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
☐	☑	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.
☐	☑	Ensure data is properly classified and inventoried.

Yes	No	
☑	☐	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.

By implementing the list I have made below, controls, and compliance measures within Botium Toys will significantly reduce security risks, enhance data protection, and improve overall cybersecurity resilience.

- Enforce least privilege and separation of duties to ensure employees can only access the data necessary for their roles.
- Implement role-based access control (RBAC) to limit unauthorized access to sensitive data.

- Implement encryption for customers' credit card data at rest and in transit to protect sensitive information.
- Ensure PCI DSS compliance to safeguard cardholder data.
- Restrict employee access to personally identifiable information (PII) and sensitive personal identifiable information (SPII).
- Install an IDS to monitor and detect suspicious activities or security breaches in real time.
- Regularly update firewall rules and integrate IDS alerts with security monitoring tools.
- Implement regular data backups and test restoration processes.
- Develop a disaster recovery plan (RDP) to ensure business continuity in case of cyber incidents or system failures.
- Enforce a strong password policy (e.g., minimum 12-character length, complexity requirements, periodic changes).
- Implement multi-factor authentication (MFA) to enhance login security.
- Deploy a centralized password management system to reduce security gaps and minimize IT department workload related to password resets.
- Conduct a compliance gap assessment to ensure alignment with U.S. and international regulations (GDPR, PCI DSS).
- Ensure privacy policies are enforced company-wide, not just within IT.
- Maintain records of compliance measures and regularly update them as regulations evolve.
- Create a scheduled maintenance plan for legacy systems to ensure they remain functional and secure.
- Evaluate options for phasing out or upgrading outdated systems that pose security risks.
- Conduct mandatory cybersecurity training for all employees to promote awareness of phishing, social engineering, and secure data handling.
- Provide periodic security refreshers and simulated attack exercises.