AUDIT FLASH

Vos informations

Bienvenue !

Ce questionnaire vous permet de réaliser, en quelques minutes, une évaluation succincte de votre démarche de gestion des risques au sein de votre établissement.

En moins de 48h, les experts RiskAttitude vous répondent et vous proposent des pistes d'amélioration en gestion des risques en fonction de vos résultats.

Si vous souhaitez faire un diagnostic plus complet de votre niveau de maîtrise des risques, n'hésitez pas, contactez nous.

Veuillez remplir vos informations de contact

Nom de l'entreprise	Contact de l'entreprise	Téléphone	Adresse email
Nom de l'entreprise	Contact de l'entreprise	Téléphone	Adresse email

Sécurité des SI

Avez-vous, un jour, procédé à un audit de sécurité du système d'information de votre entreprise par une entreprise externe ?

Des audits de sécurité permettent de détecter les éléments dangereux et les corrigés rapidement. L'audit doit être fait par une entreprise externe pour être avoir un résultat le plus neutre possible.

- (•) Inconnu
- ( ) Non
- ( ) Une fois
- ( ) Récemment
- ( ) Régulièrement

Avez-vous procédé à un inventaire des OS & logiciels, installés sur le matériel fixe et portable de l'entreprise ?

Connaître les programmes installés sur les ordinateurs et machines permet de limiter l'installation de nouveaux programmes et l'oublie de renouvellement de licences.

- (•) Inconnu
- ( ) Non
- ( ) Rarement
- ( ) Occasionnellement
- ( ) Régulièrement

Votre matériel informatique fixe et portable est-il équipé de logiciels de sécurité (antivirus, firewall, etc.) ?

Les matériaux informatiques doivent être obligatoirement équipés de logiciels de sécurité sous peine d'être contaminé très rapidement.

- (•) Inconnu
- ( ) Non
- ( ) Matériel portable
- ( ) Matériel fixe et portable
- ( ) Tous types de matériels

Les logiciels détenus par l'entreprise sont-ils mis à jour ?

Les logiciels non mis à jour possèdent souvent des failles de sécurité.

- (•) Inconnu
- ( ) Non
- ( ) Rarement
- ( ) Occasionnellement
- ( ) Régulièrement

Avez-vous mis en place une charte d'utilisation du système d'information et de communication, et/ou une clause de reconnaissance de responsabilité, pour l'usage d'internet et d'intranet, des matériels informatiques et des logiciels de l'entreprise, signée par chaque salarié ?

- (•) Inconnu
- ( ) Non
- ( ) Peu
- ( ) En fonction du poste occupé
- ( ) Systématiquement

Avez-vous mis en place une politique d'attribution et de gestion des droits d'utilisation du Système d'Information en fonction des besoins de chaque salarié ?

- (•) Inconnu
- ( ) Non
- ( ) Rarement
- ( ) En fonction du poste occupé
- ( ) Systématiquement

Avez-vous une réglementation pour l'installation de tout nouveau matériel ou logiciel sur les ordinateurs fixes et mobiles de l'entreprise ?

- (•) Inconnu
- ( ) Non
- ( ) Peu
- ( ) Partiellement
- ( ) Systématiquement

Avez-vous mis en œuvre une procédure d'authentification (identification par login & mot de passe) du personnel pour accéder au système d'information ?

- (•) Inconnu
- ( ) Non
- ( ) Rarement
- ( ) Occasionnellement
- ( ) Systématiquement

Les mots de passe utilisés pour accéder au matériel informatique de l'entreprise sont-ils une combinaison de chiffres ou bien de lettres et de caractères spéciaux ?

- (●) Inconnu
- ( ) Non
- ( ) Entre 1 et 4 caractères
- ( ) Entre 4 et 7 caractères
- ( ) Plus de 8 caractères

Sécurité du Réseau

Présence d'un pare-feu ?

> Un pare-feu est un outil indispensable pour la sécurité de votre réseau. L'essentiel des menaces peut être bloqué grâce à cet outil performant. Il doit néanmoins être bien configuré pour être efficace.

- (●) Inconnu
- ( ) Aucun pare-feu sur le réseau
- ( ) Oui mais il n'est pas mis à jour
- ( ) Oui mis à jour régulièrement

Les appareils important sont-ils reliés à un onduleur ?

> Les onduleurs permettent de gérer les coupures de courant et des orages. Ils assurent les fonctionnalités des appareils reliés.

- (●) Inconnu
- ( ) Non
- ( ) En partie
- ( ) Oui

La baie serveur est-elle nettoyée ?

> La baie de brassage est un goulot d'étranglement et peut paralyser pendant plusieurs heures votre réseau en cas de dysfonctionnement. La saleté essouffle les ventilateurs et risque de ralentir vos appareils.

- (●) Inconnu
- ( ) Non
- ( ) Oui, tous les mois
- ( ) Oui, toutes les semaines

Existe-t-il un plan réseau ?

> Un mapping réseau est dangereux car il montre tous les équipements réseau avec leurs adresses ip. Néanmoins il est très utile pour gérer un réseau ou pour une reprise rapide en cas de défaillance.

- (●) Inconnu
- ( ) Non
- ( ) Oui mais seulement une partie du réseau
- ( ) Oui mais pas mis à jour
- ( ) Oui tout le réseau et mis à jour régulièrement

Les serveurs et autres appareils sont-ils dans des locaux sécurisés ?	Les éléments importants de votre réseau doivent être protégés par des locaux sécurisés (Climatiseur, détection incendie, fermé à clé, etc.).	◉ Inconnu ○ Non ○ En partie ○ Oui

Facteur humain

Les salariés ont-ils été sensibilisés et/ou formés sur la confidentialité qu'ils doivent accorder à leurs login et mots de passe ?		◉ Inconnu ○ Non ○ Tous les ans ○ Tous les 6 mois ○ Rappels réguliers
Existe-t-il un Responsable de la Sécurité des Systèmes d'Information (RSSI), désigné ou recruté ?		◉ Inconnu ○ Non / Prestataire externe à temps partiel ○ Prestataire externe à plein temps ○ Oui à temps partiel
Existe-t-il un Responsable de la Sécurité des Systèmes d'Information (RSSI), désigné ou recruté ?		◉ Inconnu ○ Non / Prestataire externe à temps partiel ○ Prestataire externe à plein temps ○ Oui à temps partiel ○ Oui à plein temps
Le personnel est-il sensibilisé aux règles élémentaires en matière de sécurité informatique (fermeture de session, mails frauduleux, etc.) ?		◉ Inconnu ○ Non ○ Tous les ans ○ Tous les 6 mois ○ Rappels réguliers

Vos collaborateurs sont-ils sensibilisés aux conséquences de pertes / vols / destructions de données ?

- (●) Inconnu
- ( ) Non
- ( ) Tous les ans
- ( ) Tous les 6 mois
- ( ) Rappels réguliers

Vos employés vous avertissent lors d'un problème ou d'éléments étranges ?

> Les éléments peuvent être des mails frauduleux, un site internet frauduleux,etc.

- (●) Inconnu
- ( ) Jamais
- ( ) Rarement
- ( ) Occasionnellement
- ( ) Systèmatiquement

Incidents et gestion de crise

Avez-vous élaboré un Plan de Continuité d'Activité (PCA) et un plan de reprise d'activité régulièrement testés ?

> Le plan de reprise et le plan d'action permettent lors d'un bug ou d'une attaque de reprendre une activité normale en un minimum de temps.

- (●) Inconnu
- ( ) Non
- ( ) Oui mais non mis à jour
- ( ) Oui et mis à jour occasionnellement
- ( ) Oui et mis à jour régulièrement

Délai estimé pour reprendre les activités après une attaque informatique ou autre perte/corruption de données ?

- (●) Inconnu
- ( ) > 24h
- ( ) < 24h
- ( ) < 12h
- ( ) < 3h

Temps durant lequel l'entreprise aura cessé son activité du fait d'un arrêt du système informatique entraînant des conséquences graves pour sa pérennité et son développement ?

- (●) Inconnu
- ( ) > 24h
- ( ) < 24h
- ( ) < 12h
- ( ) < 3h

Un plan de sauvegarde est-il formalisé et mis à jour régulièrement ?

- (●) Inconnu
- ( ) Non
- ( ) Oui

Envoyer

AUDIT FLASH