

Controls and compliance checklist exemplar

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 traffic based on an appropriately defined set of</i>

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,	<i>The store's physical location,</i>

		warehouse)	<i>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

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 touchpoints and data.	<i>The company does not currently use encryption to better ensure the confidentiality of customers' financial information.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Adopt secure password management policies.	<i>Password policies are nominal and no password management</i>

system is currently in place.

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 employees have access to internally stored data.</i>
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sensitive data (PII/SPII) is	<i>Encryption is not currently</i>

	confidential/private.	<i>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):

To enhance Botium Toys' security posture and reduce risks to assets, I recommend the following actions to the IT manager:

- **Implement Least Privilege and Separation of Duties:** Restrict access to sensitive data, such as customers' credit card information and PII/SPII, to only authorized personnel. Enforce separation of duties to minimize the risk of insider threats or compromised accounts.
- **Enable Data Encryption:** Apply encryption to credit card information during acceptance, processing, transmission, and storage to ensure compliance with PCI DSS and protect data confidentiality.
- **Establish a Centralized Password Management System:** Deploy a password management system that enforces strong password policies (e.g., minimum 8 characters with letters, numbers, and special characters) to reduce password fatigue and enhance account security.
- **Develop Disaster Recovery Plans and Backups:** Create and test disaster recovery plans to ensure business continuity. Implement regular backups of critical data to prevent data loss.

- **Install an Intrusion Detection System (IDS):** Deploy an IDS to detect and prevent network threats, improving overall network security. These actions will help Botium Toys align with PCI DSS, GDPR, and SOC standards while mitigating high-priority risks