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.)

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.
●		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: 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.

Recomendações prioritárias:

Controle de acesso: Dadas as informações a falha mais perigosa(combinada com a política de senhas fracas) é a falta de controle de acessos e permissões primordiais aos respectivos colaboradores. Deve ser o princípio de menor privilégio, juntamente com a separação de função para cada colaborador.

Política de senhas fortes: Deve ser reajustado também a política de senha existente, para que a mesma atenda as normas de segurança como, número mínimo de 8 caracteres, utilização de maiúsculas e minúsculas, utilização de números e caracteres especiais, histórico salvas e permitidas a serem reutilizadas, e número de dias de vencimento de senhas(e mais recomendações personalizadas, como não ser possível utilizar o nome da empresa, ano atual, etc).

Disponibilidades das informações (Backups de dados): A ausência total de backups é um risco existente, pois qualquer falha seja ela por acidente ou incidente, pode levar a sérios prejuízos dentro da empresa. Deve ser implementada a prática de Backups frequentes, seguindo o padrão 3-2-1.

Proteção de dados de clientes (LGPD): Deve ser implementada a criptografia nas informações confidenciais dos clientes, para que em caso de ataque, informações importantes como senhas, números de cartões de créditos, CVV's, não sejam vazados e utilizados por atacantes ou pessoas más intencionadas.