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.

INTERNAL SECURITY AUDIT

Scope: IT audit will cover user permissions, in use controls, systems, procedures, current compliance with relevant regulations and accounting for technology currently in use.

Goals: Establish systems and procedures to meet compliance with regulations, strengthen system controls, Develop and enforce polices, implement least privilege in necessary areas.

Botium Toys does not have the proper security controls in place and is not compliant with the U.S, and GDPR, Payment Card Industry Data Security Standard (PCI DSS), SOC Type 1 and SOC Type 2.

Recommendations:

Botium Toys needs to implement controls in order to address certain compliance, procedural and system gaps:

High Risk (Imediate Action Required)

1. Separation of duties and least privilege would reduce the risk of compromised accounts.
2. Password policies and management systems should be continuously updated to protect from brute force attacks.
3. A disaster recovery plan should be put in place that would ensure business continuity.

4. Intrusion Detection Systems (IDS)
5. Sensitive and confidential data could be at risk due to the lack of encryption within the company.
6. Botium Toys needs to classify their assets as Low, Medium, or High risk in order to create a better plan to protect sensitive information and PII/SPII and ensure customer and organizational data is handled properly to avoid further compliance issues.
7. In order for Botium to be compliant with the PCI DSS they should ensure only those who are authorized to handle customers credit card information are the only ones that have access. They also need to ensure that all CC information is stored, accepted, processed and transmitted internally.There is currently a plan in place to alert customers from the E.U. within 72 hours about any potential breach or if their data has been compromised. However there is no way for us to confidently say that E.U. customers data is secured because of the current state of our security management and lack of controls.
8. In order for Botium Toys to comply with SOC Type 1&2 we must ensure PII/SPII is kept confidential. Ensure that only those with authorization have access to certain data and keep a separation of duties so no one can have to much power/information and take advantage of the company and its customers.
9. Locks for cabinets with tech gear.

Medium/Low risk:

1. Fire Detection Systems to protect customers, employees, and assets.
2. Adequate lighting to deter physical attacks/ break ins
3. Security alarm service provider sign. This needs to be removed so threat actors don't have an advantage when trying to break in.

Currently I would give a risk score of 8 on a 1-10 scale which is considerably high. This is due to the lack of policies, procedures and proper account management. If nothing is done the company can expect a multitude of fines, and loss of trust from customers and other companies.

Once these controls are in place the organization's security posture will improve and enable the IT department to continue to find more areas to improve on data and account security. There will be a much lower risk of fines, stolen data, authorization, and privacy issues