

Controls and compliance checklist

- Name: Botium Toys
- Industry type: Toys
- Organization size: Small
- Geo-location: 1 location in US - main office, storefront and warehouse
- Observations:
 - Growing online - IT department under pressure
 - IT manager concerns about not having solidified plan for business continuity
 - IT manager concerns about compliance with EU regulations internal process and online payments
 - IT manager wants to implement NIST CSF

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 |
| <input checked="" type="checkbox"/> | <input type="checkbox"/> | Fire detection/prevention (fire alarm, sprinkler system, etc.) |
-

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 type="checkbox"/> | <input checked="" 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 type="checkbox"/>	<input checked="" type="checkbox"/>	Data is available to individuals authorized to access it.

The scope of this audit is the entire security program at Botium Toys and the goal is to assess existing assets and complete the controls and compliance checklist to improve Botium Toys' security posture.

There are a lot of existing risks: Least privilege, separation of duties, disaster recovery plans, separation of duties, IDS, backups, encryption, and password management systems have not been implemented. The company has a weak password policy that does not fulfill the minimum password complexity requirements. The company also needs to classify the remaining assets to identify additional controls that may need to be implemented. These risks need to be addressed as soon as possible to keep up with the major online growth.

The company is not in compliance with GDPR or PCI DSS.