Controls and compliance checklist

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.)

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.

Recommendations :

With these recommendations, we can ensure the privacy and security of the clients confidential information. There are some concerns that should be addressed immediately witch can seriously impact the financial reputational standing of the company.

Implement strong encryption for credit card data.

Establish and enforce robust password policies and implement MFA.

Define and implement access controls based on the principle of least privilege. (This will require the IT department to work hand in hand with authorized managers to rank employees' levels of access based on nessesity)

There are also some short-term goals and long-term strategies we can implement to hit the nail on the head and solidify our PII needs. Some things we can consider moving forward are:

Classify and inventory data to comply with GDPR (General Data Protection Regulation) requirements.

*I have included a link to some resources on best and most current requirements this will help you build a better understanding of E.U. privacy law.

https://docs.google.com/document/d/12IAOkBzdYupKFsrEAn7--hmDGt11c0fUTIghoFeHdtU/edit?usp=drive_link

Develop and document privacy policies, procedures, and processes.

Implement technical solutions to ensure data integrity (e.g., checksums, backups).

Finally, let's implement a few long-term strategies that will fortify our mission.

Regularly review and update security policies and procedures.

Conduct ongoing vulnerability scans and penetration testing.

Consider pursuing SOC 2 compliance to demonstrate a commitment to security and data protection.

Invest in employee training and awareness programs to foster a culture of security.

By addressing these areas, Botium Toys can significantly enhance its cybersecurity posture and protect both its business and its customers. Let me know if you'd like any further clarification or guidance on specific steps!

Junaid Shakoor

Shakoor.Junaidre@gmail.com

717-644-6870