1. **Quel est le champ d'application de l'audit de sécurité interne pour Botium Toys ?** 
   * Le champ d'application de l'audit couvre l'ensemble du programme de sécurité de Botium Toys, y compris toutes les ressources numériques, les processus et procédures internes.
2. **Quels sont les objectifs de l'audit de sécurité interne pour Botium Toys ?** 
   * Les objectifs de l'audit sont d'adhérer au cadre de cybersécurité du NIST CSF, de mettre en place de meilleurs processus pour les systèmes, de renforcer les contrôles du système, d'implémenter le concept des moindres autorisations dans le cadre de la gestion des informations d'identification des utilisateurs, d'établir leurs politiques et procédures, y compris leurs playbooks, et de veiller à ce qu'ils respectent les exigences en matière de conformité.
3. **Quel est le score de risque actuel pour Botium Toys ?** 
   * Le score de risque actuel pour Botium Toys est de 8 sur une échelle de 1 à 10.
4. **Quels sont les contrôles techniques que Botium Toys devrait mettre en œuvre ?** 
   * Botium Toys devrait mettre en œuvre des pare-feu, des systèmes de détection d'intrusion (IDS), le chiffrement, des sauvegardes, des systèmes de gestion des mots de passe, des logiciels antivirus (AV), et assurer la surveillance, la maintenance et l'intervention manuelles.
5. **Botium Toys est-elle conforme aux réglementations relatives à l'acceptation des paiements en ligne et à la conduite des affaires dans l'UE ?** 
   * Je devrai vérifier la conformité de Botium Toys aux réglementations relatives à l'acceptation des paiements en ligne et à la conduite des affaires dans l'UE et identifier les écarts et les recommandations pour y remédier.

# \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Évaluation des contrôles

Pour passer en revue les catégories de contrôles, les types et les objectifs de chacun, lisez le document sur les [catégories de contrôles](https://docs.google.com/document/d/1Ut_H5A9FHwuQEy6_qG6Lfy3zwF6GSJnj3DZTMaNRWEE/template/preview?usp=sharing&resourcekey=0-i4dR5qZFqQyfzr8uk3OOmA).

## 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 | Elevé |
| 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 | Elevé |
| 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 | Elevé |
| Politiques de contrôle d'accès | Préventif ; renforcer la confidentialité et l'intégrité des données | X | Elevé |
| Politiques de gestion des comptes | Préventif ; réduire la surface d'attaque et limiter l'impact global des employés mécontents/anciens employés | X | Elevé |
| 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 | Moyenne |

|  |  |  |  |
| --- | --- | --- | --- |
| 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 | X | Moyenne |
| Système de détection d'intrusion (IDS) | Détectif ; permet à l'équipe informatique d'identifier rapidement d'éventuelles intrusions (par exemple, un trafic anormal) | X | Elevé |
| Chiffrement | Dissuasif ; rend les informations/données confidentielles plus sûres (par exemple, les transactions de paiement sur des sites web) | X | Elevé |
| Sauvegardes | Correctif ; permet de maintenir la productivité en cas d'événement ; s'aligne sur le plan de reprise après sinistre | X | Elevé |
| Système de gestion des mots de passe | Correctif ; récupération des mots de passe, réinitialisation, notifications de verrouillage | X | Moyenne |
| Logiciel antivirus (AV) | Correctif ; détecter et mettre en quarantaine les menaces connues | X | Elevé |
| 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 | Elevé |

|  |  |  |  |
| --- | --- | --- | --- |
| 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 | Moyenne |
| Éclairage adéquat | Dissuasif ; limiter les cachettes pour dissuader les menaces | X | Moyenne |
| 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 | Elevé |
| 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 | Elevé |
| Panneau indiquant le fournisseur de services d'alarme | Dissuasif ; diminue la probabilité d'une attaque réussie | X | Moyenne |
| Verrous | Préventif ; les ressources physiques et numériques sont plus sécurisées | X | Moyenne |
| 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 | Elevé |