**Table des matières**

[Audit de Cybersécurité pour Botium Toys 2](#__RefHeading___Toc2171_2067123913)

[Résumé, portée et objectifs de l’audit 2](#__RefHeading___Toc2201_2067123913)

[Portée 2](#__RefHeading___Toc2193_2067123913)

[Objectif 2](#__RefHeading___Toc2191_2067123913)

[Évaluation des risques 3](#__RefHeading___Toc2207_2067123913)

[Ressources numériques actuelles 3](#__RefHeading___Toc2185_2067123913)

[Description des risques 3](#__RefHeading___Toc2199_2067123913)

[Les bonnes pratiques en matière de contrôle 3](#__RefHeading___Toc2189_2067123913)

[Scores de risque 4](#__RefHeading___Toc2187_2067123913)

[Commentaires supplémentaires 4](#__RefHeading___Toc2197_2067123913)

[Évaluation des contrôles 4](#__RefHeading___Toc2205_2067123913)

[Ressources numériques actuelles 4](#__RefHeading___Toc2195_2067123913)

[Liste de contrôle de conformité 7](#__RefHeading___Toc2203_2067123913)

[\_\_\_\_\_ La Federal Energy Regulatory Commission - North American Electric 7](#__RefHeading___Toc2173_2067123913)

[Reliability Corporation (FERC-NERC) 7](#__RefHeading___Toc2183_2067123913)

[\_\_X\_\_ Règlement général sur la protection des données (RGPD) 8](#__RefHeading___Toc2181_2067123913)

[\_\_X\_\_ Norme de sécurité de l'industrie des cartes de paiement (PCI DSS) 8](#__RefHeading___Toc2179_2067123913)

[\_\_\_\_\_ Le Health Insurance Portability and Accountability Act (HIPAA) 8](#__RefHeading___Toc2177_2067123913)

[\_\_X\_\_ Contrôles des systèmes et des entreprises (System and Organization Controls, SOC type 1, SOC type 2) 8](#__RefHeading___Toc2175_2067123913)

****Audit de Cybersécurité pour Botium Toys****

# **Résumé, portée et objectifs de l’audit**

****Résumé****  
Botium Toys connaît une croissance remarquable sur le marché en ligne, exposant ses systèmes à de nouveaux risques. Cet audit interne a été réalisé pour évaluer la posture de cybersécurité de l’entreprise, identifier les vulnérabilités et vérifier la conformité aux exigences réglementaires (PCI DSS, RGPD, etc.).

L’évaluation révèle plusieurs faiblesses, notamment l’absence de plan de continuité d’activité, un contrôle d’accès insuffisant, et des procédures de conformité incomplètes. Des recommandations immédiates ont été formulées.

## **Portée**

**L’audit informatique interne de Botium Toys évaluera les éléments suivants :**

* **Autorisations actuelles des utilisateurs dans les systèmes suivants : comptabilité, détection des endpoints, pare-feu, système de détection d'intrusion, outils de gestion des informations et des événements de sécurité (SIEM)**
* **Contrôles actuellement mis en œuvre dans les systèmes suivants : comptabilité, détection des endpoints, pare-feu, système de détection d'intrusion, outils de gestion des informations et des événements de sécurité (SIEM)**
* **Procédures et protocoles en vigueur pour les systèmes suivants : comptabilité, détection des endpoints, pare-feu, système de détection d'intrusion, outils de gestion des informations et des événements de sécurité (SIEM)**
* **Veiller à ce que les autorisations, contrôles, procédures et protocoles en place pour les utilisateurs soient conformes aux exigences de conformité nécessaires.**
* **Veiller à ce que les technologies actuelles soient prises en compte. Accès au matériel et au système.**

## **Objectif**

**Les objectifs de l’audit informatique interne de Botium Toys sont les suivants :**

* **Adhérer au cadre de cybersécurité de l’Institut national des normes et de la technologie (NIST CSF)**
* **Mettre en place un meilleur processus pour leurs systèmes afin de s’assurer qu’ils sont conformes**
* **Renforcer les contrôles du système**
* **Mettre en œuvre le concept des moindres privilèges dans le cadre de la gestion des informations d’identification des utilisateurs**
* **Établir leurs politiques et procédures, y compris leurs playbooks**
* **Veiller à ce qu’ils respectent les exigences réglementaires en matière de conformité**

# **Évaluation des risques**

## **Ressources numériques actuelles**

**Les ressources numériques gérées par le service informatique sont les suivantes :**

* **Équipement sur place pour les besoins de l’entreprise**
* **Équipement des employés : appareils des utilisateurs (ordinateurs de bureau/portables, smartphones), postes de travail à distance, casque, câbles, claviers, souris, stations d’accueil, caméras de surveillance, etc.**
* **Gestion de systèmes, de logiciels et de services : comptabilité, télécommunications, base de données, sécurité, e-commerce et gestion des stocks**
* **Accès Internet**
* **Réseau interne**
* **Gestion d’hébergement de centres de données**
* **Conservation et stockage des données**
* **Lecteurs de badge**
* **Maintenance des systèmes anciens : systèmes en fin de vie qui nécessitent une surveillance humaine**

## **Description des risques**

Actuellement, la gestion des ressources est inadéquate. Par ailleurs, Botium Toys n’a pas mis en place les contrôles appropriés et ne peut pas être en conformité avec les réglementations et les normes américaines et internationales.

## **Les bonnes pratiques en matière de contrôle**

La première des cinq fonctions du NIST CSF est identifier. Botium Toys devra se consacrer à la gestion des ressources. De plus, ils devront déterminer l’impact de la perte de ressources existantes, notamment des systèmes, sur la continuité des activités.

## **Scores de risque**

**Sur une échelle de 1 à 10, le score de risque est de 8, ce qui est assez élevé. Cela est dû à un manque de contrôles et d’adhésion aux réglementations et normes de conformité nécessaires.**

## **Commentaires supplémentaires**

L’impact potentiel de la perte d’une ressource est jugé moyen, car le service informatique ne sait pas quelles ressources seraient perdues. La probabilité d’une perte de ressources ou d’amendes de la part des instances gouvernementales est élevée car Botium Toys n’a pas mis en place tous les contrôles nécessaires et n’adhère pas aux réglementations et aux normes requises en matière de confidentialité des données des clients.

# **Évaluation des contrôles**

## **Ressources numériques actuelles**

Les ressources numériques gérées par le service informatique sont les suivantes :

* Équipements sur place pour les besoins de l'entreprise
* Équipements des employés : appareils des utilisateurs (ordinateurs de bureau/portables, smartphones), postes de travail à distance, casques, câbles, claviers, souris, stations d'accueil, caméras de surveillance, etc.
* Gestion de systèmes, de logiciels et de services : comptabilité, télécommunications, bases de données, sécurité, e-commerce et gestion des stocks
* Accès Internet
* Réseau interne
* Gestion des accès des fournisseurs
* Services d'hébergement de centres de données
* Conservation et stockage des données
* Lecteurs de badge
* **Maintenance des systèmes anciens : systèmes en fin de vie qui nécessitent une surveillance humaine**

| Contrôles administratifs | | | |
| --- | --- | --- | --- |
| Nom du contrôle | Type de contrôle et explication | Doit être mis en œuvre (X) | Priorité |
| Moindre privilège | Préventif ; réduit les risques en s'assurant que les vendeurs et le personnel non autorisé n'ont accès qu'aux ressources informatiques/données dont ils ont besoin pour faire leur travail | X | Élevé |
| Plans de reprise après sinistre | Correctif ; continuité des activités pour s'assurer que les systèmes peuvent fonctionner en cas d'incident/qu'il y a une perte de productivité limitée ou nulle due aux temps d'arrêt/un faible impact sur les composants du système, notamment : l'environnement de la salle informatique (climatisation, alimentation électrique, etc.) ; le matériel (serveurs, équipements des employés) ; la connectivité (réseau interne, sans fil) ; les applications (e-mail, données électroniques) ; données et restauration | X | Élevé |
| Politiques de mots de passe | Préventif ; établir des règles sur la force des mots de passe pour améliorer la sécurité/réduire la probabilité de compromission des comptes par des techniques d'attaque par force brute ou par dictionnaire | X | Élevé |
| Politiques de contrôle d'accès | Préventif ; renforcer la confidentialité et l'intégrité des données | X | Élevé |
| Politiques de gestion des comptes | Préventif ; réduire la surface d'attaque et limiter l'impact global des employés mécontents/anciens employés | X | Élevé/  Moyen |
| Séparation des tâches | Préventif ; veiller à ce que personne ne dispose d'un accès qui pourrait lui permettre d'abuser du système à des fins personnelles | X | Élevé |

|  |  |  |  |
| --- | --- | --- | --- |
| Contrôles techniques | | | |
| Nom du contrôle | Type de contrôle et explication | Doit être mis en œuvre  (X) | Priorité |
| Pare-feu | Préventif , des pare-feux sont déjà en place pour filtrer le trafic indésirable/malveillant qui pénètre dans le réseau interne | S.O. | S.O. |
| Système de détection d'intrusion (IDS) | Détectif ; permet à l'équipe informatique d'identifier rapidement d'éventuelles intrusions (par exemple, un trafic anormal) | X | Élevé |
| Chiffrement | Dissuasif ; rend les informations/données confidentielles plus sûres (par exemple, les transactions de paiement sur des sites web) | X | Élevé/  Moyen |
| Sauvegardes | Correctif ; permet de maintenir la productivité en cas d'événement ; s'aligne sur le plan de reprise après sinistre | X | Élevé |
| Système de gestion des mots de passe | Correctif ; récupération des mots de passe, réinitialisation, notifications de verrouillage | X | Élevé/  Moyen |
| Logiciel antivirus (AV) | Correctif ; détecter et mettre en quarantaine les menaces connues | X | Élevé |
| Surveillance, maintenance et intervention manuelles | Préventif/correctif ; requis pour les systèmes existants afin d'identifier et d'atténuer les menaces, les risques et les vulnérabilités potentiels | X | Élevé |

|  |  |  |  |
| --- | --- | --- | --- |
| Contrôles physiques | | | |
| Nom du contrôle | Type de contrôle et explication | Doit être mis en œuvre  (X) | Priorité |
| Coffre-fort temporisé | Dissuasif ; réduction de la surface d'attaque/de l'impact des menaces physiques | X | Moyen/  Faible |
| Éclairage adéquat | Dissuasif ; limiter les cachettes pour dissuader les menaces | X | Moyen/  Faible |
| Surveillance par télévision en circuit fermé (CCTV) | Préventif/détectif ; peut réduire le risque de certains événements ; peut être utilisé après l'événement à des fins d'enquête | X | Élevé/  Moyen |
| Armoires verrouillables (pour les équipements de réseau) | Préventif ; accroître l'intégrité en empêchant le personnel/les personnes non autorisées d'accéder physiquement aux équipements de l'infrastructure du réseau ou de les modifier | X | Moyen |
| Panneau indiquant le fournisseur de services d'alarme | Dissuasif ; diminue la probabilité d'une attaque réussie | X | Faible |
| Verrous | Préventif ; les ressources physiques et numériques sont plus sécurisées | X | Élevé |
| Détection et prévention des incendies (alarme incendie, système de gicleurs, etc.) | Détectif/préventif : détecter un incendie sur le site physique du magasin de jouets afin d'éviter d'endommager les stocks, les serveurs, etc. | X | Moyen/  Faible |

# **Liste de contrôle de conformité**

#### \_\_\_\_\_ La Federal Energy Regulatory Commission - North American Electric

#### Reliability Corporation (FERC-NERC)

La réglementation FERC-NERC s'applique aux entreprises du secteur de l'électricité ou impliquées dans le réseau électrique aux États-Unis et en Amérique du Nord. Les entreprises ont l'obligation de se préparer, d'atténuer et de signaler tout incident de sécurité potentiel susceptible d'avoir un impact négatif sur le réseau électrique. Les entreprises sont légalement tenues d'adhérer aux normes de fiabilité relatives à la protection des infrastructures critiques (CIP) définies par la FERC.

**Explication :** S.O.

#### \_\_X\_\_ Règlement général sur la protection des données (RGPD)

Le RGPD est un règlement général européen sur les données, qui encadre le traitement des données des citoyens de l'Union européenne (UE) et leur droit à la confidentialité au sein et hors de l'UE. Par ailleurs, si une violation se produit et que les données d'un citoyen de l'UE sont compromises, celui-ci doit être informé dans les 72 heures suivant l'incident.

Explication : Botium Toys doit adhérer au RGPD parce qu'elle exerce des activités commerciales et collecte des informations personnelles auprès de personnes du monde entier, y compris de l'Union européenne.

#### \_\_X\_\_ Norme de sécurité de l'industrie des cartes de paiement (PCI DSS)

La PCI DSS est une norme de sécurité internationale visant à garantir que les entreprises qui stockent, acceptent, traitent et transmettent des informations relatives aux cartes de crédit le fassent au sein d'un environnement sécurisé.

**Explication :** Botium Toys doit adhérer à la norme PCI DSS parce qu'elle stocke, accepte, traite et transmet des informations relatives aux cartes de crédit en personne et en ligne.

#### \_\_\_\_\_ Le Health Insurance Portability and Accountability Act (HIPAA)

L'HIPAA est une loi fédérale établie en 1996 pour protéger les informations de santé des patients américains. Cette loi interdit le partage d'informations sur les patients sans leur consentement. Les entreprises ont l'obligation légale d'informer les patients d'une violation.

**Explication :** S.O.

#### \_\_X\_\_ Contrôles des systèmes et des entreprises (System and Organization Controls, SOC type 1, SOC type 2)

Les rapports SOC1 et SOC2 portent sur les politiques d'accès des utilisateurs à différents niveaux de l'entreprise. Ils sont utilisés pour évaluer la conformité financière et les niveaux de risque des entreprises. Ils couvrent également la confidentialité, le respect de la vie privée, l'intégrité, la disponibilité, la sécurité et la sûreté de l'ensemble des données. Les défaillances de contrôle dans ces domaines peuvent conduire à des fraudes.

**Explication :** Botium Toys doit établir et appliquer un accès utilisateur approprié pour le personnel interne et externe (fournisseur tiers) afin d'atténuer les risques et de garantir la sécurité des données.

## **Recommandations**

1. **Mettre en place un plan de continuité d'activité (PCA/PRA)**
2. **Appliquer la politique de moindre privilège** sur tous les systèmes
3. **Renforcer les contrôles d'accès** , de surveillance et de gestion des comptes
4. **Mettre à jour et formaliser les politiques internes**
5. **Effectuer des sauvegardes régulières**
6. **S'assurer que le chiffrement est bien appliqué aux données sensibles**
7. **Sensibiiser et former le personnel à la cybersécurité** (hameçonnage, mots de passe, etc.)
8. **Réaliser un suivi régulier des incidents de sécurité et des journaux système**