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.)
☑	☐	

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.

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.

Recommendations : Based on the security audit for Botium Toys, there aren't just compliance issues associated with GDPR, SOC type 1, SOC type 2 and PCI DSS, but there are also critical risks Administrative/managerial controls.

The company does not adhere to any of the best practices of PCI DSS. I would recommend the company to secure the customer's credit card database so only people with access can access it instead of the entire organization. The information should always be secure to preserve the confidentiality, integrity and availability of the data. Encrypt all the data and adopt secure password management policies.

More specifically, E.U. the union's customer data should be securely stored and classified to ensure compliance with GDPR.

Since PII and SPII are important pieces of information as it could result in severe consequences for the organization if leaked, the principle of least privilege should be implemented so only necessary individuals have access to the data. That information

should also be securely stored. The company needs to ensure user policies are established to meet compliance with SOC type 1 and SOC type 2.

There are a lot of security controls that need to be implemented within the organization to mitigate risks, threats, and vulnerabilities. Some of them include implementing disaster recovery plans, password policies, separation of duties, backups, IDS, Manual monitoring, maintenance, and intervention for legacy systems, encryption, and password management system.