Controls and compliance checklist

Please refer to the information provided in the scope, goals, and risk assessment report for the effective review of the controls and compliance checklist. For more details about each control, including the type and purpose, refer to the control categories document.

Does Botium Toys currently have these controls in place?

Controls assessment checklist

Yes	No	Control	Explanation
	X	Least Privilege	*Currently, all employees have access to both SPII and PII; limits to access must be implemented to reduce risks of data breaches.*
	X	Disaster recovery plans	*In the case of errors or malfunctions, this is essential in order for seamless business continuity and no interruption in services.*
X		Password policies	*The current policy is rather weak and needs to be iterated upon for the creation of stronger passwords along with enforcing it. This is necessary in order to prevent aiding unauthorized access.*
	X	Separation of duties	*Essential in order to separate core duties, and avoid the tampering and manipulation of data.*

X		Firewall	*The firewall in current deployment is sufficient for blocking unwanted traffic which uses an appropriately defined set of security rules.*
	X	Intrusion detection system (IDS)	*The absence of an IDS poses significant risks to the integrity, confidentiality and availability of both physical and digital company assets.*
	X	Backups	*In the case of data loss or breach, this is essential in order to retrieve both user data and company data for business continuity.*
X		Antivirus software	*Has been implemented and monitored regularly by the IT department.*
	X	Manual monitoring, maintenance, and intervention for legacy systems	*Although legacy systems are monitored and maintained, a regular schedule and clear implementation methods are needed to be in effect to address this concern, avoid data loss and ensure business continuity.*
	X	Encryption	*No encryption of data risks both PII and SPII to be leaked and modified accordingly by threat actors. Confidentiality and integrity is compromised as a result.*
	X	Password management system	*A password management system is needed to avoid password fatigue, and*

		maintain authorized, reliable and safe access to confidential data.
X	Locks (offices, storefront, warehouse)	*Botium Toys’ physical locations have sufficient locks in place to secure physical assets.*
X	Closed-circuit television (CCTV) surveillance	*CCTV surveillance has been set up which allows checking previous incidents in the workspace and the continuous monitoring of any physical or digital threat to company assets.*
X	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Correctly set up; Prevents the damage and loss of physical and digital assets that are present in the physical workspace.*

Does Botium Toys currently adhere to these compliances’ best practices?

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	Explanation
	X	Only authorized users have access to customers’ credit card information.	*All employees have access to all private company data at the current moment.*
	X	Credit card information is stored, accepted,	*All data is currently*

		processed, and transmitted internally, in a secure environment.	*stored unencrypted and is always accessible by all employees of the company.*
	X	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	T*his is non-negotiable in order to adhere to the PCI DSS and to the European GDPR.*
	X	Adopt secure password management policies.	*Both secure password management and the creation and enforcing creation of secure passwords is necessary to keep the access and integrity of data.*

General Data Protection Regulation (GDPR)

Yes	**No**	**Best practice**	**Explanation**
	X	E.U. customers' data is kept private/secured.	*All users' data, including the ones in the EU, is accessible to all the employees in an unencrypted manner, making it both non-private and non-secure.*
X		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*Plan is in effect to notify E.U. customers within 72 hours if their data is compromised.*
	X	Ensure data is properly classified and inventoried.	*Data is not classified but is inventoried locally.*
X		Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed and are enforced amongst all employees; data is properly documented and maintained.*

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

Yes	No	Best practice	Explanation
	X	User access policies are established.	*There is no clear authorization method, nor clear ruling as to who is allowed to access which data. Separation of duties is another thing that needs to be addressed.*
	X	Sensitive data (PII/SPII) is confidential/private.	*All employees have access to all private company data at the current moment.*
X		Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*The integrity of the data is solid, but the controls to keep it integral are missing.*
	X	Data is available to individuals authorized to access it.	*Data is available for all employees to access, but it is a must to only give access to a select few for keeping the internal company data's integrity.*

Recommendations:

In order to avoid legal consequences, improve the security posture and significant financial losses, Boltium Toys must implement the following controls in place:

- Encryption of all data must be put into effect as soon as possible in order to deter the easy access and manipulation of data by threat actors, and to comply with the GDPR, SOC (Types 1 and 2) and PCI DSS.
- Least Privilege: Allowing the minimal set of permissions and authority that only selected entities can fully exercise on internal company data.
- Separation of Duties: Employees in the IT Department must be tasked with only specific tasks. For example: someone who is in charge of handling product

purchases should not be tasked with the handling of SPII of customers in order to minimize data tampering and keeping data confidential within the company.

- Replace legacy systems with modern, more secure ones as soon as possible and establish a consistent routine for the maintenance and an outline of clear implementation methods of current systems.
- For the physical offices, the installation of an Intrusion Detection System (IDS) is essential for the safety of both physical and digital assets of the company.
- Recurring backups of current and future internal company data must be made in the event that data is lost or corrupted due to malfunctions or other reasons, alongside creating a disaster recovery plan to ensure business continuity.