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.

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.

1. Currently, all employees have access to internally stored data, and may even have access to PII/SPII. The principle of least privilege would strongly benefit Botium Toys, providing employees the minimum amount of access needed to do their job function.
2. There is currently no disaster recovery plan. In order to maintain business continuity, Botium Toys should establish a risk disaster recovery plan, and take regular backups of its assets and data.
3. While there is a password policy, it was noted that the requirements are nominal and not in-line with minimum password complexity requirements. All employees should be adhering to a strong password policy, as well as requirements to update their password

often. Passwords that are stored locally should be done securely and with an appropriate key-safe.

4. Separation of duties refers to dividing responsibilities amongst different employees or entities to create a system of checks and balances.Currently all users have access to internally stored data, and linking back to principle of least privilege, SoD should be implemented so that organisations can minimise the risk of conflicts of interest, unauthorized access, and insider threats.
5. It's good that Botium Toys has a firewall that blocks traffic based on an appropriately defined set of security rules. To further improve on this, the company should regularly review the firewall rules and perform updates. They should also implement an IDS/IPS (Implement Intrusion Detection/Prevention Systems). This would help provide additional layers of defence against malicious activities.
6. Antivirus software is installed and regularly maintained, which is good.
7. Legacy systems are monitored and maintained, but with no clear scheduling and plan of action. Legacy systems can have vulnerabilities due to out-dated software / updates. Botium Toys should consider replacing these legacy systems, and in the meantime implementing regular system checks to look for vulnerabilities and risks.
8. There is no use of encryption for securing data, which is very insecure. It can lead to Data interception and tempering, unauthorised access, and compliance violations. For Botium Toys, I would recommend AES (Advanced Encryption Standard). Which is a widely used symmetric encryption algorithm known for its efficiency and security.
9. Overall the organisation has good physical controls. However, with inadequate management of assets, the organisation should identify all assets and data and implement the necessary protections to help adhere to regulations and standards. Also as it was not mentioned, there should be sufficient lighting in the buildings as a deterrent from attacks.
10. There is a plan to notify EU customers within 72 hours, however the organisation has poor management of data access and controls, making it highly vulnerable to inside threats. As mentioned, the company needs to address this by implementing privilege of least principle and separation of duties.