Controls and compliance checklist

Does Botium Toys currently have this control in place?

Controls assessment checklist

Yes	**No**	**Control**	***Explanation***
☐	☑	Least Privilege	*At the moment, all of the employees have access to all of the customers' information, including sensitive information.*
☐	☑	Disaster recovery plans	*The IT department has established disaster recovery plans at this moment.*
☐	☑	Password policies	*Despite there being password policies in place, they do not meet the minimal required complexity requirements.*
☐	☐	Separation of duties	*There has been no implementation regarding the separation of duties at the current moment.*
☑	☐	Firewall	*There is a firewall in place which is based on appropriately defined security protocols.*
☐	☑	Intrusion detection system (IDS)	*The IT department has not installed any IDS systems.*
☐	☑	Backups	*There are no backups for critical data on record.*

☑	□	Antivirus software	*They have installed an antivirus and is regularly monitored by the IT department.*
□	☑	Manual monitoring, maintenance, and intervention for legacy systems	*Not clear intervention plan in place. No set regular schedule for monitoring and maintaining the systems.*
□	☑	Encryption	*There is no encryption in use at the moment, leaving essential customer information vulnerable.*
□	☑	Password management system	*No system in place that enforces the password policy requirements.*
☑	□	Locks (offices, storefront, warehouse)	*There are locks in place at the physical location.*
☑	□	Closed-circuit television (CCTV) surveillance	*There is an up to date CCTV system in place.*
☑	□	Fire detection/prevention (fire alarm, sprinkler system, etc.)	*There is a functioning fire detection system in place.*

Compliance checklist

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.	*With no least privilege policy/system in place, all employees have access to the information.*

☐	☑	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*The credit card information is not encrypted and all employees have access to the information, making it not securely stored.*
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*No encryption procedures in use at the moment for credit card transactions.*
☐	☑	Adopt secure password management policies.	*No central password management system has been put in place.*

General Data Protection Regulation (GDPR)

Yes	**No**	**Best practice**	***Explanation***
☐	☑	E.U. customers' data is kept private/secured.	*There is no encryption systems in use to ensure the information is secured.*
☑	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach.*
☐	☑	Ensure data is properly classified and inventoried.	*Current inventory has not been classified.*
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed and are enforced, 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.	*Currently all employees have access to internally stored data.*
□	☑	Sensitive data (PII/SPII) is confidential/private.	*Currently no encryption is in place to ensure confidentiality.*
☑	□	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.	*Least privilege is not in place. All employees have access to internal data.*

Recommendations :

To strengthen Botium Toys' security posture and keep sensitive information safe, several key controls need to be put in place. These include applying Least Privilege, setting up disaster recovery plans, enforcing strong password policies, ensuring separation of duties, using an intrusion detection system (IDS), managing legacy systems, applying encryption, and introducing a password management tool.

When it comes to compliance gaps, Botium Toys should focus on controls like Least Privilege, encryption, and separation of duties. It's also important to properly classify their assets—this helps identify where additional security measures are needed to better protect important data.