

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	Explanation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Least Privilege	<i>Currently, all employees have access to customer data; privileges need to be limited to reduce the risk of a breach.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Disaster recovery plans	<i>There are no disaster recovery plans in place. These need to be implemented to ensure business continuity.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Password policies	<i>Employee password requirements are minimal, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Separation of duties	<i>Needs to be implemented to reduce the possibility of fraud/access to critical data, since the company CEO currently runs day-to-day operations and manages the payroll.</i>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Firewall	<i>The existing firewall blocks</i>

traffic based on an appropriately defined set of security rules.

<input type="checkbox"/>	<input checked="" type="checkbox"/>	Intrusion detection system (IDS)	<i>The IT department needs an IDS in place to help identify possible intrusions by threat actors.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Backups	<i>The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.</i>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Antivirus software	<i>Antivirus software is installed and monitored regularly by the IT department.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Manual monitoring, maintenance, and intervention for legacy systems	<i>The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is not a regular schedule in place for this task and procedures/policies related to intervention are unclear, which could place these systems at risk of a breach.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Encryption	<i>Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Password management system	<i>There is no password management system currently in place; implementing this control would improve IT department/other employee productivity in the case of password issues.</i>

<input checked="" type="checkbox"/>	<input type="checkbox"/>	Locks (offices, storefront, warehouse)	<i>The store's physical location, which includes the company's main offices, store front, and warehouse of products, has sufficient locks.</i>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Closed-circuit television (CCTV) surveillance	<i>CCTV is installed/functioning at the store's physical location.</i>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Fire detection/prevention (fire alarm, sprinkler system, etc.)	<i>Botium Toys' physical location has a functioning fire detection and prevention system.</i>

Compliance checklist

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 ?

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	Explanation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Only authorized users have access to customers' credit card information.	<i>Currently, all employees have access to the company's internal data.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	<i>Credit card information is not encrypted and all employees currently have access to internal data, including customers' credit card information.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Implement data encryption procedures to better secure credit card transaction	<i>The company does not currently use encryption to better ensure the confidentiality of customers'</i>

		touchpoints and data.	<i>financial information.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Adopt secure password management policies.	<i>Password policies are nominal and no password management system is currently in place.</i>

General Data Protection Regulation (GDPR)

Yes	No	Best practice	Explanation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	E.U. customers' data is kept private/secured.	<i>The company does not currently use encryption to better ensure the confidentiality of customers' financial information.</i>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	<i>There is a plan to notify E.U. customers within 72 hours of a data breach.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Ensure data is properly classified and inventoried.	<i>Current assets have been inventoried/listed, but not classified.</i>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Enforce privacy policies, procedures, and processes to properly document and maintain data.	<i>Privacy policies, procedures, and processes have been developed and enforced among IT team members and other employees, as needed.</i>

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice	Explanation
<input type="checkbox"/>	<input checked="" type="checkbox"/>	User access policies are established.	<i>Controls of Least Privilege and separation of duties are not currently in place; all</i>

			<i>employees have access to internally stored data.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sensitive data (PII/SPII) is confidential/private.	<i>Encryption is not currently used to better ensure the confidentiality of PII/SPII.</i>
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	<i>Data integrity is in place.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Data is available to individuals authorized to access it.	<i>While data is available to all employees, authorization needs to be limited to only the individuals who need access to it to do their jobs.</i>

Recommendations (optional): *Multiple controls need to be implemented to improve Botium Toys' security posture and better ensure the confidentiality of sensitive information, including:*

1- Least Privilege

Implement measures to reduce the risk and overall impact of malicious insider activities or compromised accounts. Restricting employee privileges to essential functions can mitigate potential security breaches..

2- Disaster recovery plans

Develop and establish comprehensive disaster recovery plans to ensure business continuity in the event of unforeseen incidents. These plans should outline steps for data recovery and system restoration..

3- Password policies do exist in the system but their requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters) and that will reduce likelihood of account compromise through brute force or dictionary attack techniques.

4-Separation of duties

Implement a robust separation of duties framework to reduce the risk and overall impact of malicious insider activities or compromised accounts. Clearly define and assign roles to different personnel to enhance accountability and security.

5- an IDS

Deploy an Intrusion Detection System (IDS) to effectively detect anomalous traffic that matches predefined signatures or rules. This system will aid in identifying and preventing unauthorized access attempts, enhancing overall system security.

6-Backups

Establish a comprehensive backup strategy to facilitate the swift restoration of data in the event of data loss or corruption. Regularly scheduled backups will ensure that data can be quickly recovered to its normal functioning state.

7-ongoing legacy system management

Implement a structured and continuous management plan for legacy systems. This includes regular monitoring, maintenance, and clear procedures and policies related to intervention. This proactive approach will minimize the risk of security breaches associated with legacy systems.

8- encryption

Introduce encryption measures to provide an additional layer of confidentiality to sensitive information. Implementing encryption protocols will safeguard data from unauthorized access, ensuring the protection of sensitive information.

9- a password management system

Integrate a robust password management system to alleviate password fatigue, which is a significant threat to operational systems. Such a system will enhance overall security by promoting secure password practices and reducing the likelihood of security incidents.

To address gaps in compliance, Botium Toys needs to implement controls such as Least Privilege, separation of duties, and encryption. The company also needs to properly classify assets, to identify additional controls that may need to be implemented to improve their security posture and better protect sensitive information.