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**
☐	☑	Least Privilege
☐	☑	Disaster recovery plans
☐	☑	Password policies
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	Antivirus software
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems
☐	☑	Encryption
☐	☑	Password management system
☐	☑	Locks (offices, storefront, warehouse)
☑	☐	Closed-circuit television (CCTV) surveillance
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Answers by Amir Sebastian Flores Cardona

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
☐	☑	Only authorized users have access to customers' credit card information.
☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
☐	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	☑	E.U. customers' data is kept private/secured.
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☐	☑	Ensure data is properly classified and inventoried.
☐	☑	Enforce privacy policies, procedures, and processes to properly document and maintain data.

Answers by Amir Sebastian Flores Cardona

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

Yes	**No**	**Best practice**
☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is confidential/private.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☑	☐	Data is available to individuals authorized to access it.

Answers by Amir Sebastian Flores Cardona

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

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.

<u>Areas for Improvement:</u>

- *Controls Assessment:*
    - Ensure the Least Privilege principle is fulfilled to prevent data leaks.
    - Develop and Implement a Disaster Recovery Plan in case of an incident.
    - Ensure password policies are fulfilled for better data and asset's protection.
    - Ensure each employee doesn't have lots of control over critical parts of an important process by implementing the separation of duties principle.
    - Our current firewall complies with the current audit, but still open to future improvements
    - Make sure an IDS is implemented in our current system to efficiently detect any potential threat.
    - Make sure that a backup system is implemented in case of a loss event.
    - Our current Anti-virus is up to date, but open to any improvements in the future.
    - The current monitoring and maintenance of the legacy systems require human intervention, but there is not a regular schedule for these tasks and intervention methods (which are unclear).
    - Encryption and a Password Management System should start its implementation after this audit to protect the SPII and PII of the clients.
    - Locks are insufficient, and should invest more on physical security.
    - CCTV surveillance and Fire detection are up to date, open to any improvements in the future.

- *Compliance*:
    - All authorized users have access to all the customer’s credit card information. The Least Privilege principle should resolve this matter.
    - Credit card information is stored, accepted, processed, and transmitted internally. But not in a secure environment.
    - Implementing encryption and password secure management should be implemented to better secure card transactions. As for now, still not implemented.
    - Implementing encryption and the password secure management should solve the password management policies.

- *General Data Protection Regulation (GDPR):*
    - E.U. is still to be completely secured. Right now the passwords are not encrypted and the data isn’t in a CypherText format for better security.
    - As for now, there’s a plan to notify E.U. within 72 next hours if data is compromised.
    - As for now, data isn’t properly classified nor inventoried properly (need more context for this one in particular).
    - As for now, privacy policies, procedures, and processes to properly document and maintain data are not properly enforced by the company.

- Systems and Organizations Controls:
    - Users access policies are still to be defined and implemented.
    - SPII and PII are confidential (within the company), but the Least Privilege principle should be implemented for better security.
    - According to the Additional comments of the current audit, the IT department has ensured availability and has integrated controls to ensure data integrity.
    - Even though the LP principle is not yet implemented, we could say that the data is available for all authorized individuals (which are all users according to the audit file).

Answers by Amir Sebastian Flores Cardona