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
☐	☑	Least Privilege
☐	☑	Disaster recovery plans
☐	☑	Password policies(not in line with current minimum password complexity requirements)
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	Antivirus software
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems
☐	☑	Encryption
☐	☑	Password management system
☑	☐	Locks (offices, storefront, warehouse)

☑	☐	Closed-circuit television (CCTV) surveillance
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)

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.

Yes	No	
☐	☑	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.

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.

These are the preventative controls you need to have in place to make sure you are compliant, mitigating risk and handling vulnerabilities. For your preventative controls, you're in need of Least privilege, Separation of Duties, Manual monitoring maintenance and intervention and password management. These are needed to ensure the reduction of risk and overall impact of malicious insider or compromised accounts, reduce password fatigue and to identify and manage threats, risks, or vulnerabilities to out-of-date systems. For your corrective controls you're in need of a Disaster recovery plan and Backups. These are needed to provide business continuity and restore/recover in case of an event/breach. Lastly, you're in need of a detective control,

which will be an IDS which will help to detect anomalous traffic. As of right now you are not compliant with Payment Card Industry Data Security Standards, for the General Data Protection regulation their data is not properly classified or inventoried. Also your Systems and Organization Controls are not following best practices like protecting sensitive data. This is a great place to start and once we start to implement the proper controls, we can raise the security posture of Botium Toys.