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 :

Achieving PCI DSS compliance is critical to avoid reputational and financial risks, and it requires immediate action. Our organization currently lacks essential compliance measures, so we should first focus on identifying and classifying all assets based on sensitivity and data storage locations. This will ensure proper data tracking and enable us to determine how best to secure these assets.

Once asset details are in place, we can begin implementing preventive controls. Enforcing the principle of least privilege will restrict user access to only what's necessary, minimizing damage if a breach occurs.

Deterrent controls that will help us to restrain the attack when an unauthorized user has accessed our system.

Encryption :- Encrypting sensitive data, so unauthorized access does not mean compromised information.

Preventive controls includes:

Least Privilege :- Implementation of least privilege will ensure that people have access to only what's necessary for them to do their job which will also reduce the impact of damage in case the breach happens.

Password Policies :- Password policies need updating to meet current standards, which will reduce brute-force attack risks.

Access Control Policies :- Additionally, proper access control policies should be implemented to uphold confidentiality and integrity, limiting widespread access to confidential data.

Account management policies :- Strengthening account management policies will support the account lifecycle, reducing the attack surface, and preventing unauthorized access from former employees or default accounts.

Password management :- A password management system should also be deployed to facilitate secure password handling and recovery

Implementing these controls above could help us to get compliance with the PCI DSS as the payment data is very sensitive information and that needs to be protected at the first priority.

Furthermore,

Separation of duties :- Separation of duties will help reduce risks associated with compromised accounts.

Following separation of duties, least privileges and Encryption would help to ensure that data is private and secure which would allow us to comply with GDPR and SOC type1 and SOC type2.

Additionally we can improve the overall security and resilience of our organization by following some extra layers of controls.

Regular monitoring and maintenance of legacy systems should be scheduled monthly or quarterly. **Clear intervention methods** should be defined to address risks, vulnerabilities, and threats effectively. We should ensure **system backups** are available for quick recovery in the event of an incident, and a **disaster recovery plan** should be developed to support business continuity. Finally, an **Intrusion Detection System (IDS)** on all endpoints and networks will help detect and prevent malicious activity.