

SCENARIO:

This scenario is based on a fictional company.

OBJECTIVE:

Review the IT manager's scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist.

SCOPE AND GOALS:

The scope will focus on the (physical and digital) security infrastructure of Botium Toys, and the objectives will be to revise the security policies and suggest new ones if necessary.

RISK ASSESSMENT:

The physical security structure meets the requirements, as physical controls, such as locks, where only authorized persons have access to the keys, closed-circuit television (CCTV) and fire prevention help mitigate potential risks. On the part of technical controls, the firewall is well configured and the antivirus and software used in the store are always up to date, but they present many security flaws in administrative controls and some technical controls.

RECOMMENDATIONS:

Taking into consideration the objectives of the manager of Botium Toys for conducting business with the U.S., the company needs to comply with the GDPR and to ensure the security of its customers' data with PCI DSS.

Administrative Controls that need to be implemented: Least Privilege, Disaster recovery plans, Password policies, Access control policies and Separation of duties.

Technical Controls that need to be implemented: IDS/IPS, Encryption, Backups, Password management and Manual monitoring, maintenance, and intervention.

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 checked="" type="checkbox"/>	<input 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.)

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 type="checkbox"/> | <input checked="" 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. |