

# Liste de contrôle des contrôles et de la conformité

Pour compléter la liste de contrôle d'évaluation des contrôles, reportez-vous aux informations fournies dans le [portée, objectifs et rapport d'évaluation des risques](#). Pour plus de détails sur chaque contrôle, y compris le type et l'objectif, reportez-vous au [catégories de contrôle](#) document.

Ensuite, sélectionnez « oui » ou « non » pour répondre à la question : *Botium Toys a-t-il actuellement mis en place ce contrôle ?*

## Liste de contrôle pour l'évaluation des contrôles

Oui	Non	Contrôle
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Moindre privilège
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Plans de reprise après sinistre
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Politiques de mot de passe
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Séparation des tâches
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Pare-feu
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Système de détection d'intrusion (IDS)
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Sauvegardes
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Logiciel antivirus
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Surveillance, maintenance et intervention manuelles pour les systèmes existants
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Cryptage
<input type="checkbox"/>	<input checked="" type="checkbox"/>	Système de gestion de mots de passe
<input checked="" type="checkbox"/>	<input type="checkbox"/>	Serrures (bureaux, vitrines, entrepôts)

- Surveillance par télévision en circuit fermé (CCTV)
- Détection/prévention incendie (alarme incendie, système de gicleurs, etc.)
- 

Pour compléter la liste de contrôle de conformité, reportez-vous aux informations fournies dans le [portée, objectifs et rapport d'évaluation des risques](#). Pour plus de détails sur chaque réglementation de conformité, consultez le [contrôles, cadres et conformité](#) en lisant.

Ensuite, sélectionnez « oui » ou « non » pour répondre à la question : *Botium Toys adhère-t-il actuellement à cette bonne pratique de conformité ?*

### Liste de contrôle de conformité

#### Norme de sécurité des données du secteur des cartes de paiement (PCI DSS)

Oui	Non	Meilleure pratique
-----	-----	--------------------

- |                          |                                     |  |
|--------------------------|-------------------------------------|--|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Seuls les utilisateurs autorisés ont accès aux informations de carte de crédit des clients.  |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Les informations de carte de crédit sont stockées, acceptées, traitées et transmises en interne, dans un environnement sécurisé.                       |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Mettez en œuvre des procédures de cryptage des données pour mieux sécuriser les points de contact et les données des transactions par carte de crédit. |
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | Adoptez des politiques de gestion des mots de passe sécurisées.  |

#### Règlement Général sur la Protection des Données (RGPD)

Oui	Non	Meilleure pratique
-----	-----	--------------------

- |                          |                                     |   |
|--------------------------|-------------------------------------|---|
| <input type="checkbox"/> | <input checked="" type="checkbox"/> | UE. les données des clients restent privées/sécurisées. |
|--------------------------|-------------------------------------|---|

- Il existe un plan en place pour informer l'UE. clients dans les 72 heures si leurs données sont compromises/en cas de violation.
- Veiller à ce que les données soient correctement classées et inventoriées.
- Appliquez les politiques, procédures et processus de confidentialité pour documenter et conserver correctement les données.

#### Contrôles du système et des organisations (SOC type 1, SOC type 2)

**Oui    Non    Meilleure pratique**

- |                                     |                                     |   |
|-------------------------------------|-------------------------------------|---|
| <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Des politiques d'accès des utilisateurs sont établies.  |
| <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Les données sensibles (PII/SPII) sont confidentielles/privées.  |
| <input checked="" type="checkbox"/> | <input type="checkbox"/>            | L'intégrité des données garantit que les données sont cohérentes, complètes, exactes et ont été validées. |
| <input type="checkbox"/>            | <input checked="" type="checkbox"/> | Les données sont accessibles aux personnes autorisées à y accéder.  |
- 

Cette rubrique est *facultatif* et peut être utilisé pour fournir un résumé des recommandations au responsable informatique concernant les contrôles et/ou les meilleures pratiques de conformité que Botium Toys doit mettre en œuvre, en fonction du risque posé s'il n'est pas mis en œuvre en temps opportun.

**Recommandations (facultatif) :** Dans cette section, fournissez des recommandations, liées aux contrôles et/ou aux besoins de conformité, que votre responsable informatique pourrait communiquer aux parties prenantes afin de réduire les risques pour les actifs et d'améliorer la posture de sécurité de Botium Toys.

### **Mes Recommandations:**

Beaucoup de politiques doivent être mises en œuvre comme celle du moindre privilège , une politique de mot passe fort, séparations des tâches, sauvegarde et reprise après sinistre. Mais un surveillance des systèmes existants, le cryptage des données, IDS sont aussi des meures qui aident BOTIUM TOYS à faire évoluer sa posture de sécurité.