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.

Yes	No	
☑	☐	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. Least privilege and separation of duties - all employees currently have access to data including PII/SPII. This information should be restricted to only certain employees that need access to specific data. Employees should only have access to data relevant to their role at the organisation. **I would recommend restricting privileges in order to reduce the risk of malicious exploitation by internal threat actor or in the event that employee accounts have been breached.**

2. Disaster recovery - currently no plan in place. Should Botium Toys suffer an attack there is currently no plan to recover data. **Recommendation is to create a disaster recovery plan in the event of security breach.**

3. Passwords - password policy exists but do not adhere to current password complexity requirements that are stipulated. They need to be 8 characters long and a combination of letters and at least one number as well as one special character. More specifically, there is no password management system in place which would enforce the password complexity and ultimately avoid risk. **Set up a password management system to enforce employee compliance of password complexity rules.**

4. Intrusion detection system - no current IDS in place therefore Botium Toys has limited means of knowing if their system is compromised. **Recommendation is to install an intrusion detection system.**

5. Backups - none currently in place. **Recommendation is to implement a means of backing up critical data in the event of breach.**

6. Legacy systems - it is good that Botium toys monitor and maintain legacy systems but I **recommend they put together a regular schedule for this process as well as an intervention plan.**

7. Encryption - is not in place which compromises confidentiality of customers' credit information. **Recommendation is to implement encryption when storing customer data to preserve confidentiality and be compliant with GDPR.**