Controls and compliance checklist

Related information can be found 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.

Select “yes” or “no” to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control	*Explanation*
☐	☑	Least Privilege	*All employees currently have access to customer data; PoLP must be followed to reduce the risk of a breach.*
☐	☑	Disaster recovery plans	*No disaster recovery plans are in place. These need to be implemented, beginning with backups of critical information, to ensure business continuity.*
☐	☑	Password policies	*Employee password requirements are inadequate, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network. These requirements must be updated to meet the current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at*

			— least one number; special characters).
☐	☑	Separation of duties	*This control must be implemented to reduce the risk to critical data (fraud/unauthorized access), since the company CEO currently manages daily operations and the payroll.*
☑	☐	Firewall	*The existing firewall blocks traffic based on an appropriately defined set of security rules, however, a secure default is also recommended.*
☐	☑	Intrusion detection system (IDS)	*The IT department must install an IDS to identify possible intrusions by threat actors.*
☐	☑	Backups	*Backups of critical information must be made by the IT department, to ensure business continuity in the event of a breach.*
☑	☐	Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems	*The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is currently no regular schedule for this task and procedures/policies related to intervention are undefined. A schedule for related tasks and*

			— defined intervention plans must be implemented to reduce the risk of a breach to systems.
☐	☑	Encryption	*Encryption is not currently used; implementing this is a necessity as it provides greater confidentiality of sensitive information and adheres to compliance best practice.*
☐	☑	Password management system	*There is currently no password management system in place; implementing this control would improve IT department/other employee productivity in the event of password issues.*
☑	☐	Locks (offices, storefront, warehouse)	*The store's physical location, which includes the company's main offices, store front, and warehouse of products, has sufficient locks.*
☑	☐	Closed-circuit television (CCTV) surveillance	*CCTV is up-to-date and installed/functioning at the store's physical location.*
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical location has functioning fire detection and prevention systems.*

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*
☐	☑	Only authorized users have access to customers’ credit card information.	*All employees currently have access to customers’ SPII and internally stored company data; PoLP must be implemented to mitigate risk.*
☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information is not encrypted, and all employees currently have access to internal data, including customers’ credit card information; encryption must be implemented to mitigate risk.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*Botium Toys does not currently use encryption; encryption must be implemented to mitigate risk and to ensure the confidentiality of customers’ financial information.*
☐	☑	Adopt secure password management policies.	*Password policies are nominal, and no password management system is currently in place; current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters) should be met, and a password management system implemented to improve productivity.*

General Data Protection Regulation (GDPR)

Yes	No	Best practice	*Explanation*
☐	☑	E.U. customers' data is kept private/secured.	*Botium Toys does not currently use encryption; encryption must be implemented to mitigate risk and to ensure the confidentiality of customers' financial information.*
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*There is a plan to notify E.U. customers within 72 hours of a data breach.*
☐	☑	Ensure data is properly classified and inventoried.	*Current assets have been inventoried/listed, but not yet classified.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed and enforced among IT team members and other employees to properly document and maintain data.*

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

Yes	No	Best practice	*Explanation*
☐	☑	User access policies are established.	*Least Privilege and separation of duties are not in place; all employees currently have access to internally stored data.*
☐	☑	Sensitive data (PII/SPII) is confidential/private.	*Botium Toys does not currently use encryption; encryption must be —*

			implemented to mitigate risk and to ensure the confidentiality of PII/SPII.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity is in place through integrated controls.*
☐	☑	Data is available to individuals authorized to access it.	*While data is available to employees authorized to access it, all employees currently possess authorization, therefore authorization must be limited by PoLP and specific access only provided where an individual requires it to complete their jobs.*

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.

Several controls must be implemented to improve Botium Toys' security posture and ensure the confidentiality of sensitive information, including: JEA & JIT, disaster recovery plans (including but not limited to back-ups of critical information), a password management system, adequate password policies, separation of duties, an IDS, legacy systems; regular scheduling, defined intervention methods, and ongoing management, and encryption of PII/SPII. A time-controlled safe, adequate lighting, and signage indicating alarm service provider, could also be implemented as physical controls to deter threat actors.

For Botium Toys to address the gaps in compliance, Botium Toys must classify its assets to identify additional controls that require implementation to improve their security posture, adequately protect PII/SPII, and begin by implement controls including: JEA & JIT, separation of duties, and encryption.