

Checklist dei controlli e della conformità

Controls assessment checklist

Yes	No	Control
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Least Privilege (Privilegio minimo)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Piani di disaster recovery
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Policy sulle password
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Separazione dei compiti
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Firewall
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Intrusion detection system (IDS)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Backups
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Antivirus software
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Monitoraggio, manutenzione e intervento manuale per sistemi legacy
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Crittografia
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sistema di gestione delle password
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Serrature (uffici, negozio, magazzino)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Videosorveglianza CCTV (Closed-Circuit Television)
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Rilevazione/prevenzione incendi (allarme, sprinkler, ecc.)

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes No Best practice

- Solo utenti autorizzati hanno accesso alle informazioni delle carte di credito dei clienti.
- Le informazioni delle carte di credito sono archiviate, accettate, elaborate e trasmesse internamente in un ambiente sicuro.
- Implementare procedure di crittografia per proteggere meglio i punti di contatto e i dati delle transazioni con carta.
- Adottare politiche di gestione sicura delle password.

General Data Protection Regulation (GDPR)

Yes No Best practice

- I dati dei clienti UE sono mantenuti privati e sicuri.
- È presente un piano per notificare ai clienti UE entro 72 ore se i loro dati sono compromessi o c'è una violazione.
- Assicurare che i dati siano correttamente classificati e inventariati.
- Applicare politiche, procedure e processi sulla privacy per documentare e mantenere correttamente i dati

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

Yes No Best practice

- Sono stabilite le politiche di accesso degli utenti.
- I dati sensibili (PII/SPII) sono riservati/privati.

- L'integrità dei dati assicura che i dati siano coerenti, completi, accurati e convalidati.
 - I dati sono disponibili per gli individui autorizzati ad accedervi
-

Raccomandazioni: Dalla valutazione dei sistemi e delle risorse di Botium Toys emergono diverse aree critiche da migliorare. Si raccomanda di applicare il principio del privilegio minimo, limitando l'accesso ai dati sensibili solo al personale autorizzato, e di implementare piani di disaster recovery e backup regolari per garantire la continuità operativa.

È importante rafforzare la separazione dei compiti e aggiornare le policy sulle password, introducendo un sistema centralizzato per ridurre i reset e aumentare la sicurezza. Dal punto di vista tecnico, va installato un sistema di rilevamento delle intrusioni (IDS) e applicata la crittografia dei dati sensibili, mentre i sistemi legacy devono essere monitorati e mantenuti regolarmente.

Infine, Botium Toys deve rispettare le normative PCI DSS e GDPR, proteggendo i dati dei clienti e predisponendo procedure chiare per eventuali violazioni, oltre a garantire integrità e disponibilità dei dati secondo gli standard SOC 1/2.