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.

Currently, there are many controls that need to be implemented by Botium Toys in order to improve their security posture and comply with multiple laws and regulations. Adding access control to the Botium Toys' internal network is a glaring need. Implementing access control will allow Botium Toys to limit access to customer's PII and SPII to employees that require it, making sensitive information confidential and implementing the principle of least privilege. Implementing access control will also allow Botium Toys to properly implement separation of duties, ensuring that no single employee has access over too much of the internal network and further improving security posture.

In addition to access control, strengthening the password requirements and implementing a password management system is also a very glaring need. The current password requirements for both employees and vendors are currently too lenient and these requirements are not being enforced by a

password management system. Implementing stricter password requirements and ensuring they are at least consistent with current minimum password complexity requirements (at least 8 characters, at least one special character, and at least one number) will greatly improve security posture. Additionally, implementing a centralized password management system to enforce these new password requirements would also be greatly beneficial.

Encrypting passwords and other sensitive data would also greatly improve Botium Toys' security posture. Implementing encryption policies ensures that sensitive data is properly protected in the Botium Toys' internal systems. Currently, with no implemented encryption, sensitive data is at high risk and could be compromised by attackers.

Currently, Botium Toys does not have an intrusion detection system (IDS) in place. Ensuring that an IDS is implemented is essential for ensuring that attackers who gain access to the Botium Toys' network are detected and proper response can take place. With no current IDS, detecting intruders becomes much more difficult.

Additionally, while current legacy systems are manually monitored and maintained, there are no current schedules for these tasks and there are no intervention methods in place for these systems. Ensuring schedules are in place to manually monitor and maintain legacy systems ensures that any problems with these systems are detected. Additionally, making sure that intervention methods are in place ensures that intervention is possible and any problems or vulnerabilities can be addressed.

Moving on to recovery, creating and implementing disaster recovery plans as well as ensuring that critical data is backed up is also a necessity. Implementing disaster recovery plans ensures that procedures are in place to respond to an incident and backing up data ensures that it can be recovered properly and efficiently.

Taking into account the recommendations above will greatly improve Botium Toys' security posture and adhere to the NIST CSF framework. Additionally, these recommendations will allow Botium Toys to take major steps towards compliance with the PCI DSS, GDPR, SOC Type 1, and SOC Type 2.