software is installed and routinely monitored.* |
| ☑ | ☐ | Manual monitoring, maintenance, and intervention for legacy systems | *Legacy systems are checked and fixed without a regular schedule or clear steps to follow.* |
| ☐ | ☑ | Encryption | *Encryption is not being used, which puts sensitive data at risk of being exposed.* |
| ☐ | ☑ | Password management system | *This control will boost employee productivity and lower the chances of password-related issues if it is not in place.* |

| | | | |
|---|---|---|---|
| ☑ | ☐ | Locks (offices, storefront, warehouse) | *Physical locations have secure locks.* |
| ☑ | ☐ | Closed-circuit television (CCTV) surveillance | *CCTV is installed and working at all locations.* |
| ☑ | ☐ | Fire detection/prevention (fire alarm, sprinkler system, etc.) | *The company has working fire detection and prevention systems.* |

---

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. | *All employees can access internal data, including credit card information.* |
| ☐ | ☑ | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. | *Credit card data is not properly encrypted or protected.* |

| | | | |
|---|---|---|---|
| ☐ | ☑ | Implement data encryption procedures to better secure credit card transaction touchpoints and data. | *Sensitive financial information is not protected by encryption.* |
| ☐ | ☑ | Adopt secure password management policies. | *The password policies are weak, and there is no system to manage passwords.* |

General Data Protection Regulation (GDPR)

| Yes | No | Best practice | Explanation |
|---|---|---|---|
| ☐ | ☑ | E.U. customers' data is kept private/secured. | *Customer data is not protected because encryption is not being used.* |
| ☑ | ☐ | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. | *A plan for notifying in the event of a breach has been established.* |
| ☐ | ☑ | Ensure data is properly classified and inventoried. | *The assets have been listed but not properly classified.* |
| ☑ | ☐ | Enforce privacy policies, procedures, and processes to properly document and maintain data. | *Privacy policies are established for IT staff and other employees.* |

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

| Yes | No | Best practice | Explanation |
|---|---|---|---|

| | | | |
|---|---|---|---|
| ☐ | ☑ | User access policies are established. | *The organization does not use Least Privilege or separate duties.* |
| ☐ | ☑ | Sensitive data (PII/SPII) is confidential/private. | *Failing to use encryption endangers the confidentiality of data.* |
| ☑ | ☐ | Data integrity ensures the data is consistent, complete, accurate, and has been validated. | *The data is reliable, comprehensive, and validated.* |
| ☑ | ☐ | Data is available to individuals authorized to access it. | *Data is available, but access should be limited to those who are authorized.* |

---

**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.

*Botium Toys must implement critical controls to enhance its security posture. These measures include adopting the principle of least privilege to limit access to sensitive data, developing disaster recovery plans for business continuity, and implementing encryption to secure customer and business data. Separation of duties must also be introduced to reduce the risks of fraud and unauthorized access, and an intrusion detection system (IDS) must be established to help detect and mitigate threats.*

*The company should also implement a Password Management System to enforce stronger password policies and enhance efficiency. Legacy Systems require scheduled maintenance and transparent procedures to mitigate risks. Proper classification and data inventory will help identify vulnerabilities and additional control requirements. Finally, enforcing secure access controls and ensuring compliance with PCI DSS and*

*GDPR standards is essential for maintaining the company’s reputation and customer trust and will significantly improve Botium Toys' security posture.*