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 all customer data. Limitations need to be set.
☐	☒	**Disaster recovery plans**	There needs to be a disaster recovery plan set in place because there is not one.
☐	☒	**Password policies**	There needs to be a stronger password policy to include special characters, numbers, capitalization, more characters, and resets every 180 days
☐	☒	**Separation of duties**	Since all employees have access to all data, separation of duties needs to be implemented to protect critical data.
☒	☐	**Firewall**	The firewall successfully blocks appropriate traffic with the current security rules set in place.
☐	☒	**Intrusion detection system (IDS)**	There is no IDS set in place, there needs to be one implemented.

□	☒	**Backups**	Critical data needs to be backed up in case of a security breach.
☒	□	**Anti-virus software**	Anti-virus software is installed and monitored regularly by the IT department.
□	☒	**Manual monitoring, maintenance, and intervention for legacy systems**	A schedule needs to be in place for the legacy systems to be regularly be monitored and maintained
□	☒	**Encryption**	There is no encryption. Having encryption will provide confidentiality.
□	☒	**Password management system**	There is no password manager in place. This will help IT with password issues if implemented.
☒	□	**Locks (offices, storefront, warehouse)**	The store has functioning locks implemented at all locations.
☒	□	**Closed-circuit television (CCTV) surveillance**	The store has a functioning CCTV implemented at all locations.
☒	□	**Fire detection/prevention (fire alarm, sprinkler system, etc.)**	The store has a functioning fire detection and prevention system implemented at all locations.

To complete the compliance checklist, refer to the information provided in the scope, goals, and risk assessment report. For more details about each compliance regulation, review the controls, frameworks, and compliance reading.

Then, select “yes” or “no” to answer the question: *Does Botium Toys currently adhere to this compliance best practice?*

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
☐	☒	Only authorized users have access to customers’ credit card information.
☐	☒	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
☐	☒	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
☐	☒	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
☐	☒	E.U. customers’ data is kept private/secured.
☒	☐	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☐	☒	Ensure data is properly classified and inventoried.
☒	☐	Enforce privacy policies, procedures, and processes to properly document and maintain data.

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

Yes	No	Best practice
☐	☒	User access policies are established.
☐	☒	Sensitive data (PII/SPII) is confidential/private.
☒	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☐	☒	Data is available to individuals authorized to access it.

This section is *optional* and can be used to provide a summary of recommendations to the IT manager regarding which controls and/or compliance best practices Botium Toys needs to implement, based on the risk posed if not implemented in a timely manner.

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.

Least Privilege, separation of duties, encryption, and a stronger password policy needs to be implemented to better protect PII and SPII information.