Controls and compliance checklist

To complete the controls assessment checklist, refer to the information provided 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.

Then, 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 have access to customer data, therefore privileges need to be limited.
☐	☑	Disaster recovery plans	There is no disaster recovery plans in place which is needed for business continuity.
☐	☑	Password policies	Employee password was minimal which could allow easy access to information.
☐	☑	Separation of duties	No form of separation of duties which is ideal so as to reduce critical access to data.
☑	☐	Firewall	The IT department had a firewall to block traffic based on a defined set of security rules.
☐	☑	Intrusion detection system (IDS)	No IDS which is necessary so as to alert them in any intrusion.
☐	☑	Backups	There was no form of backup

			available which is bad. Assuming a breach occurs, back up is necessary to store data for business continuity.
☑	☑	Antivirus software	IT department regularly monitored the antivirus software
☐	☐	Manual monitoring, maintenance intervention for legacy systems.	Legacy systems were monitored but no schedule for procedures.
☐	☑	Encryption	Encryption wasn't used as to which is a necessity to ensure confidentiality of data.
☐	☑	Password management system	There was no centralized password management system that enforces policy minimum requirement
☑	☐	Locks (offices, storefront, warehouse)	There was sufficient locks in the physical location of the office.
☑	☐	Closed-circuit television (CCTV) surveillance.	Present to monitor the location.
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.).	Present in case of any fire disaster.

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	
☐	☑	Only authorized users have access to customers' credit card information.	Employees have access to all data.

☐	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.	It is not encrypted and stored stored locally in company's database.
☐	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	Company has no form of encryption.
☐	☑	Adopt secure password management policies.	Password policies are nominal and no password management.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	
☐	☑	E.U. customers' data private/secured.	The company does not ensure is kept confidentiality of data.
☑	☐	There is a plan in place to notify E.U. customers within, 72 hours if their data is compromised/there is a breach.	There was a plan to notify customers within 72 hours.
☐	☑	Ensure data is properly categorized.	Current assets have been listed not classified and inventoried
☑	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.	Privacy policies and procedures were enforced by the IT department team.

Recommendations : From the checklist various controls need to be implemented to improve Botium Toys' security posture and ensure the confidentiality of sensitive information, including: Least Privilege,disaster recovery plans, password policies, separation of duties, an IDS, ongoing legacy system management, and a password

management system. To improve compliance, Botium Toys should incorporate controls like separation of duties, and encryption. To strengthen security, the organization should appropriately classify assets and apply necessary procedures to secure critical information.