

Controls & Compliance Checklist Audit Report

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.

used to better ensure the confidentiality of PII/SPII.



Data integrity ensures the data is consistent, complete, accurate, and has been validated.

Data integrity is in place.



Data is available to individuals authorized to access it.

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.

Recommendations

Botium Toys must implement a range of security controls to strengthen its security posture and protect the confidentiality of sensitive information. These controls include least privilege access, disaster recovery plans, password policies, separation of duties, an intrusion detection system (IDS), ongoing management of legacy systems, encryption, and a password management solution. To address gaps in compliance, the company should prioritize controls like least privilege access, separation of duties, and encryption. Proper classification of assets is also essential to identifying further controls that can bolster security and ensure data protection. By implementing these measures, Botium Toys can safeguard its critical assets and meet its security objectives.

The recent audit identified key areas where Botium Toys needs to act immediately to align with compliance standards such as GDPR, PCI DSS, SOC 1, and SOC 2, while also strengthening its overall security framework. Central to this is identifying and categorizing current assets and adopting essential security controls, many of which can be guided by the NIST Cybersecurity Framework (CSF). As the company expands, disaster recovery plans and business continuity measures will become even more vital. The full controls assessment and compliance checklist provide detailed action items to improve security posture. Additionally, adopting the NIST Risk Management Framework early on can significantly aid in meeting long-term security goals as Botium Toys grows.