Ryan Chevarria

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, type an X in the "yes" or "no" column to answer the question: *Does Botium Toys currently have this control in place?*

Controls assessment checklist

Yes	No	Control
	X	Least Privilege
	X	Disaster recovery plans
	X	Password policies
	X	Separation of duties
X		Firewall
	X	Intrusion detection system (IDS)
	X	Backups
X		Antivirus software
	X	Manual monitoring, maintenance, and intervention for legacy systems
	X	Encryption
	X	Password management system
X		Locks (offices, storefront, warehouse)
X		Closed-circuit television (CCTV) surveillance
X		Fire detection/prevention (fire alarm, sprinkler system, etc.)

Ryan Chevarria

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, type an X in the "yes" or "no" column 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
	X	Only authorized users have access to customers' credit card information.
	X	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
	X	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
	X	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

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

Ryan Chevarria

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

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

1. **Asset Identification and Classification:** Dedicate resources to identify and classify all assets, including on-premises equipment, employee devices, storefront products, management systems, and legacy systems. Assess the impact of potential asset loss on business continuity.
2. **Access Controls and Encryption:** Implement access controls such as least privilege and separation of duties. Utilize encryption to ensure the confidentiality of sensitive data, especially credit card information stored in the internal database.
3. **Intrusion Detection System (IDS):** Install and maintain an intrusion detection system (IDS) to monitor and detect unauthorized access or activities within the network.

4. **Disaster Recovery and Data Backups:** Develop and implement disaster recovery plans, including regular backups of critical data. This ensures data availability and minimizes the risk of data loss in the event of a security incident.
5. **Password Policy Enforcement:** Strengthen the password policy to meet current minimum complexity requirements. Implement a centralized password management system to enforce and streamline password policies, improving overall security.
6. **EU Customer Notification and Privacy Compliance:** Maintain the plan to notify EU customers within 72 hours of a security breach. Ensure ongoing enforcement of privacy policies, procedures, and processes to protect and document sensitive data.
7. **Legacy System Maintenance:** Establish a regular schedule for monitoring and maintaining legacy systems. Clearly define intervention methods to address issues promptly.
8. **Risk Awareness and Training:** Provide training and awareness programs for employees to enhance understanding of security risks, controls, and compliance requirements. This will contribute to a more secure organizational culture.
9. **Regular Security Audits:** Conduct regular security audits to identify and address potential vulnerabilities and non-compliance issues. This ensures continuous improvement of Botium Toys' security posture.