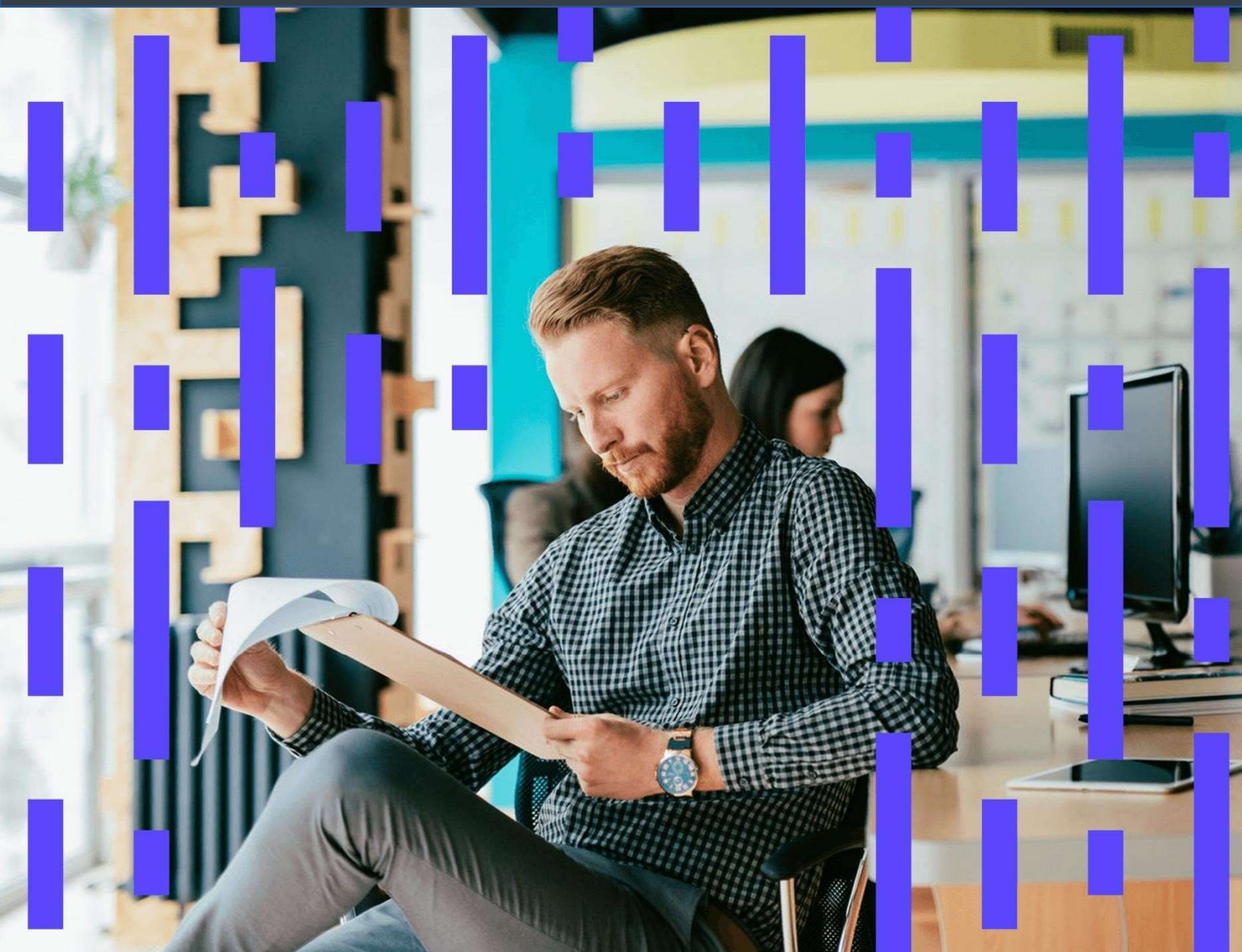
Prevalent™
acensi CYBERSECURITY

Guide des bonnes pratiques

# Cinq étapes pour une gestion proactive des risques liés aux fournisseurs

Un guide pour construire, faire mûrir ou optimiser votre programme TPRM



# Table des matières

## La réalité d'aujourd'hui : Équilibrer la croissance des entreprises et les risques commerciaux

Toutes les organisations s'appuient sur des vendeurs et des fournisseurs à un certain niveau pour fournir des produits et des services à leurs clients, ces tiers recevant et traitant souvent des informations sensibles. Toutefois, compte tenu de la surveillance accrue et des sanctions liées aux exigences réglementaires et aux exigences en matière de confidentialité des données, du risque de perte de clients et de poursuites judiciaires en cas de violation de données par des tiers, et de la possibilité permanente d'une perturbation opérationnelle due à une faiblesse de la chaîne d'approvisionnement, il est important de s'assurer que ces fournisseurs ont mis en place les contrôles de sécurité appropriés.

Qu'elle soit manuelle, sur tableur ou ad hoc, l'évaluation du risque liée aux tiers peut prendre énormément de temps, être sujette à des erreurs et des omissions, et laisser les décideurs s'appuyer sur des informations obsolètes et incomplètes. Un processus efficace de gestion des risques tout au long du cycle de vie de la relation avec le fournisseur comprend :

- Identifier, intégrer et hiérarchiser les fournisseurs en fonction de leur risque inhérent
- Evaluer de manière centralisée les fournisseurs en utilisant le bon contenu de questionnaire et en surveillant les contrôles internes de chaque tiers en fonction de leur risque inhérent
- Valider la diligence raisonnable et les preuves soumises par rapport à la notation de sécurité externe et à d'autres renseignements sur les risques, puis utiliser ces informations pour déterminer un niveau de risque résiduel
- Remédier aux risques et en rendre compte à un niveau acceptable en établissant des priorités appropriées
- Évaluer, contrôler et éliminer les risques liés aux fournisseurs de manière proactive et continue

Gérer les fournisseurs manuellement est un processus coûteux, inefficace et, surtout, non modulable à l'échelle de tout un écosystème de partenaires. Pourtant, les risques de ne pas le faire correctement sont douloureusement apparents : amendes, audits ratés, non-conformité et, pire que tout, la redoutable violation des données et sa divulgation (trop) publique.

La question cruciale à laquelle vous devez répondre est la suivante : Comment pouvez-vous automatiser vos processus afin de garantir rapidement et efficacement que vos tiers ne créent pas un potentiel inacceptable de perturbation des activités dans votre chaîne d'approvisionnement ?

Ce guide des bonnes pratiques vous aidera à répondre à ces questions en vous indiquant par où commencer un programme de gestion des risques par des tiers (TPRM), comment le faire évoluer pour en faire un programme évolutif et souple qui s'adapte aux changements de l'entreprise, et quels sont les résultats commerciaux auxquels vous pouvez vous attendre tout au long de votre parcours. Pour préparer le terrain, nous définirons d'abord les niveaux de maturité du programme et nous définirons les attributs d'un programme TPRM en fonction de ces niveaux. Ensuite, nous passerons en revue les cinq étapes nécessaires à l'optimisation du TPRM.

Tout au long de ce guide, vous trouverez divers panneaux indicateurs pour vous guider. Surveillez-les !

**C'est un piège !**
*Les pièges à éviter*

**Attributs techniques**
*Capacités clés*

**Conseils et bonnes pratiques**
*Ce que nous avons appris en cours de route*

**Étude de cas**
*Ce que font les vrais clients pour résoudre ce problème*

# L'objectif : un programme de gestion des risques plus mature et optimisé pour les tiers

Bien que Gartner indique clairement que le principal moteur du TPRM est la conformité, les programmes TPRM peuvent découler d'un certain nombre d'exigences organisationnelles - de la conformité à la gestion des risques de la chaîne d'approvisionnement, en passant par la prévention des violations de données. Sur la base de notre expérience, nous avons défini trois niveaux de maturité des programmes de gestion des risques liés à la chaîne d'approvisionnement.

## Niveau 1 : TPRM centré sur l'automatisation

Les programmes qui commencent en réaction à des perceptions personnelles de taches fastidieuses à réaliser (par exemple, la charge de travail ou la complexité) ont tendance à être les moins mûrs. Ils ne sont généralement pas motivés par des préoccupations de gestion des risques ou de conformité, mais plutôt par un individu, peut-être dans le domaine des achats, qui cherche à accélérer le processus d'intégration du fournisseur. Les organisations de niveau 1 n'ont pas la supervision des programmes plus matures qui sont liés à un effort de gouvernance, de risque et de conformité (GRC). L'objectif ici est d'automatiser autant que possible le processus de collecte et d'analyse des preuves des fournisseurs afin de réduire les allers-retours incessants entre l'entreprise et les fournisseurs à l'aide de feuilles de calcul. Il n'y a rien de mal à démarrer votre programme TPRM ici. Après tout, il faut bien commencer quelque part, et vous pouvez réussir à justifier le financement d'un tel projet en liant des processus manuels incohérents au risque d'erreurs pouvant entraîner des violations de données.

## Niveau 2 : TPRM axé sur la conformité

En remontant l'échelle de maturité, les programmes de niveau 2 sont principalement axés sur la conformité en ce sens que l'organisation doit répondre à une ou plusieurs exigences réglementaires. Les organisations à ce niveau de maturité réalisent qu'elles ont besoin d'un *programme, et* non d'un *projet,* pour évaluer le risque de leurs fournisseurs de premier rang. Cependant, elles ont souvent une visibilité limitée avec trop de feuilles de calcul et trop d'interactions par courrier électronique avec leurs fournisseurs. Si votre organisation se situe à ce niveau de maturité, sachez que la plupart des autres entreprises se trouvent également à ce niveau.

## Niveau 3 : TPRM centré sur le risque

Les programmes TPRM les plus matures sont dirigés de haut en bas par des programmes de gestion des risques - et la conformité est un sous-produit de cet effort. Les organisations de niveau de maturité 3 connaissent le nombre de fournisseurs et peuvent quantifier le risque de ces fournisseurs, bien qu'avec des niveaux d'automatisation moins qu'idéaux. Leurs programmes TPRM et GRC/IRM sont étroitement liés ; ils bénéficient d'un parrainage de la direction ; et ils s'assurent probablement les services de l'un des cinq grands cabinets d'audit pour l'externalisation ou la gestion des programmes. Ce niveau de maturité est rare en dehors des grandes organisations hautement réglementées qui disposent de ressources, d'une vision et d'une échelle suffisantes.

Consultez le tableau de la page suivante pour évaluer où en est votre programme et où vous aimeriez le voir évoluer.

*Tableau 1 : Exemples de niveaux de maturité du TPRM*

| Maturité | Chauffeur | Attributs |
|---|---|---|
| Niveau 1 | Automatisation | • Une approche ascendante<br>• Processus manuel<br>• Besoin de questionnaires simples et personnalisés<br>• Un projet (par opposition à un programme)<br>• Commence petit avec un nombre limité de fournisseurs<br>• Sensibilisation limitée/visibilité du risque<br>• Les entreprises ne dirigent pas les efforts de réduction des risques ou de mise en conformité |
| Niveau 2 | Conformité | • Approche intermédiaire<br>• A un projet spécifique de mise en conformité<br>• Processus manuels pour évaluer un sous-ensemble de fournisseurs<br>• Fournisseurs classés par service ou dépense critique<br>• Comprend le manque de visibilité sur le risque<br>• Cherche à créer un programme TPRM mais a besoin d'aide pour le définir |
| Niveau 3 | Gestion des risques | • Une approche descendante<br>• Comprendre la situation dans son ensemble<br>• Partie d'un programme plus large de gestion des risques<br>• Connaît le nombre total de fournisseurs et est capable de quantifier le risque<br>• Évalue actuellement un pourcentage du nombre total de fournisseurs utilisant des processus manuels<br>• Parrainage de niveau C et budget alloué<br>• Comprend qu'il s'agit d'un programme, et non d'un projet |

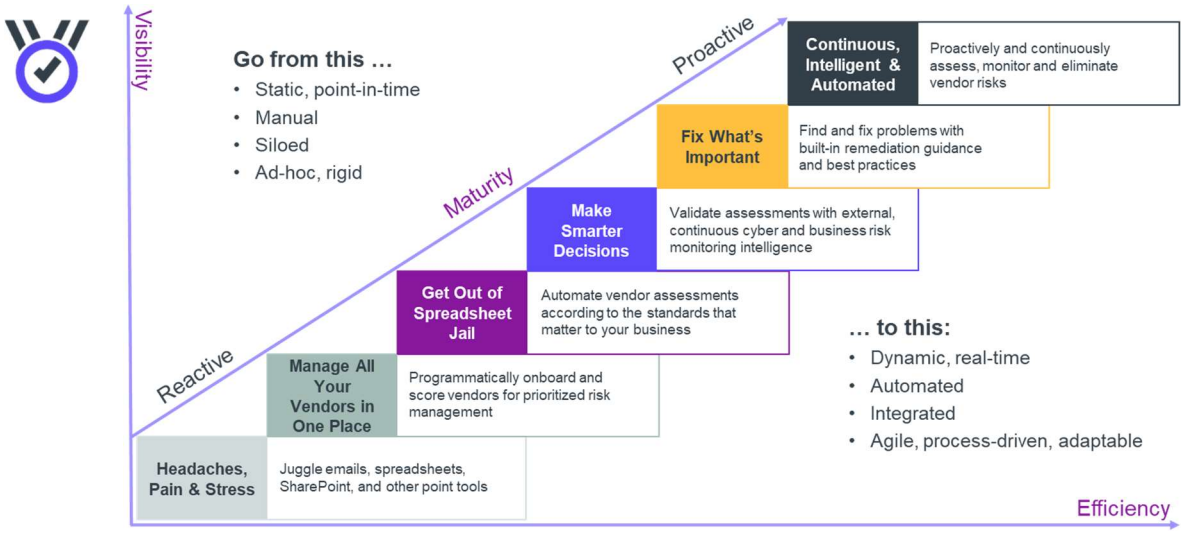
Le chemin vers la maturité n'est pas facile. Et il n'est pas rapide. Il n'y a pas de raccourcis. Toutefois, en investissant dans les bonnes personnes, les bons processus et les bonnes technologies, vous pouvez atteindre des niveaux d'automatisation plus élevés qui, en fin de compte, augmenteront la productivité de votre équipe de gestion des risques. Cela vous aidera à aligner vos efforts sur vos priorités. La section suivante de ce guide présente une approche en cinq étapes pour parvenir à un programme de gestion des risques des tiers plus mature, plus proactif et plus efficace.

# Ce qu'il faut chercher : Cinq étapes vers un programme de gestion des risques plus mature et plus proactif pour les tiers

Un processus programmatique est la voie la plus rapide pour arrêter la pénibilité de la gestion des risques par des tiers, pour prendre des décisions éclairées fondées sur les risques, et pour adapter et développer un programme au fil du temps. Cette section du guide présente un plan de déploiement en cinq étapes pour le TPRM et identifie les capacités clés à rechercher chez un fournisseur de solutions. Voir la figure 1 ci-dessous pour une représentation du processus.

Le résultat de ce processus est une visibilité dynamique et en temps réel des risques liés aux fournisseurs, une automatisation et une intégration accrues pour accélérer l'évaluation de vos fournisseurs, ainsi qu'une approche agile, axée sur les processus, pour adapter et faire évoluer votre programme afin de répondre aux demandes futures.

*Figure 1 : Un processus progressif de maturation d'un programme TPRM*




Tout au long du processus d'élaboration de votre programme de gestion des risques des tiers, gardez à l'esprit ces exigences commerciales, car elles vous aideront à défendre efficacement ce programme auprès de vos collègues :

- Minimiser le coût total du programme
- Fournir un délai de rentabilisation rapide
- Fournir des informations pour prendre les meilleures décisions en fonction des risques

## Étape 1 : Gérez tous vos fournisseurs en un seul endroit

Plusieurs décisions doivent être prises avant de lancer un programme de gestion des risques par un tiers. Des services consultatifs d'experts peuvent vous aider à définir les paramètres du programme, à vous assurer que vous évaluez les bons fournisseurs en fonction du risque inhérent et de la criticité de l'entreprise, et à définir le bon contenu à collecter auprès des fournisseurs sur la base de cadres réglementaires ou de normes industrielles. Une fois ces décisions prises, la première étape concrète consiste à prendre le contrôle de vos fournisseurs, à les intégrer et à se faire une idée de leur risque inhérent.

Les décisions clés à prendre à cette étape sont notamment les suivantes :

- Quel est le bon mécanisme pour l'intégration/onborading des fournisseurs ?
- Quels facteurs prendrez-vous en considération pour prendre des décisions concernant l'échelonnement des fournisseurs ?
- Comment allez-vous recueillir des informations pour évaluer les risques inhérents présentés par un vendeur ?

### Options pour l'intégration des fournisseurs

Le processus d'intégration des fournisseurs implique généralement un téléchargement manuel ou en un transfert de masse. Nous avons constaté que la combinaison d'un tableur préconfigurée ou d'une connexion API à une solution existante de gestion des fournisseurs est le mécanisme le plus efficace pour télécharger les fournisseurs. L'accès basé sur les rôles devrait permettre aux équipes de remplir les données des fournisseurs et d'inviter d'autres employés à y contribuer.

### Facteurs à prendre en compte pour prendre des décisions d'échelonnement

Vous pouvez utiliser n'importe quel critère pour classer ou catégoriser les fournisseurs, des dépenses annuelles au risque inhérent, à la criticité des services et à la sensibilité de l'accès. Toutefois, les décisions de hiérarchisation doivent être principalement influencées par l'environnement réglementaire dans lequel vous opérez. Par exemple, si la GDPR est un moteur important pour votre organisation, alors la hiérarchisation des fournisseurs en fonction de leur accès aux données personnelles de vos clients doit être une considération primordiale dans le processus. Un processus typique de hiérarchisation des fournisseurs pourrait suivre cette logique :

#### *Définir les attributs clés*

- Type de contenu requis pour informer les rapports de contrôle
- Criticité pour les performances des entreprises
- Localisation du fournisseur et si cette localisation soulève des obligations légales ou réglementaires telles que la GDPR
- Déterminer si les services du fournisseur reposent sur des tiers

### *Considérations sur la criticité des fournisseurs*

Il est important de bien comprendre l'impact qu'un fournisseur pourrait avoir sur votre entreprise s'il échouait en termes de livraison ou de performance des services. Par conséquent, vous devez utiliser un système de notation qui détermine le groupe de niveaux de fournisseurs. Ce système pourrait inclure les critères suivants :

- Processus opérationnels ou contact avec les clients
- Interaction avec les données à caractère personnel
- Situation financière et implications
- Obligations légales et réglementaires
- Réputation

Une fois que vous avez déterminé les niveaux de vos fournisseurs, vous devez avoir une ventilation claire des fournisseurs les plus critiques. Par exemple, vous devez pouvoir établir un rapport sur tous les fournisseurs basés en France, qui traitent des données personnelles et qui sont de premier rang.

Lorsque vous commencez votre exercice de profilage et de hiérarchisation des tiers, il y a certaines considérations à prendre en compte pour assurer son succès :

- **Commencez à petite échelle, puis augmentez :** Les premières évaluations seront une expérience d'apprentissage. Commencez par un petit nombre d'enquêtes jusqu'à ce que les connaissances et les processus de l'équipe aient été optimisés.
- **Fixez des délais réalistes :** Bien que vous puissiez publier des enquêtes en vrac, considérez que chaque enquête doit être remplie par une personne et créez des objectifs réalisables en conséquence.
- **Tenez compte de la capacité :** Lorsque vous planifiez un exercice de profilage et de hiérarchisation réussi, estimez combien d'enquêtes un seul intervenant peut gérer sur une période donnée et planifiez l'exercice en conséquence.
- **Préparez le support :** Envisagez de préparer un document de foire aux questions (FAQ) sur l'orientation des réponses.
- **Planifier la communication :** Créer un plan de communication pour les intervenants afin d'encourager les progrès. Cela peut inclure l'identification des objectifs, aux personnes à contacter pour toute assistance.

## Calcul du risque inhérent

Afin de bien comprendre le risque que les fournisseurs représentent pour une organisation, vous devez être en mesure de calculer le **risque inhérent,** ou le niveau de risque actuel compte tenu de ce qui est considéré comme l'ensemble des contrôles existants (ou l'absence de contrôles) pour ce fournisseur. Le calcul du risque inhérent est important lors de l'intégration de nouveaux fournisseurs et pour éclairer les décisions de profilage, de hiérarchisation et de catégorisation. Une fois le risque inhérent défini, il est beaucoup plus simple de calculer le **risque résiduel, c'**est-à-dire le niveau de risque restant après l'application des contrôles.

Le calcul du risque inhérent nécessite une visibilité granulaire et contextuelle de la situation actuelle et historique du risque d'un fournisseur et doit aller au-delà des questions de profilage de base. Une vue plus complète de la notation du risque inhérent à l'intégration comprendrait des données opérationnelles, juridiques et réglementaires, financières, de réputation et autres, et inclurait de multiples parties prenantes internes répondant chacune à des questions spécifiques sur le fournisseur.

La notation du risque inhérent doit être basée sur le score de risque en temps réel d'un fournisseur par rapport au score le plus élevé possible qu'il aurait obtenu si aucun contrôle n'avait été mis en place. Utilisez une matrice qui combine la probabilité et l'impact pour déterminer le score.

Cette fonction de notation et de rapport sur les risques vous permettra d'établir une base de référence cohérente sur les risques que les nouveaux fournisseurs apportent à votre entreprise, d'accélérer l'intégration en toute sécurité et de fournir des renseignements en temps réel sur la manière de remédier aux risques au fil du temps pour parvenir à un risque résiduel acceptable.

## Top 5 des capacités à rechercher lorsque vous centralisez vos fournisseurs :

1. API et connecteurs vers des solutions communes pour automatiser l'intégration.
2. Modèle préétabli pour programmer l'intégration des fournisseurs.
3. Évaluation de profilage et de hiérarchisation pour mettre en œuvre une méthodologie reproductible d'évaluation des fournisseurs.
4. Evaluation et suivi des risques inhérents et résiduels afin d'identifier clairement les fournisseurs qui présentent les risques les plus importants pour l'entreprise.
5. Services permettant d'intégrer et d'évaluer de nouveaux fournisseurs pour les équipes aux ressources humaines insuffisantes.

L'organisation des services d'évaluation des risques des fournisseurs de Prevalent a pour but de vous libérer du fardeau de la gestion des risques par des tiers. Prevalent peut s'occuper de tout, de l'intégration des fournisseurs et de la réalisation d'évaluations, à l'identification des risques et au suivi des mesures correctives. Prevalent s'occupe de la partie fastidieuse pour que vous puissiez vous concentrer sur la stratégie des fournisseurs et la réduction globale des risques.

## Étude de cas : Allianz réalise un gain de temps de 50%.

Allianz Insurance plc est l'un des plus grands assureurs généraux du Royaume-Uni et fait partie du groupe Allianz SE, le plus grand assureur de dommages au monde. La société a été mise au défi de respecter ses objectifs de conformité et de gestion des risques de la Prudential Regulation Authority (PRA) et de la Financial Conduct Authority (FCA). Cela était dû en grande partie à un manque de cohérence dans les rapports, ainsi qu'à un long processus d'évaluation des fournisseurs qui s'appuyait sur des feuilles de calcul et des visites sur place. Une fois déployée, la plateforme de gestion des risques des tiers (TPRM) a simplifié l'ensemble du processus, permettant à Allianz d'effectuer des évaluations et d'intégrer les fournisseurs deux fois plus rapidement qu'auparavant. Depuis, Allianz a étendu l'utilisation de la plate-forme à la gestion des processus de demande d'informations et de demande de propositions de l'organisation.

## Étape 2 : Sortir de la prison des tableurs

Une fois que vous avez décidé comment intégrer, classer et évaluer le risque inhérent de vos fournisseurs, l'étape suivante de la gestion complète des risques liés aux tiers consiste à se débarrasser de ces feuilles de calcul, à recueillir des preuves et à effectuer un examen de diligence raisonnable des réponses soumises, conformément aux normes et aux exigences de conformité qui vous importent. La collecte et l'examen de diligence raisonnable peuvent prendre de nombreuses formes : gestion du processus par vous-même, utilisation d'un répertoire de questionnaires préremplis, sous-traitance à un partenaire ou une combinaison de ces méthodes. Mais il faut d'abord déterminer quel questionnaire utiliser.

Les décisions clés à prendre à cette étape sont notamment les suivantes :

- Quel questionnaire sera utilisé pour recueillir des informations sur les contrôles de votre vendeur ? Utiliserez-vous des enquêtes standard ou propres a votre entreprise ?
- Quelle(s) méthode(s) de collecte sera(ont) utilisée(s) ? Gérerez-vous la collecte vous-même ? Profiterez-vous des dépôts de questionnaires préremplis ? Sous-traiterez-vous la collecte à un partenaire ? Une combinaison des méthodes ?

### Quel questionnaire utiliser ? Standard de l'industrie ou propriétaire ?

Il y a des cas à faire pour les deux. L'utilisation de questionnaires standard (par exemple, le questionnaire standard de collecte d'informations ou SIG, ou le questionnaire H-ISAC pour les organismes de santé) peut vous permettre de démarrer plus rapidement en fournissant un ensemble de contenus acceptés que vos fournisseurs connaissent probablement déjà. L'évaluation de tous les fournisseurs utilisant le même contenu standard permet également d'assurer une certaine cohérence. Vous obtenez une comparaison plus proche de services similaires, tout en permettant à vos fournisseurs de partager leurs réponses avec d'autres partenaires s'ils le souhaitent. Répondre une fois à un questionnaire et le partager avec de nombreux partenaires présente un avantage tangible.

D'autre part, la création de contenu propriétaire à partir de questions ou de questionnaires multiples est utile pour les organisations qui ont moins de fournisseurs à évaluer (c'est-à-dire où la cohérence est moins importante), ou pour celles qui ont besoin d'un instrument d'enquête spécifique aux besoins de leur entreprise.

L'utilisation d'un référentiel d'évaluations prédéfinies - comprenant des questionnaires standard comme SIG Core, SIG Lite et H-ISAC, et des questionnaires spécifiques au cadre de conformité et de sécurité comme CMMC, GDPR, FCA, PCI-DSS, ISO 27001, NIST et autres - simplifie et automatise le processus de collecte et de gestion des enquêtes. Recherchez la possibilité d'importer ou de créer des éléments à examiner au cours du processus d'évaluation, avec des capacités de personnalisation pour répondre à des besoins uniques.

Que vous utilisiez l'approche normalisée ou propriétaire, assurez-vous que les fournisseurs potentiels de TPRM ont la flexibilité nécessaire pour fournir les deux types de questionnaires, afin de ne pas vous enfermer dans un questionnaire unique et rigide.

## Choisir la méthode de collecte des données et d'analyse – le DIY, la bibliothèque partagée ou l'externalisation ?

### *DIY (do it yourself)*

Une fois que vous avez défini votre questionnaire, vous pouvez gérer en interne la collecte et l'analyse des données sur les fournisseurs. Toutefois, assurez-vous de disposer d'une solution pour gérer le flux de travail, les communications avec les fournisseurs et la gestion des documents/preuves afin de centraliser, suivre et simplifier le processus de diligence raisonnable. La solution doit comprendre un portail convivial destiné aux fournisseurs, qui affiche clairement l'état d'avancement de l'enquête et les mesures correctives suggérées, tout en conservant une piste de vérification complète pour une validation ultérieure. N'oubliez pas que plus il sera facile pour les fournisseurs de remplir et de soumettre les informations requises, plus vous pourrez identifier et corriger les risques rapidement.

### *Bibliothèque partagée*

Les processus de gestion des risques par des tiers peuvent être éprouvants pour les équipes qui manquent de ressources. Les processus de collecte de données et les échanges entre les fournisseurs représentent la plus grande partie du temps nécessaire pour réduire les risques et compléter l'assurance de l'évaluation. À cela s'ajoute le paysage réglementaire en constante évolution, qui exige une expertise pour comprendre les obligations de déclaration de conformité. Il est certain qu'atteindre la conformité et répondre aux exigences de gestion des risques des fournisseurs tout en maximisant les compétences de votre équipe est un exercice d'équilibre.

Pour faire face aux contraintes de ressources, de nombreuses organisations - en particulier celles qui disposent d'un solide plan de hiérarchisation des fournisseurs - choisissent de tirer parti des contenus déjà soumis et partagés dans le cadre d'un échange industriel. Ces échanges de fournisseurs sont des prophéties qui se réalisent d'elles-mêmes : plus les fournisseurs y participent, plus il y a de chevauchements avec d'autres entreprises, ce qui accélère le processus d'identification et d'atténuation des risques et minimise le temps nécessaire à la collecte des données.

Prevalent gère deux réseaux mondiaux de renseignements sur les fournisseurs propres à l'industrie : le Legal Vendor Network (LVN) et le Healthcare Vendor Network (HVN) par l'intermédiaire du H-ISAC. Nous proposons également un "réseau de réseaux" appelé Prevalent Exchange. Chaque réseau s'appuie sur un questionnaire standard accepté par les membres ou l'organe de direction concernés, ce qui simplifie et accélère l'analyse et l'atténuation des risques, et offre un accès à la demande à plus de 10 000 profils de fournisseurs constamment mis à jour. Si votre organisation est un cabinet d'avocats ou un organisme de soins de santé (par exemple, l'industrie pharmaceutique, l'assurance, etc.), assurez-vous d'enquêter sur les réseaux prévalents. Les clients indiquent qu'environ 40 % de leurs fournisseurs font déjà partie du réseau. Cela permet des économies immédiates de temps et de coûts de 44 %.

*Externalisation*

Une dernière option consiste à externaliser la collecte et l'analyse des preuves à un vendeur de TPRM, une société d'audit ou un intégrateur de systèmes. Votre fournisseur de solutions ou votre intégrateur de systèmes peut vous offrir des capacités de correction et d'analyse sans immobiliser vos ressources internes. Cela permet à votre équipe de se concentrer sur les efforts de gestion des risques (par exemple, l'identification et la remédiation), plutôt que sur la collecte de preuves du fournisseur et la garantie de leur exactitude. Cela permet d'accélérer la rentabilité des efforts de réduction des risques et constitue une option solide pour les équipes dont les ressources sont extrêmement limitées, ou celles dont les compétences internes sont restreintes.

Comme pour la sélection des questionnaires, les fournisseurs de TPRM qui offrent une flexibilité dans les méthodes de collecte permettront à votre équipe de rester agile.

## Top 7 des capacités de collecte et d'examen des preuves :

1. Bibliothèque de centaines de milliers de profils de fournisseurs vérifiés, permettant d'identifier, d'intégrer et d'évaluer les risques plus rapidement et avec moins de ressources.
2. Le plus grand nombre de modèles d'évaluation préétablis et prêts à l'emploi pour garantir que les fournisseurs sont évalués de manière flexible et en fonction du mandat ou du cadre qui est important pour l'entreprise.
3. Assistant de création d'évaluations personnalisées offrant une certaine souplesse pour évaluer les fournisseurs en fonction de leurs exigences particulières.
4. Automatisation des flux de travail et des tâches pour accélérer le processus d'évaluation.
5. Documents, contrats, accords et preuves centralisés, constituant un dépôt pour plusieurs équipes.
6. Des rapports prêts à l'emploi sur de multiples exigences de conformité et de cadre en utilisant un seul questionnaire pour alimenter les réponses, ce qui permet de gagner du temps.
7. Options permettant d'externaliser la conception du questionnaire ainsi que la collecte et l'analyse des éléments probants à des experts afin de pallier la pénurie de ressources.

Le Prevalent Vendor Intelligence Network permet aux équipes de gestion des risques et des IT/OT de se concentrer sur l'élimination des risques et la mise en conformité en s'appuyant sur un répertoire de questionnaires remplis par les fournisseurs, étayé par des renseignements de surveillance continue. Grâce à la collecte externalisée de la diligence raisonnable et de la surveillance, les organisations économisent du temps et des ressources, ce qui leur permet d'étendre rapidement leur programme de gestion des risques des tiers. Chez Prevalent, ce programme est piloté par les services d'évaluation des risques des fournisseurs, des équipes d'experts en gestion des risques de tiers qui recueillent les preuves des fournisseurs, les examinent pour s'assurer qu'elles sont complètes et fournissent des conseils pour remédier aux principaux risques.

## Étude de cas : Une entreprise pharmaceutique mondiale obtient un retour sur investissement tangible

Une entreprise pharmaceutique mondiale a pris du retard dans la réalisation de ses 250 à 550 évaluations annuelles des risques par des tiers et risquait de manquer d'importants délais de mise en conformité en raison de problèmes de complexité permanents avec son outil TPRM existant. En mettant en œuvre la plate-forme TPRM, elle a depuis supprimé 18 étapes manuelles de son processus, ce qui équivaut à une réduction d'une heure-personne par évaluation. L'entreprise économise ainsi entre 250 et 550 heures-personnes (soit 31 à 68 jours) pour effectuer ses évaluations des risques liés aux fournisseurs. Cela a également éliminé le besoin d'externaliser les ressources contractuelles, libérant ainsi des ressources pour d'autres projets de gestion des risques dans l'organisation.

## Étape 3 : Prendre des décisions plus intelligentes

Une fois que vous avez décidé comment intégrer, classer et évaluer vos fournisseurs, l'étape suivante de la gestion complète des risques des tiers consiste à valider ces évaluations des fournisseurs par une veille externe et continue des risques cyber et commerciaux. Bien que des évaluations périodiques soient essentielles pour comprendre comment les fournisseurs gèrent leurs programmes de sécurité de l'information et de confidentialité des données à un moment donné, il peut arriver beaucoup de choses à un fournisseur au cours d'une année entre deux évaluations ! La surveillance de vos fournisseurs présente plusieurs avantages, notamment :

- **Immédiateté** - L'obtention d'une vue instantanée des risques exploités par les pirates informatiques peut éclairer votre logique de hiérarchisation et de priorisation des fournisseurs.
- **Validation** - Validation des réponses des fournisseurs aux enquêtes lorsqu'ils commencent à arriver.
- **Fréquence** - Obtenir plus fréquemment des informations impartiales sur les cyber-vulnérabilités potentielles de votre fournisseur ou sur les risques commerciaux pertinents qui peuvent avoir un impact négatif sur votre entreprise.

Prenez un peu de recul pour voir si un "score" ou une "cote de sécurité" résoudra votre problème. Ces outils ne fournissent qu'une analyse externe du réseau qui montre les cyber-risques de base. Sans garantie pour le fournisseur, sans contexte et avec des limites d'information limitées en fonction de la pertinence pour votre entreprise, la notation et l'évaluation des fournisseurs donnent une vue limitée du risque du fournisseur, ce qui signifie qu'il n'y a pas de véritable évaluation. Vous vous souvenez de l'étape 1, où nous disions que la plupart des programmes TPRM sont motivés par la conformité ?
Considérez ceci :

- Qu'en est-il de la mesure de l'adhésion interne d'un fournisseur mandats de conformité ? Une analyse externe peut-elle le révéler ?
- Une note de sécurité peut-elle vous indiquer comment un fournisseur traite vos données ?
- Comment les notes de sécurité peuvent-elles automatiser la collecte des preuves des fournisseurs et leurs obligations ?

Si la notation ou le classement des risques de l'extérieur vers l'intérieur peut fournir des informations sur les risques, elle ne répondra pas aux exigences de conformité lorsqu'elle sera utilisée comme seul mécanisme d'évaluation des risques des fournisseurs. Les bonnes pratiques pour le TPRM, telles que publiées par Shared Assessments, Gartner, Forrester et d'autres, comprennent des évaluations par questionnaire pour les fournisseurs, ainsi qu'un contrôle continu pour une vue complète des risques des fournisseurs.

## Quelles sont les cyber données à surveiller

La surveillance des réseaux de votre fournisseur est plus qu'une simple gestion des vulnérabilités, bien que la gestion des vulnérabilités en soit une partie importante. Combinez-la avec de multiples sources externes de renseignements sur les menaces cybersécurité, notamment les réseaux de capteurs Internet, les bases de données mondiales sur les menaces, les partenaires de sécurité et les utilisateurs d'antivirus, pour obtenir des renseignements :

- **Dark Web** - Les mentions récentes et fréquentes d'une entreprise sur le dark web sont souvent en corrélation avec une plus grande activité de menace contre l'entreprise, ce qui augmente la probabilité d'une attaque. L'attention portée au dark web peut indiquer la vente illicite d'actifs ou de comptes de l'entreprise, ou des manœuvres frauduleuses.
- **Abus de domaine / Typosquatting - Les** nouveaux enregistrements de domaines présentant une similitude de style typosquatting avec des domaines d'entreprise existants sont des indications potentielles d'abus de domaine (comme le phishing), ou d'enregistrement à titre préventif pour atténuer l'abus de domaine, ou les deux.
- **Sécurité du courrier électronique -** Configurations des politiques du cadre stratégique de l'expéditeur (SPF), du courrier identifié par des clés de domaine (DKIM) et de l'authentification, de la notification et de la conformité des messages par domaine (DMARC).
- **Fuite de credentials** - L'exposition des informations d'identification et emails indique une réutilisation potentielle de mot de passe ou de l'adresse mail de l'entreprise, ce qui augmente le risque d'attaques et de ciblage par les hackeurs.
- **Incidents** - Les divulgations de violations de la sécurité et les rapports de cyber-attaques validés indiquent qu'une entreprise a probablement été victime d'une cyber-attaque, d'une violation ou d'un événement récent qui a mis en danger son parc informatique.
- **Infrastructure** - violations de la politique de sécurité, intrusions dans l'infrastructure de l'entreprise, logiciels malveillants, mauvaises configurations, vulnérabilités, hôtes infectés, logiciels non pris en charge.
- **Sécurité des applications web** - Certificats et configurations SSL/TLS.

Ces informations sont exactement ce qui est visible pour les pirates informatiques. Les renseignements peuvent être utilisés pour aider les fournisseurs à nettoyer leur empreinte open-source ou à modifier les processus internes afin de réduire les risques en comblant les lacunes et les écarts d'anomalies - comme vous le feriez pour nettoyer votre rapport de crédit avant de demander un prêt au logement.

## Les risques commerciaux sont également importants !

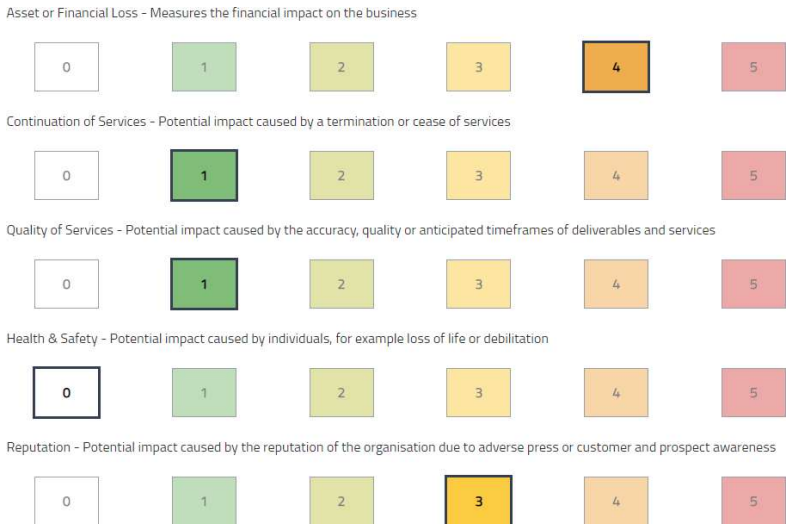
- **Opérationnel** - activités de fusion et d'acquisition, licenciements, changements de direction, changements de partenariat, relations avec les clients et expansion géographique
- **Marque** - Violations de données, rappels de produits et changements de marque
- **Réglementaire/juridique** - Sondages, amendes, sanctions économiques/listes noires et procès et règlements importants.
- **Financier** - Les faillites, les transactions en capital (dettes, capitaux propres, etc.) et les violations de données ont un impact sur la viabilité financière

Ensemble, la surveillance des risques en cybersécurité et commerciaux donne une vision beaucoup plus complète d'un fournisseur. Cette vue "extérieur-intérieur" vous donne un avantage pour interpréter l'impact potentiel du risque d'un fournisseur tout en augmentant vos évaluations "intérieur-extérieur" pour obtenir un score de risque plus informé et plus précis.

## L'intérêt d'un registre central des risques

La meilleure approche pour l'analyse et la notation consiste à centraliser d'abord les résultats dans un registre des risques et de la conformité. La génération automatique d'un registre des risques une fois l'enquête ou l'analyse terminée permet de filtrer les bruits inutiles et d'aider votre équipe à se concentrer sur les domaines susceptibles de poser problème.

Comme tous les risques ne sont pas créés égaux, il est important d'avoir une certaine souplesse dans la manière dont vous pondérez les risques. Par exemple, si un fournisseur répond à une question indiquant l'absence d'un programme de sensibilisation des employés à la sécurité, mais que cela n'est pas important pour votre organisation, il faut alors pondérer les risques afin que votre équipe puisse déterminer ou sont réellement les risques. Ceci est illustré ci-dessous :




Lorsque les fournisseurs répondent à des questions dans le cadre d'une évaluation, vous devriez pouvoir créer des risques en fonction des réponses. En règle générale, vos évaluateurs ou les responsables des fournisseurs effectuent ensuite des recherches sur les preuves soumises pour identifier les faux positifs ou négatifs dans le cadre du processus de soumission. En examinant les éventuelles lacunes, ils pourraient mettre en évidence des points nécessitant une attention particulière. L'examinateur validerait les preuves et créerait ensuite le risque si les preuves le justifiaient. Le fait de signaler les points préoccupants dans les réponses des fournisseurs garantit que les bons risques sont étudiés, ce qui contribue à réduire le profil de risque global de votre organisation.

Une pratique de TPRM mise en œuvre avec succès permettra de classer les risques selon leur probabilité et leur impact. Comme une carte thermique, cette capacité peut aider les équipes à se concentrer sur les risques les plus importants.

Un exemple de cette capacité est illustré à droite.


## L'importance d'un score inside-out/outside-in

Comme nous l'avons mentionné dans notre avertissement, la notation et les cotes de sécurité fournies par une analyse du réseau externe ne révéleront que la moitié de l'histoire du TPRM. C'est pourquoi il est important de combiner ces résultats avec ce que vous obtenez à partir de votre évaluation par questionnaire. Cette combinaison donne une représentation fidèle de la conformité de votre fournisseur et de son statut de risque, avec des conseils beaucoup plus complets pour remédier à ces risques.

## Top 9 des capacités de surveillance continue :

1. La cybersurveillance à partir du deep/dark web pour obtenir des informations en temps réel sur les risques.
2. Surveillance des entreprises à partir de centaines de milliers de sources fournissant des informations sur les questions commerciales, réglementaires ou juridiques.
3. API RESTful pour permettre les connexions à d'autres systèmes.
4. Un registre des risques unifié qui établit une corrélation entre les risques cybersécurité et commerciaux et les résultats de l'évaluation de chacun de vos fournisseurs, ce qui permet de valider les données de contrôle communiquées par les fournisseurs.
5. Transformez les données des cyber-événements et des événements commerciaux des fournisseurs entrants en risques actionnables, en vous donnant une visibilité des risques en temps réel.
6. Déclencher des actions telles que l'envoi de notifications, la création de tâches ou de flags, ou l'élévation des notes de risque, accélérant ainsi le processus d'atténuation des risques.
7. Des pondérations de risques flexibles qui définissent de manière granulaire l'importance de risques spécifiques pour l'entreprise.

8. Le marquage et la catégorisation - automatique ou manuelle - pour faire remonter un risque et l'acheminer vers le contact approprié pour remédier.
9. Une matrice qui permet d'analyser dynamiquement les risques en fonction de la probabilité d'un incident et de son impact potentiel sur l'entreprise.

Faisant partie de la plate-forme de gestion des risques des tiers basée sur le cloud, Vendor Threat Monitor est intégré à l'évaluation interne des risques des fournisseurs. Toutes les données de surveillance et d'évaluation sont centralisées dans un registre des risques unifié pour chaque fournisseur, ce qui vous permet de mettre rapidement en corrélation les résultats et de rationaliser les initiatives d'examen, de rapport et de réponse aux risques.

## Étude de cas : Une grande entreprise américaine du secteur de l'énergie et des services publics acquiert une visibilité immédiate sur des risques jusque-là inconnus

Une grande entreprise américaine du secteur de l'énergie/des services publics a été mise au défi d'évaluer des milliers de fournisseurs. Avec un personnel limité, l'organisation réagissait constamment aux menaces liées aux fournisseurs, avec un manque de confiance et de validation adéquate des politiques et procédures de sécurité des fournisseurs. Elle a mis en place le Service de surveillance des menaces des fournisseurs, afin d'élargir le contexte des risques liés aux fournisseurs. En moins d'une semaine, la solution Prevalent a identifié un événement à risque concernant un service web actif et très peu sécurisé sur le site web d'un fournisseur. Le site a exposé les logins et les informations critiques en texte clair et Prevalent a identifié la vulnérabilité du site web associée. Le service public a averti le vendeur, qui a immédiatement remédié à la vulnérabilité, évitant ainsi l'exposition du client (et d'autres). En combinant la surveillance avec les capacités d'évaluation de Prevalent, le service public a obtenu une protection à 360 degrés et l'assurance du fournisseur.

## Étape 4 : Corriger ce qui est important

À ce stade, vous avez probablement fait des allers-retours avec vos fournisseurs pour faire remplir des questionnaires et soumettre des preuves tangibles. Vous avez peut-être même procédé à une validation de ces preuves à distance ou sur place. Malheureusement, le va-et-vient n'est pas encore terminé. Le plus difficile est maintenant de remédier aux résultats.

Vous vous souvenez de la hiérarchisation des fournisseurs dont nous avons parlé à l'étape 1 et du registre des risques que nous avons couvert à l'étape 4 ? Ces attributs seront extrêmement importants au cours de cette étape et vous aideront à classer les fournisseurs de manière dynamique en fonction des niveaux de risque et de la criticité pour l'entreprise. Ils permettront également un flux de travail bidirectionnel pour les mesures correctives et la gestion des documents dans le registre des risques.

Il peut être difficile de prévoir les niveaux de risque futurs. Il faut donc rechercher des capacités qui montrent comment les niveaux de risque évoluent dès la mise en application des remédiations par le fournisseur.

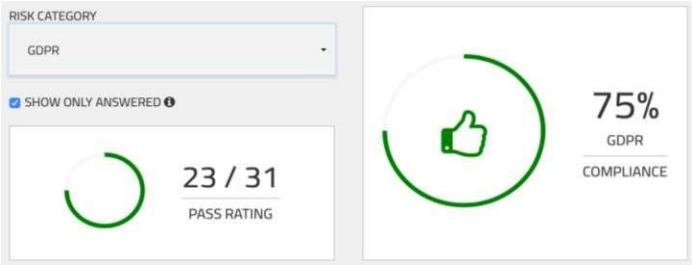
### L'importance des rapports spécifiques aux autorités réglementaires

Étant donné que la gestion des risques liés aux tiers est un élément de contrôle essentiel dans la plupart des régimes réglementaires et des secteurs, il est important de montrer les progrès réalisés dans la mise en conformité avec ces exigences - pour les auditeurs à l'intérieur et à l'extérieur de votre organisation. Toutefois, les rapports de conformité peuvent être complexes et longs à établir, compte tenu des nombreux outils de gestion des risques. L'intégration de rapports pour les réglementations communes et les cadres sectoriels est donc essentielle pour accélérer et simplifier le processus de conformité.

Prevalent dispose d'un livre blanc détaillé qui extrait les exigences spécifiques de gestion des risques des tiers énoncées dans de multiples réglementations et cadres industriels, explique ce que ces exigences signifient, puis associe les principales capacités de la solution aux exigences pour démontrer comment une plate-forme TPRM complète peut contribuer à alléger le fardeau de la conformité. Sauvez votre santé mentale et téléchargez ce document !

L'un des moyens d'accélérer la production de rapports de conformité est de gagner en visibilité sur le niveau de conformité de chaque vendeur. Commencez par établir un seuil de pourcentage de conformité "satisfaisant" par rapport à une catégorie de risque (par exemple, X % de conformité par rapport à un cadre ou une ligne directrice particulière). Tous les rapports seront liés à ce pourcentage de conformité et votre équipe pourra se concentrer sur les sous-domaines où les taux de réussite sont faibles. Cette évaluation doit également être effectuée au niveau macro pour tous les fournisseurs, et pas seulement au niveau des fournisseurs. Les rapports au niveau macro seront importants pour le conseil d'administration qui cherchera à déterminer dans quelle mesure l'organisation est conforme à la réglementation "Saveur du mois".

Le "pourcentage de conformité" devrait faire partie de chaque rapport d'audit, qui devrait également indiquer les domaines spécifiques nécessitant des mesures correctives supplémentaires. Voir l'exemple de GDPR à droite.



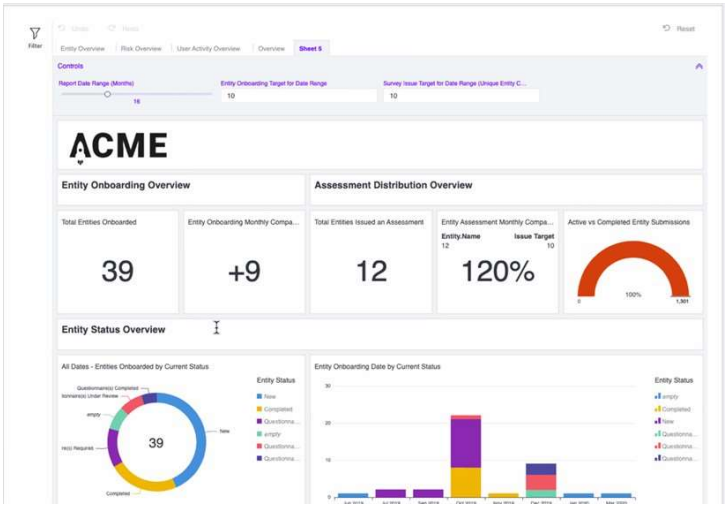
## Mais il ne s'agit pas seulement de conformité

Bien que la conformité soit un facteur essentiel de la gestion des risques par des tiers, vous devez toujours rendre compte des exigences spécifiques en matière de cybersécurité. Une solution TPRM complète doit comporter des rapports détaillés dans les domaines suivants

- Risque moyen par score et statut
- Risques par probabilité
- Risques les plus élevés par vendeur
- Risques par impact
- Risques communs identifiés
- Risques par domaine d'impact sur les entreprises
- Évolution du risque dans le temps par score/impact/vraisemblance
- Projection du score/impact/vraisemblance du risque dans le temps

La visualisation du statut de conformité et de risque dans le paysage des fournisseurs avec des vues exécutives intégrées fournit une visibilité spécifique et globale du profil de risque des tiers pour un rapport plus fiable au conseil d'administration.

L'analyse identifie les exceptions dans les comportements courants - par exemple les valeurs aberrantes dans les évaluations, les tâches, les risques, etc. - qui pourraient justifier une enquête plus approfondie. Veillez à vérifier si la solution que vous avez choisie dispose d'une **analyse d'apprentissage automatique** permettant de corréler des ensembles de données complexes et de déceler des tendances potentiellement cachées.



## Les 10 principales capacités de signalement et de correction :

1. Orientations intégrées en matière de remédiation, avec des recommandations visant à accélérer le processus d'atténuation des risques.
2. Un cadre de rapport unifié qui vous permet de prendre les réponses à n'importe quelle question et de les faire correspondre à n'importe quel cadre réglementaire ou industriel standard, ligne directrice ou méthodologie.
3. Rapports de conformité réglementaire, de cadre et de lignes directrices spécifiques comme pour le CMMC, ISO 27001, NIST, GDPR, CoBiT 5, SSAE 18, SIG, SIG Lite et NYDFS.
4. Capacité à montrer le pourcentage de conformité pour démontrer les progrès réalisés dans les efforts d'atténuation des risques.
5. Rapports détaillés par fournisseur et pour l'ensemble des fournisseurs.
6. Projection de la notation des risques dans le temps après que les mesures correctives ont été prises et que les risques ont été atténués.
7. Flux de travail et billetterie pour automatiser les communications.
8. Faites des rapports sur plusieurs réglementations en matière de sécurité, de conformité et de confidentialité grâce aux modèles de rapport et aux statuts intégrés.
9. Tableaux de bord exécutifs et opérationnels.
10. Services de gestion du processus de remédiation pour les équipes concernées.

L'évaluation des risques des fournisseurs permet d'évaluer la conformité des fournisseurs aux exigences en matière de sécurité des données informatiques, de réglementation et de confidentialité. Avec une bibliothèque de plus de 50 évaluations standardisées, des capacités de personnalisation du contenu et un flux de travail intégré, la solution automatise tout, de la collecte et de l'analyse des enquêtes à l'identification et au rapport des risques.

## Étude de cas : Cancer Research UK réduit les risques pour accélérer la recherche qui sauve des vies grâce à des partenaires

Cancer Research UK est l'une des principales organisations caritatives de lutte contre le cancer au monde qui se consacre à sauver des vies par la recherche. L'organisation se débattait avec une approche manuelle de la gestion des risques des fournisseurs qui prenait beaucoup de temps et n'était pas évolutive. Il était donc difficile de produire les rapports nécessaires aux parties prenantes internes et de remédier efficacement aux risques, ce qui risquait d'entraver leur capacité à mener des recherches susceptibles de sauver des vies avec leurs partenaires fournisseurs. Grâce à la plateforme de gestion des risques des tiers (TPRM), Cancer Research UK a pu gagner du temps en programmant les enquêtes et en automatisant les réévaluations. Ils ont pu générer automatiquement des registres de risques et exploiter des outils de discussion intégrés pour simplifier la communication avec les partenaires et accélérer la remédiation des risques.

## Étape 5 : Programme continu, intelligent et automatisé

Vous avez réussi ! Vous avez dépassé le stress des pratiques fastidieuses manuelles de TPRM basées sur des feuilles de calcul et vous gérez maintenant tous vos fournisseurs en un seul endroit ; vous êtes sorti de la prison des feuilles de calcul ; vous prenez des décisions plus fondées ; vous pouvez régler ce qui est important. L'étape finale de l'évolution vers un programme TPRM plus proactif consiste à atteindre un niveau d'automatisation continu et intelligent - ou à évaluer, contrôler et éliminer les risques des fournisseurs de manière proactive et continue. Mais à quoi ressemble un programme continu, intelligent et automatisé ?

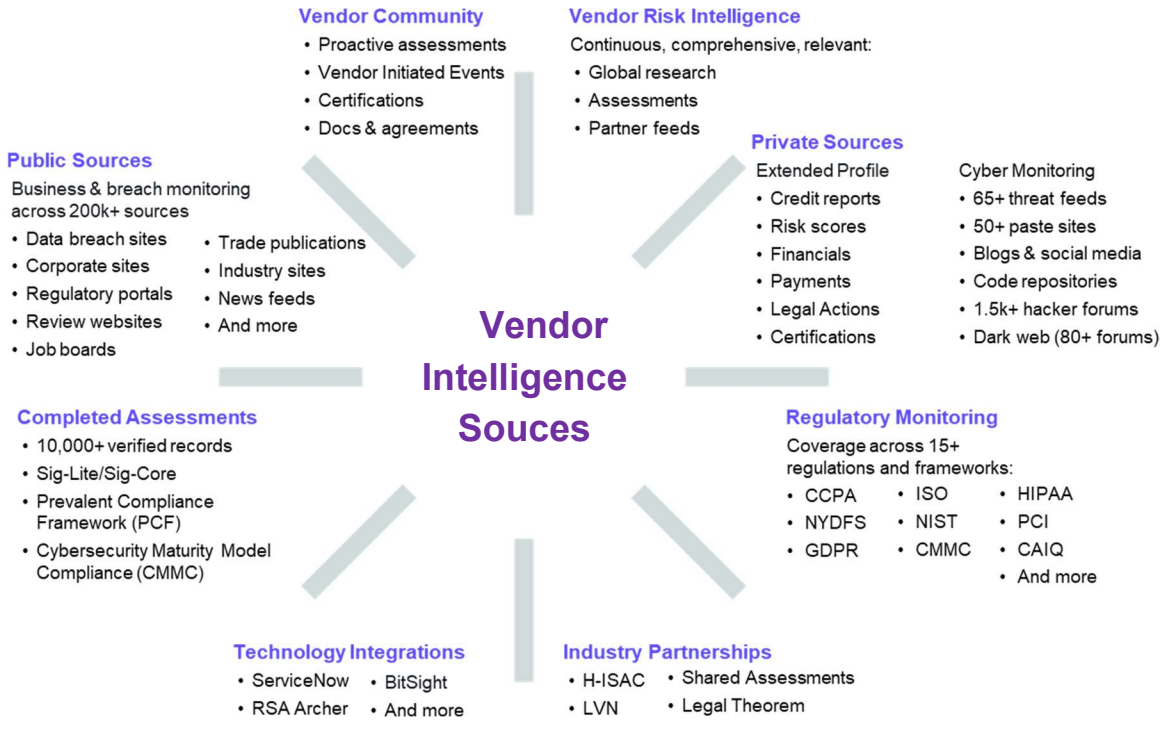
### Évaluations continues

Une façon de parvenir à un modèle d'évaluation plus continu et moins réactif est de permettre une surveillance en temps réel des cyber-entreprises et des entreprises pour informer votre calendrier d'évaluation. Un exemple : Une fois les règles en place, vous pouvez établir une corrélation entre les vulnérabilités d'un fournisseur, les violations ou les fuites d'informations sur le dark web découvertes grâce à la surveillance continue et les réponses aux évaluations révélant une gestion des mots de passe ou des pratiques de gestion des correctifs faibles et utiliser les résultats pour déclencher des évaluations. Ce niveau d'automatisation ferme véritablement la boucle du risque tiers et transforme les évaluations ponctuelles en surveillance continue du risque.

### Des renseignements de toutes parts

Prendre des décisions judicieuses en fonction des risques signifie consommer et normaliser des données provenant d'une myriade de sources. Le diagramme ci-dessous illustre les données nécessaires pour prendre de bonnes décisions fondées sur le risque.

*Figure 2 : Sources de renseignements pour les évaluations*



Les **sources publiques** et **privées**, les **renseignements sur les risques liés aux fournisseurs et l'intégration des technologies** peuvent éclairer la prise de décision fondée sur les risques en fournissant des informations quantitatives et qualitatives sur la santé cybernétique et commerciale d'un fournisseur - des risques potentiels de sécurité aux problèmes financiers.

La **communauté des fournisseurs**, les **évaluations réalisées** et les **partenariats industriels** jouent également un rôle, car ils fournissent une documentation et des informations fournies par les membres ou par la communauté, qui peuvent donner un aperçu des risques auxquels une industrie est confrontée.

La **surveillance réglementaire** fournit des informations sur les principales défaillances de contrôle auxquelles sont confrontées les entreprises dans les secteurs réglementés et peut aider à anticiper les mesures correctives à recommander à l'organisation de les mettre en œuvre pour réduire leur risque résiduel.

## Automatisation des playbooks pour rationaliser la réponse aux risques

De nombreuses organisations sont confrontées à des processus d'évaluation des fournisseurs basés sur des feuilles de calcul qui nécessitent des dizaines d'étapes manuelles pour analyser les réponses et agir en conséquence. Si la plupart des solutions TPRM servent à simplifier le processus, beaucoup ne proposent pas de règles permettant d'automatiser davantage l'identification et la gestion des risques.

Un moyen de parvenir à un programme plus automatisé est de tirer parti des capacités de déclenchement d'actions de réaction aux risques sur la base de critères "Si ceci, alors cela" pour des entités et des risques spécifiques. Les règles devraient automatiser un large éventail de tâches d'intégration, d'évaluation et d'examen - telles que la mise à jour des profils des fournisseurs et des attributs de risque, l'envoi de notifications et/ou l'activation de flux de travail. Elles devraient également fonctionner en permanence pour mettre à jour dynamiquement l'environnement du TPRM à mesure que de nouveaux événements et risques apparaissent.

### Top 6 des capacités continues, intelligentes et automatisées :

1. Évaluations proactives et progressives déclenchées par des aperçus et des résultats de suivi continu.
2. Mises à jour et notifications d'événements proactives et progressives.
3. Surveillance, notation et alerte en continu.
4. Activation de l'action - playbooks automatisés.
5. Bibliothèque des règles et des actions de renseignement.
6. Analyse et détection comportementales avec analyse multidimensionnelle.

Les services de conseil et de consultation courants vous mettent sur la bonne voie pour atteindre la maturité en matière de gestion des risques de tiers avec un minimum de tracas. Nous offrons un large éventail de services de planification, d'installation et de configuration, de transfert de connaissances et d'optimisation pour répondre à vos besoins informatiques et commerciaux spécifiques.

# Prevalent - notre différence

Nous pensons que notre différenciation sur le marché de la gestion des risques de tiers réside dans la plate-forme intégrée, la profondeur de notre offre de solutions et la valeur que vous obtenez grâce à notre expérience du secteur. Chaque facteur de différenciation est examiné ci-dessous.

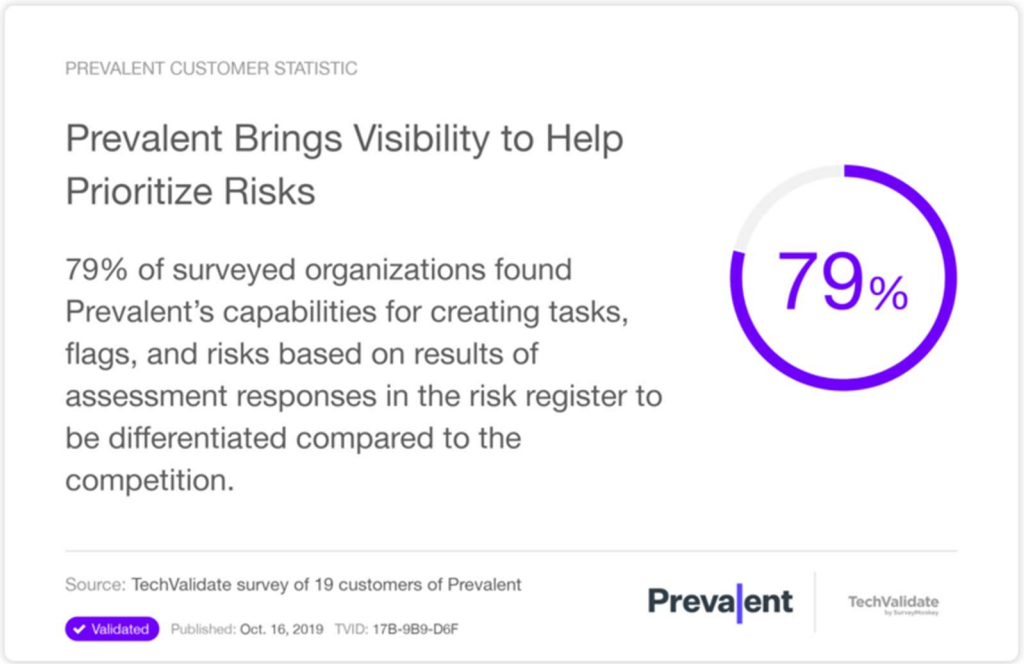
## Différentiateur n°1 : Visibilité sur les risques des fournisseurs pour aider à prendre de meilleures décisions

**Résultat commercial : Prevalent offre une vision claire des risques liés aux fournisseurs, tant à l'intérieur qu'à l'extérieur, avec des informations exploitables pour améliorer la prise de décision sur les priorités, les ressources et la conformité.**

La vieille maxime est vraie : on ne peut pas gérer ce qu'on ne peut pas mesurer - et on ne peut pas mesurer ce qu'on ne peut pas voir. Donc, sans visibilité des risques que vos fournisseurs et vendeurs tiers font courir à votre organisation, vous êtes confronté :

- Des rapports insuffisants ou peu clairs sur le respect des normes, ce qui peut entraîner des manquements a la règlementation ou des risques non vus
- La production de rapports d'audit est trop complexe, ce qui peut retarder l'élimination des risques critiques pour l'entreprise
- Coûts inutiles découlant des enquêtes et des mesures correctives prises pour résoudre les problèmes de conformité

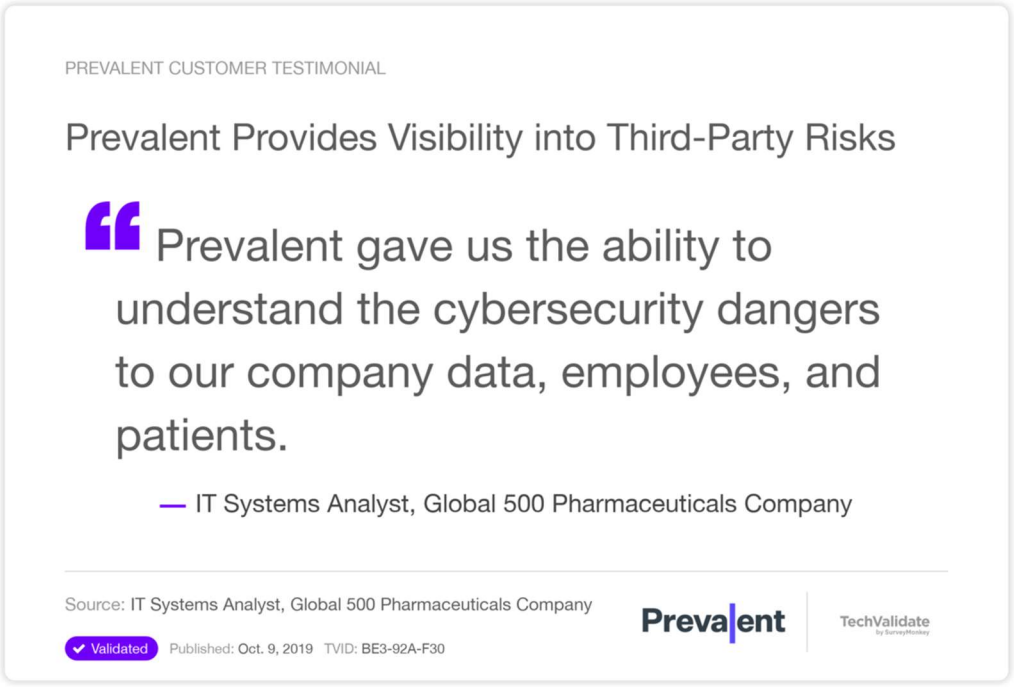
Dans une enquête réalisée en octobre 2019, les clients ont indiqué que les capacités de Prevalent à identifier et à mesurer les risques - par exemple grâce à la fonction de registre consolidé des risques - ont constitué un facteur de différenciation concurrentiel par rapport à d'autres options sur le marché de la gestion des risques par des tiers.



Ce facteur de différenciation était important pour une entreprise pharmaceutique du Global 500 basée aux États-Unis :

- Obtenir un meilleur reporting par rapport à des exigences réglementaires ou sectorielles spécifiques
- Améliorer la cybersécurité pour s'assurer que les tiers n'introduisent pas de cyber-risques qui pourraient avoir un impact négatif sur l'entreprise
- Réduire la charge opérationnelle (le processus d'évaluation des fournisseurs a pris trop de temps et de ressources)
- Obtenir davantage de renseignements fondés sur les risques

Pour relever ces défis, ils se sont tournés vers Prevalent. Selon les termes de leur analyste des systèmes informatiques :



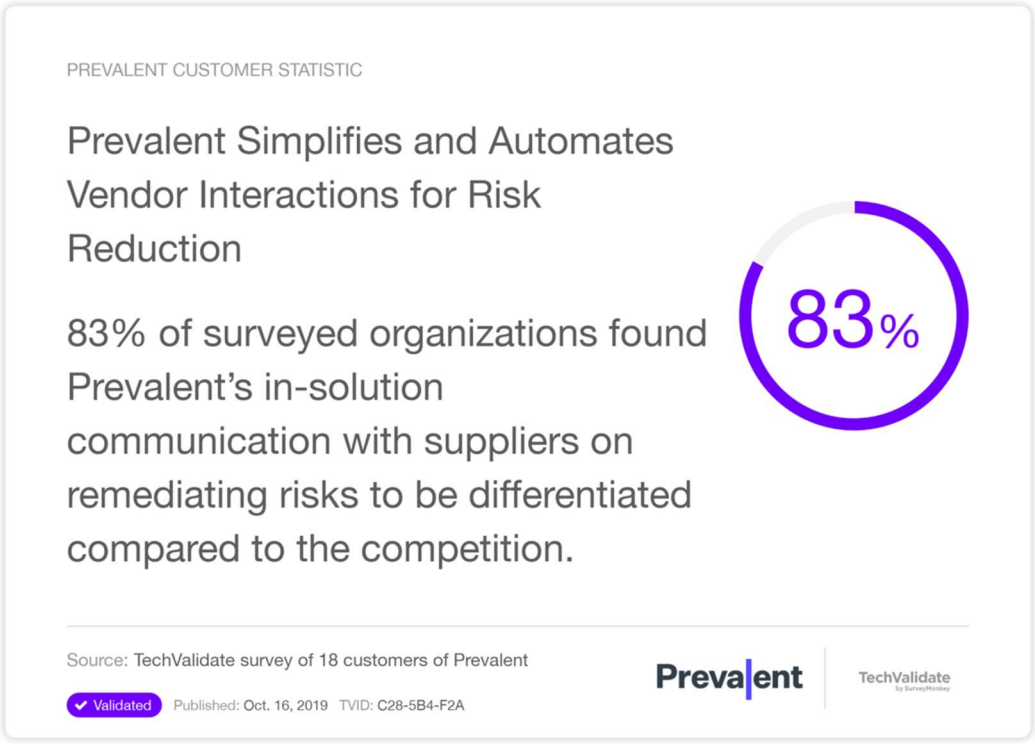
## Différentiateur n°2 : l'automatisation pour concentrer les équipes sur la gestion des risques, et non sur les tâches administratives

**Résultat commercial : Prevalent propose un processus plus rapide, plus précis et moins coûteux pour évaluer les risques que présentent les relations commerciales avec des tiers.**

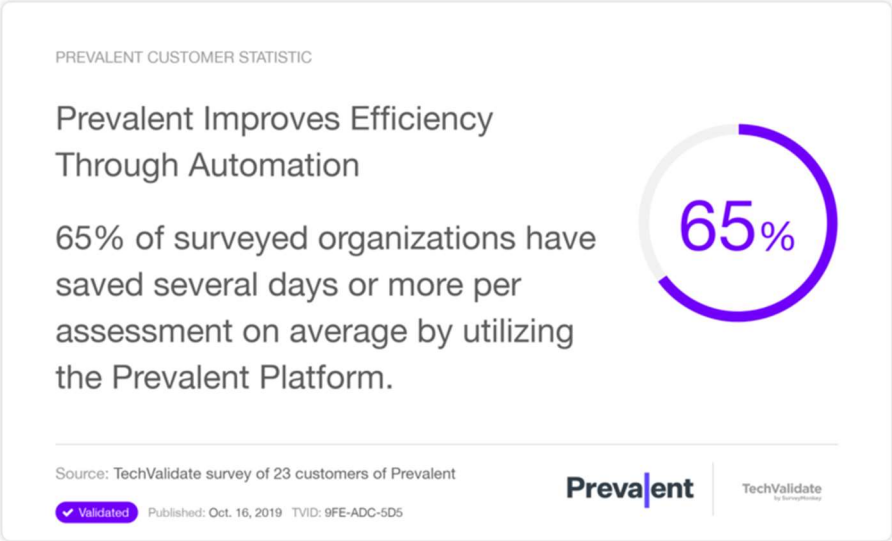
L'ancienne méthode d'évaluation des risques des fournisseurs ressemblait à ceci :

> *Déterminer les fournisseurs à évaluer. Concevoir un questionnaire pour évaluer le vendeur. Envoyer le questionnaire au vendeur par courrier électronique. Recevoir le questionnaire du vendeur par courrier électronique. Demander au vendeur de plus amples informations par courrier électronique. Et plus d'informations. Attendre. Attendre encore. Recevoir les réponses du vendeur. Remplir la feuille de calcul. Télécharger vers SharePoint. Dire au vendeur où il manque de contrôles et où il faut remédier à la situation. Effectuer une validation. Faire un rapport sur ces contrôles. Répéter l'opération pour le prochain <insérer le numéro ici> fournisseurs. Puis recommencer l'année prochaine.*

Avec Prevalent, les clients ont récupéré un temps considérable dans leur processus de gestion du risque fournisseur grâce aux capacités d'automatisation de la plate-forme. Les clients estiment que les communications au sein de la solution, la programmation et les rappels de poursuite automatisés, ainsi qu'un tableau de bord facile à utiliser pour les utilisateurs et les fournisseurs, sont des facteurs de différenciation concurrentielle par rapport aux autres options sur le marché de la gestion des risques des tiers.



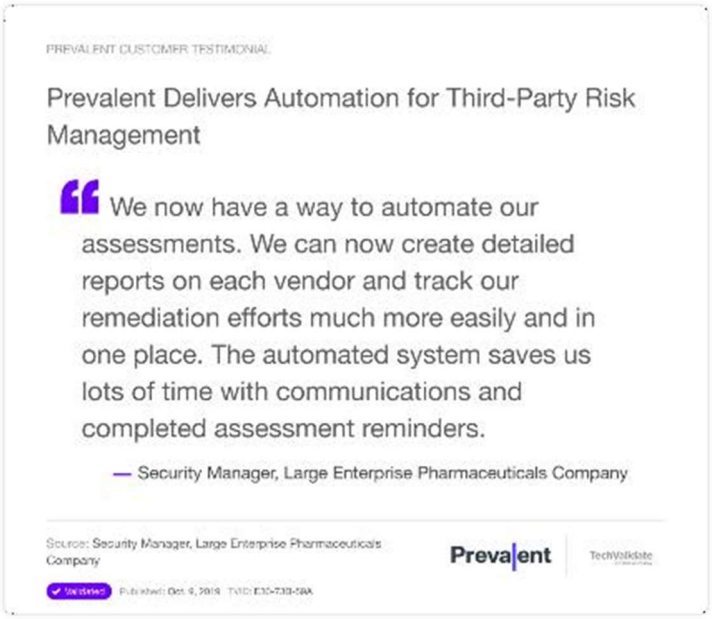
Combien de temps les clients habituels ont-ils gagné ? Plusieurs jours ou plus selon 65% des clients.




L'automatisation était importante pour une [grande entreprise pharmaceutique ] basée aux États-Unis qui bénéficiait des capacités de Prevalent, notamment

- Calendrier des évaluations et rappels automatisés des poursuites
- Gestion centralisée des documents et des preuves
- Communication avec les fournisseurs sur la résolution des

risques Selon les termes de leur responsable de la sécurité :



## Différentiateur n°3 : un processus mature pour permettre la scalabilité

**Résultat commercial : Prevalent offre un programme évolutif et plus mature.**

L'amélioration de la visibilité des risques et l'automatisation des processus de gestion de ces risques devraient déboucher sur un programme de gestion des risques par des tiers, évolutif et construit à partir de la base pour s'adapter et changer en fonction des besoins de l'entreprise.

Dans une enquête réalisée en octobre 2019, les clients ont indiqué que les capacités de Prevalent à apporter un processus cohérent à leurs programmes de gestion des risques des tiers constituaient un facteur de différenciation concurrentiel par rapport aux autres alternatives sur le marché de la gestion des risques des tiers. En fait, les capacités de Prevalent aident à automatiser leurs programmes à tel point que presque tous les répondants indiquent qu'ils peuvent augmenter leurs évaluations au cours de l'année suivante, ce qui les aide à faire évoluer leurs programmes.


L'automatisation était importante pour une entreprise de services professionnels de taille moyenne basée aux États-Unis qui était contestée par :

- Une capacité limitée à surveiller en permanence les fournisseurs
- Un manque d'orientation pour répondre aux normes industrielles ou aux exigences de conformité réglementaire des tiers en matière de risque cybernétique, d'InfoSec ou de confidentialité des données
- N'ayant pas de centralisation des fonctions du TPRM

Selon les termes de l'entreprise : *"Avec Prevalent, mon organisation a pu réorienter vers d'autres activités les ressources auparavant consacrées à la collecte et à l'analyse des questionnaires et des preuves soumis par les fournisseurs".*

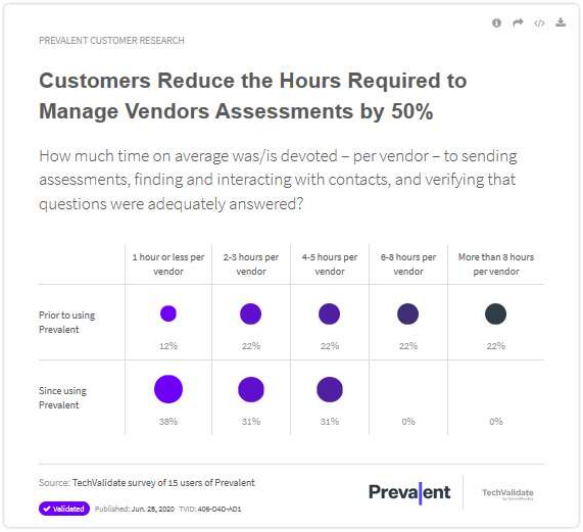
## Différentiateur n°4 : un retour sur investissement tangible et prouvé

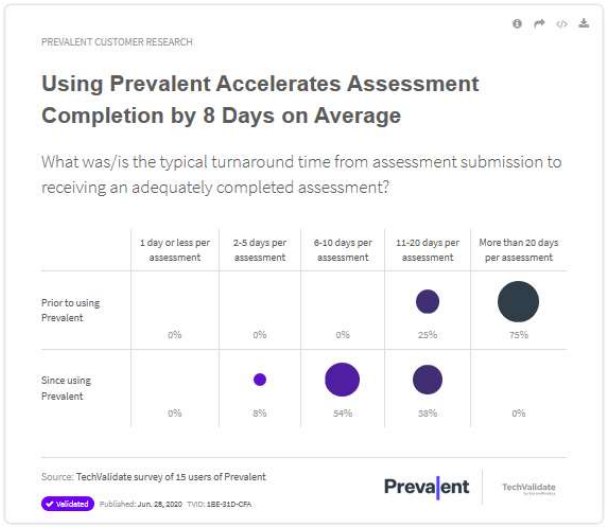
**Résultat commercial : Le résultat opérationnel : Prevalent réduit le temps et le coût généralement nécessaires pour atteindre les résultats visés en matière de réduction des risques.**

L'analyse de rentabilité pour l'achat d'une nouvelle solution peut être complexe. Les entreprises doivent donc être en mesure de démontrer un retour sur investissement tangible afin de justifier les coûts de changement. Ce qui distingue Prevalent de la concurrence est la capacité à prouver le retour sur investissement des améliorations susmentionnées en termes de visibilité, d'efficacité et d'échelle.

Dans une enquête réalisée en juin 2020, les clients ont quantifié les avantages que leurs entreprises réalisent en utilisant Prevalent pour automatiser leurs programmes TPRM dans des domaines tels que la réduction des délais, la productivité et la rapidité des évaluations. En moyenne, Prevalent aide les clients à :

- Réduire **de 50 %** le temps nécessaire à la gestion des fournisseurs et des évaluations
- Gagner **8 jours par vendeur pour** réaliser des évaluations concurrentielles
- Améliorer la productivité des équipes par **un facteur de 3**




La productivité de l'équipe était importante pour Wright Express, un fournisseur de services de traitement des paiements et de gestion de l'information pour l'industrie américaine des parcs de véhicules commerciaux et gouvernementaux, qui était confronté à un processus long et fastidieux de collecte de données sur les fournisseurs.

Selon les mots de Jacob Gregiore, officier de sécurité :


## Conclusion : Apporter une valeur ajoutée aux entreprises

Ce guide des bonnes pratiques explique à quoi ressemble un déploiement TPRM d'entreprise et décrit les principales caractéristiques à rechercher dans le processus d'évaluation de la solution. Prevalent est l'exemple même d'une solution complète de gestion des risques de tiers, offrant un programme TPRM holistique et automatisé, unifié par une plate-forme unique et facile à utiliser. Avec Prevalent, vous gagnez :

- **Une plus grande visibilité**
  - Plus de prévisibilité : Établir un processus reproductible pour l'évaluation des fournisseurs.
  - Des décisions plus fondées : Obtenez des renseignements en temps réel pour prendre des décisions mieux informées et fondées sur les risques.
- **Un temps plus rapide à valoriser**
  - De meilleurs résultats, plus rapidement : Commencez rapidement, gagnez du temps et obtenez rapidement des résultats.
  - Moins de maux de tête : Réduire le travail manuel, et accélérer la collecte et l'analyse des enquêtes.
- **Faites plus avec les ressources dont vous disposez**
  - Faites-en plus : Ajoutez de l'échelle sans ajouter de ressources.
  - Un meilleur travail d'équipe : Collaborer en interne et avec les fournisseurs dans un environnement centralisé.

Contactez Acensi dès aujourd'hui pour une session de stratégie sur la maturation de votre programme TPRM et la résolution de vos problèmes de risques liés aux tiers.

## Annexe : Liste de contrôle pour la comparaison des fournisseurs de solutions

Utilisez ce tableau pour évaluer votre programme de gestion des risques par des tiers et comparer les fournisseurs de solutions.

| Étape | Attribut | Options | Prevalent | Vendeur B | Vendeur C |
|---|---|---|---|---|---|
| **Gérer tous les vendeurs en un seul endroit** | API et connecteurs vers des solutions communes pour automatiser l'intégration. | | | | |
| | Modèle pour programmer l'intégration des fournisseurs. | | | | |
| | Évaluation et logique de profilage et de hiérarchisation pour mettre en œuvre une méthodologie reproductible d'évaluation des fournisseurs. | | | | |
| | Evaluation et suivi des risques inhérents et résiduels afin d'identifier clairement les fournisseurs qui présentent les risques les plus importants pour l'entreprise. | | | | |
| | Services permettant d'embarquer et de trouver de nouveaux fournisseurs pour les équipes aux ressources insuffisantes. | | | | |
| **Sortir de la prison des tableurs** | Bibliothèque de centaines de milliers de profils de fournisseurs vérifiés, permettant d'identifier, d'embarquer et d'évaluer les risques plus rapidement et avec moins de ressources. | | | | |
| | Le plus grand nombre de modèles d'évaluation préétablis et prêts à l'emploi pour garantir que les fournisseurs sont évalués de manière flexible et en fonction du mandat ou du cadre qui est important pour l'entreprise. | | | | |
| | Assistant de création d'évaluations personnalisées offrant une certaine souplesse pour évaluer les fournisseurs en fonction de leurs exigences particulières. | | | | |
| | Automatisation des flux de travail et des tâches pour accélérer le processus d'évaluation. | | | | |

| | | | | |
|---|---|---|---|---|
| | Documents, contrats, accords et preuves centralisés, constituant un dépôt pour plusieurs équipes. | | | |
| | Des rapports prêts à l'emploi sur de multiples exigences de conformité et de cadre en utilisant un seul questionnaire pour alimenter les réponses, ce qui permet de gagner du temps. | | | |
| | Options permettant d'externaliser la conception du questionnaire ainsi que la collecte et l'analyse des données probantes à des experts afin de remédier à la pénurie de ressources. | | | |
| **Soyez plus intelligent** | La cyber-surveillance à partir du deep/dark web pour obtenir des informations en temps réel sur les risques. | | | |
| | Surveillance des entreprises à partir de centaines de milliers de sources fournissant des informations sur les questions commerciales, réglementaires ou juridiques. | | | |
| | API RESTful pour permettre les connexions à d'autres systèmes. | | | |
| | Un registre des risques unifié qui établit une corrélation entre les risques cyber et commerciaux et les résultats de l'évaluation de chacun de vos fournisseurs, ce qui permet de valider les données de contrôle communiquées par les fournisseurs. | | | |
| | Transformez les données des cyber-événements et des événements commerciaux des fournisseurs entrants en risques actionnables, en vous donnant une visibilité des risques en temps réel. | | | |
| | Déclencher des actions telles que l'envoi de notifications, la création de tâches ou de flags, ou l'élévation des notes de risque, accélérant ainsi le processus d'atténuation des risques. | | | |
| | Des pondérations de risques flexibles qui définissent de manière granulaire l'importance de risques spécifiques pour l'entreprise. | | | |

| | | | | |
|---|---|---|---|---|
| | Le marquage et la catégorisation - automatique ou manuelle - pour faire remonter un risque et l'acheminer vers le contact approprié pour y remédier. | | | |
| | Une matrice qui permet d'analyser dynamiquement les risques en fonction de la probabilité d'un incident et de son impact potentiel sur l'entreprise. | | | |
| **Corriger ce qui est important** | Orientations intégrées en matière de remédiation, avec des recommandations visant à accélérer le processus d'atténuation des risques. | | | |
| | Un cadre de rapport unifié qui vous permet de prendre les réponses à n'importe quelle question et de les faire correspondre à n'importe quel cadre réglementaire ou industriel standard, ligne directrice ou méthodologie. | | | |
| | Rapports de conformité réglementaire, de cadre et de lignes directrices spécifiques comme pour le CMMC, ISO 27001, NIST, GDPR, CoBiT 5, SSAE 18, SIG, SIG Lite et NYDFS. | | | |
| | Capacité à montrer le pourcentage de conformité pour démontrer les progrès réalisés dans les efforts d'atténuation des risques. | | | |
| | Rapports détaillés par fournisseur et pour l'ensemble des fournisseurs. | | | |
| | Projection de la notation des risques dans le temps après que les mesures correctives ont été prises et que les risques ont été atténués. | | | |
| | Workflow et remontée des incidents pour automatiser les communications. | | | |
| | Faire des rapports sur plusieurs réglementations en matière de sécurité, de conformité et de confidentialité grâce aux modèles de rapport et aux statuts intégrés. | | | |
| | Tableaux de bord exécutifs et opérationnels. | | | |
| | Services de gestion du processus de remédiation pour les équipes concernées. | | | |

| Étape | Attribut | Options | Prévalent | Vendeur B | Vendeur C |
|---|---|---|---|---|---|
| **Être proactif en continu** | Évaluations proactives et progressives déclenchées par des aperçus et des résultats de suivi continu. | | | | |
| | Mises à jour et notifications d'événements proactives et progressives. | | | | |
| | Surveillance, notation et alerte en continu. | | | | |
| | Playbooks automatisés. | | | | |
| | Bibliothèque des règles et des actions de renseignement. | | | | |
| | Analyse et détection comportementales avec analyse multidimensionnelle. | | | | |

## À propos de Prevalent

La plupart d'entre eux se soucient de la gestion des risques par des tiers (TPRM). Les entreprises utilisent nos logiciels et services pour éliminer les risques de sécurité et de conformité qui découlent de la collaboration avec les vendeurs, les fournisseurs et autres tiers. Nos clients bénéficient d'une approche flexible et hybride de la gestion des risques des tiers, qui leur permet non seulement d'obtenir des solutions adaptées à leurs besoins, mais aussi de réaliser un retour sur investissement rapide. Quel que soit leur point de départ, nous aidons nos clients à arrêter la douleur, à prendre des décisions éclairées, à adapter et à faire mûrir leurs programmes TPRM au fil du temps.
www.prevalent.net

## À propos de Acensi Cyber

Le groupe ACENSI accompagne plus de 200 clients dans la gestion de leurs projets informatiques depuis 2003 avec plus de 1 500 employés à travers le monde.

ACENSI Cyber est un incubateur de sécurité informatique qui teste des centaines de solutions chaque année afin de pouvoir aligner la technologie et les services d'ACENSI sur les besoins clients. Nous sommes l'un des rares incubateurs technologiques en France et au BENELUX qui dispose de compétences techniques et de support dans le pays, englobant des solutions cyber, des services professionnels, des formations, du support et des offres de services managés. Nous permettons à nos clients de protéger leurs infrastructures, assets, données et utilisateurs contre les menaces actuelles et émergentes. Dans l'environnement actuel, il est plus important que jamais pour les entreprises de comprendre et d'atténuer les risques liés aux tiers. Avec Prevalent, nos clients disposent de la technologie et des services combinés à notre expertise pour les aider à réduire les risques et protéger leur organisation contre les activités malveillantes.

www.acensisec.com