




QUESTIONNAIRE D'AUTO-ÉVALUATION

La rubrique suivante présente un questionnaire simple qui peut guider la direction d'une entreprise dans l'examen de ses capacités de résilience à des menaces de cyber-sécurité, en proposant les questions clés à poser aux équipes impliquées. Ce questionnaire a été conçu pour permettre d'identifier les forces et les faiblesses de l'organisation, et mettre en avant les pistes d'amélioration à suivre pour renforcer son niveau de résilience.

Ce questionnaire peut également être utilisé comme une *checklist* par les entreprises qui en sont à leurs débuts en matière de sécurité : les questions et réponses listées peuvent alors permettre de structurer un plan d'implémentation d'un dispositif complet de cyber-sécurité.

Pour chacune des questions qui suivent, il convient de choisir l'option qui reflète le mieux les pratiques actuelles de l'entreprise. Chacune des options s'est vue attribuer un point de couleur, suivant les principes suivants :




-  C'est la réponse la moins souhaitable ; des améliorations doivent absolument être envisagées.
-  Quelques améliorations supplémentaires pourraient être apportées, afin de mieux protéger l'entreprise.
-  Cette réponse correspond à la situation recommandée, afin d'offrir un niveau de résilience suffisant face aux menaces de cyber-sécurité.

En outre, la présence d'une *checklist détaillée au-dessous de chaque question* permet d'identifier et de documenter l'état d'une série de contrôles de sécurité de base au sein de l'entreprise.

Pour chaque question, un lien avec les actions et principes décrits dans les deux précédents chapitres est proposé : ce lien permet aux répondants d'utiliser les actions et principes du Guide comme lignes directrices lors de la définition de plans d'actions.



1. EVALUEZ-VOUS LA SENSIBILITÉ DES INFORMATIONS AU SEIN DE VOTRE ENTREPRISE?

-  Non, mais nous avons un pare-feu pour nous protéger du vol d'informations.
-  Oui, nous comprenons l'importance de nos informations et données, et nous mettons en œuvre des mesures générales de sécurité.
-  Oui, et nous disposons d'un modèle de classification de l'information et nous savons où nos données sensibles sont stockées et traitées. Les mesures de sécurité que nous mettons en œuvre, le sont en fonction du niveau de sensibilité de l'information concernée.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Vos données sensibles sont-elles identifiées et classifiées ?		
Êtes-vous conscient de vos responsabilités liées aux informations identifiées comme sensibles (lois, réglementations, mesures internes, ...) ?		
Les données les plus sensibles sont-elles particulièrement protégées ou cryptées ?		
La gestion des données à caractère personnel est-elle couverte par des procédures spécifiques ?		
Vos employés sont-ils tous capables de différencier des données sensibles de données non sensibles, et de les traiter en fonction ?		




LES PRINCIPES SUIVANTS S'APPLIQUENT :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :



2. ÉVALUEZ-VOUS LES RISQUES LIÉS À LA SÉCURITÉ DE L'INFORMATION ?

-  Nous n'exécutons pas d'évaluations de risque.
-  Nous exécutons des évaluations de risque, mais pas spécifiquement sur des sujets relatifs à la sécurité de l'information.
-  Nous accomplissons des évaluations de risque sur des sujets relatifs à la sécurité de l'information.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Abordez-vous les vulnérabilités détectées par niveau de risque, du niveau le plus élevé au plus faible ?		
Les événements susceptibles d'entraîner des interruptions de l'activité de l'entreprise sont-ils identifiés, et l'impact de telles interruptions est-il évalué ?		
Disposez-vous d'un plan de continuité de l'activité (business continuity plan) qui est régulièrement testé et mis à jour ?		
Menez-vous régulièrement une évaluation des risques, permettant de réévaluer vos besoins en termes de cyber-sécurité ?		
Identifiez-vous les zones de risque au sein de vos différents processus métier, afin de définir les mesures requises pour contrer la corruption de vos données ou l'utilisation malveillante de cette information ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :





3. À QUEL NIVEAU SE PLACE LA RESPONSABILITÉ DE LA SÉCURITÉ DE L'INFORMATION AU SEIN DE VOTRE ORGANISATION ?

- ✘ Il n'y a pas de gouvernance spécifique à la sécurité de l'information au sein de notre entreprise.
- Une gouvernance de la sécurité de l'information existe, et est installée au sein du département informatique, étant donné que ce sont ces équipes qui doivent agir pour sécuriser l'information.
- ✔ Une gouvernance de la sécurité de l'information existe, et est installée au niveau de la direction de l'entreprise, afin de s'assurer que l'ensemble de l'entreprise soit concernée par la gestion de la cyber-sécurité.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Les membres du conseil d'administration allouent-ils un budget à la sécurité de l'information ?		
La sécurité de l'information fait-elle partie des pratiques de gestion du risque de la direction ?		
La direction approuve-t-elle la politique de sécurité de l'entreprise, et s'assure-t-elle de sa diffusion au personnel ?		
Les membres du conseil d'administration et la direction de l'entreprise sont-ils régulièrement informés des dernières évolutions des politiques, normes ou procédures de gestion de la sécurité de l'entreprise ?		
Est-ce qu'au moins un membre de la direction a la charge de la protection des données et de la protection de la vie privée ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :



L'ACTION SUIVANTE PEUT ÊTRE PRISE :



4. DISPOSEZ-VOUS D'UNE ÉQUIPE OU D'UNE FONCTION DÉDIÉE À LA GESTION DE LA SÉCURITÉ DE L'INFORMATION ?

- ✗ Nous n'avons pas d'équipe dédiée à la sécurité de l'information, et n'avons pas spécifiquement alloué de rôles ou responsabilités en la matière.
- Nous n'avons pas d'équipe dédiée à la sécurité de l'information, mais nous avons défini des rôles et responsabilités spécifiques concernant la sécurité de l'information au sein de l'entreprise.
- ✓ Nous avons une équipe ou une fonction spécifiquement en charge de la gestion de la sécurité de l'information.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Est-ce qu'un spécialiste ou une équipe sécurité coordonne la gestion des compétences en matière de sécurité, et assiste la direction dans la prise de décision sur les sujets de sécurité ?		
Est-ce que le responsable ou l'équipe sécurité a la responsabilité de revoir et mettre à jour la politique de sécurité en fonction des évolutions de l'entreprise, ou des incidents de sécurité rencontrés ?		
Est-ce que le responsable ou l'équipe sécurité dispose de suffisamment de visibilité et de soutien managérial pour intervenir dans toute initiative liée à l'information ?		
Différents managers sont-ils responsables des différents types de données ?		
Faites-vous régulièrement évaluer par un organe indépendant (interne ou externe) si votre politique de sécurité est réaliste et efficace et l'action de l'équipe de sécurité performante ?		

LE PRINCIPE SUIVANT S'APPLIQUE :






L'ACTION SUIVANTE PEUT ÊTRE PRISE :





5. COMMENT GÉREZ-VOUS LES RISQUES DE SÉCURITÉ LIÉS AUX FOURNISSEURS QUI ACCÈDENT À VOS DONNÉES SENSIBLES ?

-  Nous avons une relation fondée sur la confiance mutuelle avec nos fournisseurs.
-  Pour certains contrats, nous incluons des clauses relatives à la sécurité de l'information.
-  Nous avons des processus en place pour valider l'accès des fournisseurs à nos données, et avons établi des directives de sécurité spécifiques qui sont communiquées et signées par nos fournisseurs.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Les fournisseurs et autres parties externes sont-ils identifiés par un badge d'identification, lequel comprend une photo récente ?		
Avez-vous une politique de contrôle des antécédents de vos sous-traitants et fournisseurs ?		
Les accès à vos bâtiments et systèmes sont-ils automatiquement désactivés lorsqu'un sous-traitant ou un fournisseur termine sa mission ?		
En cas de perte ou vol d'information, vos fournisseurs savent-ils comment et à qui immédiatement rapporter cet incident au sein de votre entreprise ?		
Votre entreprise s'assure-t-elle que les fournisseurs maintiennent leurs logiciels et applications à jour (et notamment, installent les mises à jour de sécurité) ?		




LE PRINCIPE SUIVANT S'APPLIQUE :



L'ACTION SUIVANTE PEUT ÊTRE PRISE :



6. FAITES-VOUS ÉVALUER RÉGULIÈREMENT LA SÉCURITÉ INFORMATIQUE ET DE RÉSEAU ?

-  Nous n'effectuons pas d'audit ou de test d'intrusion pour évaluer notre sécurité informatique et de réseau.
-  Nous n'avons pas d'approche systématique pour commander des audits de sécurité et/ou des tests de pénétration mais en exécutons occasionnellement.
-  Des audits de sécurité réguliers et / ou des tests d'intrusion font systématiquement partie de notre approche pour évaluer notre sécurité informatique et de réseau.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Faites-vous des tests réguliers, et documentez-vous les menaces ainsi identifiées ?		
Disposez-vous de procédures visant à évaluer les menaces humaines, telles que la malhonnêteté, l'ingénierie sociale et l'abus de confiance ?		
Votre entreprise exige-t-elle des rapports d'audit de sécurité auprès de ses fournisseurs de services informatiques ?		
L'utilité de chaque type de données stockées est-elle également évaluée pendant les audits de sécurité ?		
Faites-vous auditer vos procédures et processus de gestion de la sécurité, pour vous assurer de leur conformité avec les autres politiques et normes établies au sein de l'entreprise ?		

LE PRINCIPE SUIVANT S'APPLIQUE :






LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :





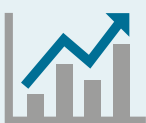
7. LORSQU'ELLE INTRODUIT DE NOUVELLES TECHNOLOGIES, VOTRE ENTREPRISE ÉVALUE-T-ELLE LES RISQUES POTENTIELS EN MATIÈRE DE SÉCURITÉ DE L'INFORMATION ?

-  L'évaluation des risques en termes sécurité de l'information ne fait pas partie du processus de mise en œuvre de nouvelles technologies.
-  La gestion de la sécurité de l'information est parfois considérée lors de la mise en œuvre de nouvelles technologies, mais cela n'est pas systématique.
-  La gestion de la sécurité de l'information est incluse dans le processus de mise en œuvre de nouvelles technologies.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Lorsque vous envisagez de mettre en œuvre de nouvelles technologies, évaluez-vous l'impact potentiel sur la politique de sécurité de l'information de votre organisation ?		
Disposez-vous de mesures de protection qui réduisent les risques éventuellement liés à la mise en œuvre de nouvelles technologies ?		
Les processus de mise en œuvre de nouvelles technologies sont-ils documentés ?		
Avez-vous noué des partenariats avec d'autres acteurs, dans une optique de collaboration et d'échange d'informations utiles relatives à la sécurité lors de l'implémentation de nouvelles technologies ?		
La politique de sécurité de votre entreprise est-elle souvent considérée comme un frein à l'innovation technologique ?		

LE PRINCIPE SUIVANT S'APPLIQUE :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :



8. LA SÉCURITÉ DE L'INFORMATION A-T-ELLE UNE PLACE DANS VOTRE ORGANISATION?

- ✘ Nous avons confiance en nos employés et nous ne considérons pas qu'un accompagnement plus important en matière de sécurité apporte de la valeur ajoutée à l'entreprise.
- Seul notre personnel informatique reçoit une formation spécifique pour sécuriser notre environnement informatique.
- ✔ Des sessions de sensibilisation à la sécurité sont régulièrement organisées, à l'attention de tous les employés.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Adaptez-vous le contenu de certaines sessions de sensibilisation au métier et à l'activité des participants (et aux menaces qui sont liées à cette activité, spécifiquement) ?		
Formez-vous vos équipes à être attentives aux violations des principes et mesures de sécurité ?		
Votre entreprise dispose-t-elle d'instructions claires à l'attention des utilisateurs, expliquant comment rapporter des faiblesses ou des menaces sécuritaires liées à vos systèmes ou à vos activités ?		
Votre personnel connaît-il les bonnes pratiques à suivre en termes d'utilisation des données de cartes de crédit et de gestion d'informations à caractère personnel ?		
Les autres utilisateurs de vos systèmes (p.ex. fournisseurs ou clients) sont-ils également formés en matière de sécurité et informés des évolutions de vos politiques et procédures de sécurité ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :



L'ACTION SUIVANTE PEUT ÊTRE PRISE :





9. COMMENT UTILISEZ-VOUS LES MOTS DE PASSE AU SEIN DE L'ENTREPRISE ?

- X** Nous partageons les mots de passe avec d'autres collègues et / ou il n'existe pas de politique définissant les règles liées à l'usage sûr des mots de passe ou leur renouvellement régulier.
- O** Tous les employés, y compris la direction, possèdent des mots de passe uniques, mais des règles relatives à la complexité de leur composition ne sont pas imposées. Le changement des mots de passe est possible, mais pas obligatoire.
- ✓** Tous les employés, y compris la direction, disposent d'un mot de passe personnel qui doit satisfaire à des exigences précises en matière de complexité et doit être changé régulièrement.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Votre entreprise a-t-elle établi et implémenté une politique en matière de mot de passe ?		
Avez-vous les moyens de garantir que tous les mots de passe ont été changés au moins une fois et sont régulièrement modifiés, correspondent à vos exigences de complexité, et ne sont pas stockés dans des fichiers facilement accessibles, et ce aussi pour les appareils mobiles ?		
Vous sentez-vous bien protégé contre un accès physique non autorisé à vos systèmes ?		
Vos utilisateurs, tant internes qu'externes, ont-ils conscience de leur responsabilité en termes de protection des équipements laissés sans surveillance (p.ex. conscients de l'importance de mettre fin à sa session avant de quitter son poste) ?		
Les employés ont-ils été formés à l'identification de tentatives d'ingénierie sociale, et aux façons de réagir à une telle menace ?		




LE PRINCIPE SUIVANT S'APPLIQUE :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :



10. DISPOSEZ-VOUS D'UNE POLITIQUE RELATIVE À LA BONNE UTILISATION D'INTERNET ET DES MÉDIAS SOCIAUX ?

-  Non, nous ne disposons pas d'une politique relative à la bonne utilisation d'internet et des médias sociaux.
-  Oui, une telle politique placée à un endroit accessible par tous les employés a été publiée, mais elle n'a pas été signée par chaque membre du personnel.
-  Oui, une telle politique existe et a été signée par chaque membre du personnel, ou fait partie de son contrat de travail.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Existe-t-il des directives à l'attention de tout membre du personnel, définissant les règles relatives aux communications effectuées au nom de l'entreprise (y compris vers la presse ou sur les médias sociaux) ?		
Existe-t-il un processus disciplinaire pour les employés qui violent les directives de communication de l'entreprise ?		
Est-ce que l'équipe ou le responsable communication de l'entreprise passe régulièrement internet en revue afin d'évaluer la 'réputation en ligne' de l'entreprise, et les éventuels risques qui la menace ?		
Votre entreprise a-t-elle évalué comment sa responsabilité serait engagée, en cas d'utilisation de ses systèmes par des utilisateurs internes ou des pirates afin de perpétrer des actes illégaux ?		
Votre entreprise a-t-elle pris des mesures pour empêcher un employé ou tout autre utilisateur interne d'attaquer d'autres sites ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :





11. EST-CE QUE VOTRE ENTREPRISE MESURE, RAPPORTE ET ASSURE LE SUIVI DES SUJETS RELATIFS À LA SÉCURITÉ ?

- ✗ Nous ne contrôlons pas, nous ne rapportons pas et nous ne suivons pas ni l'efficacité ni l'adéquation des mesures de sécurité que nous avons mises en œuvre.
- Nous avons des outils et méthodes pour mesurer, rapporter et suivre tant l'efficacité que l'adéquation de certaines de nos mesures de sécurité, mais pas toutes.
- ✓ Notre entreprise a mis en œuvre les outils et méthodes nécessaires pour mesurer l'efficacité et l'adéquation de toute mesure de sécurité mise en œuvre, faire le rapport de ces évaluations, et faire le suivi des éventuels points d'amélioration.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Les traces systèmes (traces d'audit et logs) relatives aux incidents sont-elles toujours conservées, et des actions sont-elles prises pour empêcher que l'incident ne se reproduise ?		
Votre entreprise contrôle-t-elle son degré de conformité aux exigences légales et réglementaires (p.ex. la protection des données à caractère personnel) ?		
Disposez-vous d'outils permettant aux managers d'évaluer le niveau global de sécurité de leurs activités, et leur offrant les moyens de répondre plus rapidement à d'éventuels risques de sécurité ?		
Votre entreprise dispose-t-elle d'une feuille de route relative à la sécurité de l'information, qui définisse notamment les objectifs à atteindre et les indicateurs de progrès à suivre ?		
Les rapports de contrôle et d'incidents sont-ils partagés avec les autorités compétentes, et avec d'autres groupes d'intérêts tels qu'une fédération sectorielle ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :



L'ACTION SUIVANTE PEUT ÊTRE PRISE :



12. COMMENT MAINTENEZ-VOUS VOS SYSTÈMES À JOUR ?

- ✘ Nous nous basons sur la gestion automatique des correctifs telle que proposée par le fournisseur pour la plupart de nos solutions.
- Nous installons les correctifs de sécurité systématiquement, à intervalles réguliers (p.ex. sur base mensuelle).
- ✔ Nous disposons d'un processus de gestion des vulnérabilités par lequel nous nous tenons constamment à jour sur d'éventuelles nouvelles vulnérabilités (par ex. via un abonnement à un service d'alertes signalant toute nouvelle vulnérabilité), et nous appliquons les correctifs rapidement, en fonction du niveau de risque lié à la vulnérabilité qu'ils solutionnent.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Des scans de vulnérabilités sont-ils planifiés et régulièrement exécutés au sein de l'entreprise ?		
Les applications sont-elles revues et testées, après tout changement au niveau des systèmes d'exploitation ?		
Les utilisateurs peuvent-ils contrôler eux-mêmes si les applications sont bien à jour (aucun patch de sécurité manquant) ?		
Les utilisateurs sont-ils conscients qu'au niveau de leurs appareils mobiles, ils doivent également maintenir à jour le système d'exploitation et les applications qui y sont installées (y compris les applications de sécurité) ?		
Avez-vous formé vos utilisateurs à reconnaître d'éventuels faux messages d'avertissement systèmes (p.ex. demandant l'autorisation de mettre un logiciel à jour, ou émanant d'un faux antivirus) et à systématiquement avertir vos équipes de sécurité si un tel évènement suspect s'est produit ?		

LE PRINCIPE SUIVANT S'APPLIQUE :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :





13. LES DROITS D'ACCÈS SONT-ILS RÉGULIÈREMENT REVUS ?

- Les droits d'accès des utilisateurs aux applications et systèmes de l'entreprise, ne sont pas retirés ou revus de façon structurée et systématique.
- Les droits d'accès des utilisateurs aux applications et systèmes de l'entreprise sont uniquement retirés lorsqu'un employé quitte l'entreprise ; il n'y a pas de processus de revue régulière des accès existants.
- Une politique de contrôle d'accès est en place et inclut des revues régulières des droits d'accès assignés aux utilisateurs pour toutes les applications et systèmes pertinents de l'entreprise.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
L'accès électronique et physique aux systèmes d'information est-il restreint, sur base de politiques et procédures de gestion des accès ?		
Votre entreprise s'appuie-t-elle sur une politique de protection de la vie privée indiquant l'information qu'elle recueille (par exemple concernant vos clients : les adresses physiques, les adresses électroniques, l'historique de navigation, etc.), et la façon dont cette information est exploitée ?		
Vos politiques et procédures de gestion des accès précisent-elles quelles méthodes doivent être utilisées pour contrôler l'accès physique à des zones sécurisées (p.ex. installation de portes, systèmes de contrôle d'accès, surveillance vidéo, ...) ?		
Les droits d'accès aux systèmes et aux bâtiments de votre entreprise sont-ils automatiquement désactivés lorsqu'un membre du personnel quitte votre entreprise ?		
Les données sensibles sont-elles classifiées (p.ex. confidentiel, sensible, usage interne,...) et les utilisateurs ayant droit d'y accéder inventoriés ?		

LE PRINCIPE SUIVANT S'APPLIQUE :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :



14. VOS EMPLOYÉS PEUVENT-ILS UTILISER LEURS APPAREILS PERSONNELS (SMARTPHONES, TABLETTES, ...) POUR STOCKER OU TRANSFÉRER DES INFORMATIONS DE L'ENTREPRISE ?

- ✗ Oui, nos employés peuvent stocker ou transférer des informations de l'entreprise sur des appareils personnels, sans que nous exigions la mise en œuvre de mesures de sécurité supplémentaires.
- Il existe une politique qui interdit l'utilisation d'appareils personnels pour stocker ou transférer des informations de l'entreprise, mais techniquement, nos employés peuvent les utiliser et ne sont pas forcés à mettre en œuvre des mesures de sécurité supplémentaires.
- ✓ Les appareils personnels peuvent uniquement stocker ou transférer des informations de l'entreprise après la mise en œuvre de mesures de sécurité sur l'appareil concerné et/ou moyennant l'utilisation d'une solution professionnelle.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Votre entreprise dispose-t-elle d'une politique de Bring Your Own Device, autorisant le personnel à utiliser ses appareils mobiles personnels moyennant une série de conditions ?		
Les appareils mobiles sont-ils protégés contre l'accès par des utilisateurs non autorisés ?		
Les appareils mobiles et les connexions sont-ils/elles identifié(e)s de manière permanente sur le réseau ?		
Les données des appareils mobiles sont-elles cryptées, afin de protéger leur confidentialité et leur intégrité ?		
Votre direction est-elle consciente que si chaque employé est responsable de son appareil personnel, c'est l'entreprise qui est responsable des données professionnelles qu'il pourrait contenir ?		

LE PRINCIPE SUIVANT S'APPLIQUE :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :





15. VOTRE ENTREPRISE A-T-ELLE PRIS DES MESURES CONTRE LA PERTE D'INFORMATIONS?

- ✗ Nous ne disposons pas de processus de gestion des sauvegardes ou de mécanismes garantissant la disponibilité de nos données.
- Nous disposons de processus de gestion des sauvegardes et de mécanismes garantissant la disponibilité de nos données. Cependant, aucun test de ces processus (restauration des données sauvegardées, ...) n'a été réalisé.
- ✓ Nous disposons d'un processus de gestion des sauvegardes et de mécanismes garantissant la disponibilité de nos données, lesquels incluent des tests de restauration / de résilience. Nous stockons des copies de nos sauvegardes sur un autre site sécurisé ou nous utilisons d'autres solutions de 'haute disponibilité des données'.

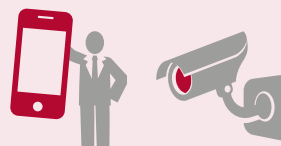
Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Votre entreprise compte-t-elle suffisamment d'employés capables de sauvegarder ou archiver vos données selon des méthodes qui permettent de rapidement les restaurer ?		
Vos équipements sont-ils protégés des coupures de courant par le biais de systèmes d'alimentation électrique permanente (utilisation de différentes lignes électriques, onduleurs ⁶ , générateurs électriques, etc.) ?		
Les supports de sauvegarde (tape, disques, etc.) sont-ils régulièrement testés, afin de vous assurer que vos données peuvent être restaurées dans les limites de temps définies?		
Votre entreprise dispose-t-elle de procédures garantissant que la perte ou le vol d'équipements portables sont immédiatement notifiés ?		
Vos employés sont-ils formés afin de savoir comment réagir en cas de suppression accidentelle de données, ou comment récupérer ces données en cas de désastre ?		

LES PRINCIPES SUIVANTS S'APPLIQUENT :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :



⁶ Aussi connu sous le nom de UPS, ou 'Uninterruptible Power Supply'

16. VOTRE ENTREPRISE EST-ELLE PRÉPARÉE À GÉRER UN INCIDENT LIÉ À LA SÉCURITÉ DE L'INFORMATION ?

- ✘ Nous ne craignons pas d'incident. Et si un incident survient, nos employés sont suffisamment compétents pour y faire face.
- Nous avons des procédures de gestion des incidents, inadaptées toutefois au traitement des incidents en matière de sécurité de l'information.
- ✔ Nous avons un processus dédié au traitement des incidents liés à la sécurité de l'information, ainsi que les dispositifs d'escalation et de communication nécessaires. Nous nous efforçons de traiter les incidents de la manière la plus performante et efficace possible, et d'en tirer les leçons qui nous permettront de mieux nous protéger à l'avenir.

Les 5 questions suivantes ont pour but de vous proposer quelques contrôles fondamentaux en matière de gestion de la sécurité de l'information.

	OUI	NON
Votre processus prend-il en compte différents types d'incidents - du déni de service (denial of service) à la violation de confidentialité, etc. - ainsi que les moyens d'y faire face ?		
Votre entreprise dispose-t-elle d'un plan de communication intégré au processus de gestion des incidents ?		
Avez-vous identifié les autorités auxquelles notifier un incident, et comment procéder à cette notification ?		
Disposez-vous de points de contacts (et de leurs coordonnées) identifiés pour chaque type d'incident ?		
Vous reposez-vous sur un représentant du service de communication interne de votre entreprise, pour les contacts avec les employés et leurs familles ?		

LE PRINCIPE SUIVANT S'APPLIQUE :



LES ACTIONS SUIVANTES PEUVENT ÊTRE PRISES :

