

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 |
|-------------------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Least Privilege |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Disaster recovery plans |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Password policies |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Separation of duties |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Firewall |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Intrusion detection system (IDS) |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Backups |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Antivirus software |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Manual monitoring, maintenance, and intervention for legacy systems |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Encryption |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Password management system |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Locks (offices, storefront, warehouse) |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Closed-circuit television (CCTV) surveillance |

- ☒ ☐ Fire detection/prevention (fire alarm, sprinkler system, etc.)

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 |
|--------------------------|-------------------------------------|--|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Only authorized users have access to customers’ credit card information. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Adopt secure password management policies. |

General Data Protection Regulation (GDPR)

| Yes | No | Best practice |
|-------------------------------------|-------------------------------------|---|
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | E.U. customers’ data is kept private/secured. |
| <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. |
| <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 type="checkbox"/> | <input checked="" 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. |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Data is available to individuals authorized to access it. |

Recommendations

1. **Implement Least Privilege and Access Controls:** Right now, all employees have access to sensitive customer data, including PII/SPII and cardholder information. We need to immediately limit access based on job roles and enforce proper user access policies.
2. **Introduce Encryption:** Customer data is being stored and transmitted without encryption, which puts us at major risk. Encrypting data at rest and in transit should be a top priority to protect confidentiality and meet compliance standards.
3. **Develop and Test Disaster Recovery Plans and Backups:** The company currently has no disaster recovery plan and no data backups. This leaves us vulnerable to major data loss. Creating and testing a disaster recovery strategy is essential for business continuity.

4. **Upgrade Password Policies and Implement a Password Management System:**

While there is a basic password policy in place, it doesn't meet today's minimum standards. We also lack a centralized password manager, which leads to inefficiencies and security gaps. Both should be addressed.

5. **Deploy an Intrusion Detection System (IDS):** We're missing a critical layer of defense.

An IDS will help detect unauthorized access and suspicious activity before it becomes a bigger issue.

6. **Regularly Monitor and Maintain Legacy Systems:** While legacy systems are being looked at, there's no consistent process. We need to set a schedule and define clear intervention methods to manage these systems better.

7. **Improve PCI DSS Compliance:** We're not currently following some of the basic best practices, like restricting credit card access and encrypting payment data. This puts us at financial and legal risk if there's a breach. Addressing this should be urgent.

8. **Start Data Inventory and Classification for GDPR Compliance:** We're missing a step when it comes to organizing and managing customer data, especially for E.U. users. This will help us stay compliant and avoid penalties.