TANIUM

# Ce que vous ignorez peut vous nuire

## Conseils d'experts pour évaluer les risques

Des conseils et recommandations de spécialistes pour évaluer les risques dans les environnements évolutifs et hautement distribués d'aujourd'hui.

TANIUM

# Ce que vous ignorez peut vous nuire : conseils d'experts pour évaluer les risques

**Des conseils et recommandations de spécialistes pour évaluer les risques dans les environnements évolutifs et hautement distribués d'aujourd'hui.**

## Contenu





# Conseils d'experts pour évaluer les risques

## Pour gérer les risques, il faut d'abord les mesurer.

Mais comment faites-vous pour mesurer les risques efficacement ? Devriez-vous identifier chaque vulnérabilité logicielle dans l'entreprise ? Ou dresser une liste de tous les appareils d'endpoints ayant besoin des correctifs logiciels ? Ou signaler les statistiques de disponibilité pour les applications les plus critiques de votre entreprise ?

Lorsque votre rôle est de mesurer le risque, vous devez vous concentrer sur l'essentiel selon l'entité à laquelle vous vous adressez. Ici, il est question des décisions essentielles en matière de risque : la direction et le conseil d'administration sont donc vos interlocuteurs de choix.

Trois experts informatiques partagent avec vous leurs connaissances de l'évaluation des risques dans cet eBook, dans un format complet, pratique et exploitable.

Leurs conseils sont résumés dans une liste de contrôle à la fin de l'eBook. *Commençons.*

# Mesurer l'essentiel : aligner la mesure des risques sur les buts et objectifs de l'entreprise

Les experts en sécurité informatique sont formels : le risque est omniprésent : endpoints non corrigés, nouvelles variantes de programmes malveillants, attaques de phishing, services cloud fantômes, ordinateurs portables à l'abandon dans les parcs... Votre équipe de gestion des risques se demande peut-être comment aborder la tâche cruciale de mesure des risques dans votre entreprise, lorsque tant de détails techniques contribuent à sa vulnérabilité.

De toute évidence, mesurer le risque n'est pas une fin en soi. Les évaluations des risques sont menées pour fournir des informations aux décideurs. La vraie question est donc la suivante : Comment mesurer le risque de manière à aider les responsables de votre organisation, la direction et le conseil d'administration à comprendre le risque afin qu'ils puissent prendre les bonnes décisions pour le réduire ?

## Mesurer les risques importants pour la direction de votre entreprise

Pour répondre à cette question, commençons par le début. L'équipe de direction et le conseil d'administration doivent définir l'orientation stratégique de votre entreprise. Le rôle consiste notamment à s'assurer que les décisions et investissements pris dans toute l'organisation soutiennent les objectifs stratégiques clés de l'entreprise.

Quelle que soit l'activité de votre entreprise, ces objectifs de haut niveau comprennent presque toujours les éléments suivants :

- Continuité des activités
- Confidentialité, intégrité et disponibilité des données (CID des données)
- Conformité réglementaire

Examinons-les.

## Mesurer le risque associé à la continuité des activités

Lorsque la continuité des activités est assurée, les employés restent productifs, les opérations de fabrication et d'expédition continuent sans interruption, de même que tout autre type d'opération : extraire du pétrole, livrer un produit SaaS...

La reprise après sinistre fait partie cette catégorie. Il en va de même pour la protection des services stratégiques contre les cybermenaces.

## Mesurer le risque associé à la confidentialité, l'intégrité et la disponibilité des données

Dans tous les secteurs, on reconnaît l'importance des données. Ce « nouveau pétrole » de l'économie numérique a autant de valeur que la protection des données confidentielles.

Les défis liés à la sécurisation de ces données se sont multipliés. D'une part, les données sensibles sont plus accessibles que jamais depuis l'émergence du télétravail, avec des employés qui utilisent de plus en plus leur propre appareil selon l'approche BYOD (apportez votre propre appareil). Les ordinateurs portables et de bureau testés et provisionnés par le service informatique sont moins répandus.

Les entreprises doivent garantir la confidentialité, l'intégrité et la disponibilité des données, peu importe où et comment les employés accèdent à ces données. Dans certaines équipes informatiques, on parle même de « CIA des données ».

## Mesurer le risque associé à la conformité réglementaire

La confidentialité des données doit nous évoquer les réglementations en vigueur, comme le RGPD et l'HIPAA, qui exigent la protection des données personnelles.

Mais ces réglementations couvrent tous les sujets, des rapports financiers à la discrimination ethnique, et les entreprises ne peuvent pas se permettre de les enfreindre. Le non-respect des réglementations peuvent entraîner de lourdes amendes financières, l'annulation de contrats et nuire durablement à votre réputation.

Pour mesurer efficacement les risques, vous devez savoir quelles réglementations sont importantes pour la direction de votre entreprise. Ensuite, vous devez suivre les actifs et processus informatiques qui aident à déterminer si votre entreprise respecte ces réglementations.

## Encadrer le risque à l'aide d'objectifs stratégiques

Il incombe à l'équipe de direction et au conseil d'administration de diriger l'entreprise pour atteindre ses principaux objectifs en matière de continuité des activités, de confidentialité des données et de conformité réglementaire. Bien sûr, l'entreprise peut être amenée à atteindre d'autres objectifs, notamment liés à un taux de croissance annuel ou à la culture d'entreprise.

Si vous souhaitez attirer l'attention de ces responsables, cadrez votre discussion sur les mesures des risques en fonction des objectifs au niveau du conseil d'administration de votre entreprise. En d'autres termes, identifiez et évaluez les différents risques techniques, réglementaires et liés à d'autres domaines pour votre entreprise, et mettez en évidence leur lien avec les objectifs stratégiques de haut niveau.

En encadrant vos mesures de risque de cette manière, vous vous concentrez sur votre travail. En outre, votre mission sera mieux comprise et appréciée par les dirigeants d'entreprise qui dessinent les orientations futures de votre société.

# Mesurer le risque en identifiant les chaînes d'approvisionnement de valeur

Dans ce chapitre, nous aborderons plus en détail la mesure des risques par rapport aux objectifs de l'entreprise, en discutant de l'importance des échelles pondérées pour divers risques et même pour les objectifs eux-mêmes.

## Identifier les risques associés aux objectifs stratégiques

La mesure des risques commence par l'identification des objectifs stratégiques de votre entreprise, puis l'exploration des personnes, des processus et de la technologie qui soutiennent la poursuite de ces objectifs par votre entreprise.

Considérez-la comme une analyse de la chaîne d'approvisionnement. Vous suivez le flux de données, de personnes et d'opérations depuis un objectif de haut niveau jusqu'à des systèmes et processus informatiques spécifiques qui aident l'entreprise à atteindre cet objectif. Ces systèmes et processus fonctionnent comme une sorte de chaîne d'approvisionnement pour les objectifs eux-mêmes.

Pour mesurer le risque, identifiez les dépendances dans cette chaîne d'approvisionnement et créez des liens pertinents selon les objectifs et capacités de votre entreprise. Pour comparer les risques au sein de la chaîne d'approvisionnement elle-même, un score doit être attribué à tout ce qui la compose.

## Élaboration d'une échelle pondérée pour les risques

Même les objectifs stratégiques eux-mêmes doivent être comparés et pondérés. Les objectifs stratégiques d'une entreprise sont rarement traités de manière égale.

Une fois que vous avez identifié ces objectifs, attribuez-leur des notes sur une sorte d'échelle, telle que 1 à 10. À l'aide de vos conversations avec l'équipe de direction, vous pouvez attribuer un score de 10 à une croissance continue du chiffre d'affaires d'au moins 10 % et un score de 7 pour la conformité réglementaire.

Ensuite, identifiez les personnes, les processus et la technologie qui permettent de soutenir chaque objectif stratégique, et classez-les selon leur importance, selon l'aide qu'ils apportent.

Apportez même des nuances, en estimant la probabilité d'apparition de certains types de défaillances. Prenons l'exemple suivant : votre entreprise dispose d'un serveur Web prenant en charge une application mobile stratégique pour l'entreprise. Des performances anormalement lentes pendant un pic d'utilisation seraient sans doute plus probables qu'une coupure de courant qui entraînerait un plantage des systèmes d'alimentation principaux et secondaires.

Vous pouvez commencer à classer les risques et à identifier les risques qui nécessitent une action plus immédiate en multipliant un score pour l'importance stratégique du serveur (par exemple, 7 sur 10) par la probabilité d'un risque spécifique (par exemple, 50 % ou 0,5).

Par exemple, le serveur aux performances lentes peut avoir une probabilité de 40 %, et le serveur qui subit une panne de courant majeure peut avoir une probabilité de 2 %. Le score de risque pour le scénario de performance lente serait de 7 x 0,40, c'est-à-dire 2,8 si l'importance du serveur est évaluée à 7 sur 10. Le score de risque pour le scénario de panne de courant s'élèverait à 7 x 0,02, c'est-à-dire 0,14). Le scénario de ralentissement des performances, associé au score de risque le plus élevé, doit évidemment être prioritaire.

## L'importance de la collaboration dans la mesure du risque

Pour réaliser ce type d'évaluation des risques, il faut collecter des informations détaillées sur les personnes, les processus et la technologie dans toute l'entreprise. Le service informatique aura besoin d'aide.

Mon conseil ? Demandez de l'aide à chaque service dont vous évaluez les processus et la technologie. Par exemple, si souhaitez vraiment comprendre les risques associés aux applications du service RH, parlez-en au personnel RH. Ces personnes peuvent connaissent mieux l'importance de leur application que l'équipe informatique.

Évitez le jargon technique lorsque vous vous adressez à des personnes extérieures au service informatique. De plus, ne préconisez jamais une méthode de travail à une personne sans lui demander au préalable comment, selon elle, une tâche devrait être réalisée. Si vous imposez votre solution, vous faites peut-être l'impasse sur une judicieuse alternative. De même, si vous appliquez une nouvelle politique sans tenir compte des idées extérieures, vous constaterez sans doute une certaine réticence à l'appliquer.

## La gestion des risques est une problématique de l'entreprise, et non seulement d'ordre informatique.

Lorsqu'une personne extérieure au service IT sentira que vous lui faites confiance et êtes réellement intéressé par leur opinion, elle s'exprimera plus librement face à vous. De plus, elle adoptera plus facilement les solutions de gestion des risques que vous avez mises en place ensemble.

Cette collaboration continue est l'un des avantages d'une approche axée sur la « chaîne d'approvisionnement » pour mesurer les risques. Vous découvrirez les informations dont vous avez besoin pour mesurer plus précisément les risques, et informerez également les parties prenantes de l'organisation sur l'importance de la mesure et de l'atténuation des risques. Et vous pourrez collaborer avec ces parties prenantes au développement de solutions pour minimiser les risques que vous avez tous deux identifiés.

CHAPITRE 3 :

# Moderniser l'évaluation des risques pour l'entreprise distribuée d'aujourd'hui

Autrefois, la mesure du risque était une évaluation ponctuelle réalisée par des consultants. Elle est aujourd'hui une pratique continue : les mesures sont plus précises, efficaces et permanentes grâce à l'automatisation et aux données en temps réel.

L'année dernière, le passage soudain à un modèle WFH a révolutionné l'informatique en entreprise, notamment en matière d'évaluation des risques.

Dans ce chapitre, nous examinons la méthode traditionnelle employée par les entreprises pour évaluer les risques. Ensuite, nous analysons le nombre d'entreprises qui ont conduit de telles évaluations depuis le début de la pandémie, et vous présentons quelques-unes des meilleures pratiques que les entreprises hautement distribuées d'aujourd'hui peuvent appliquer.

## Comment les risques et les évaluations des risques ont changé pendant la pandémie

De nombreuses organisations n'effectuaient des évaluations de risques qu'une seule fois par an. Les équipes d'évaluation des risques produisaient des rapports détaillés pour tenter de résumer tous les risques de l'organisation dans des domaines tels que la sécurité informatique, la reprise après sinistre et la conformité.

Afin de recueillir des informations pour leurs rapports, les équipes se rendaient dans les centres de données et distribuaient des questionnaires. Les évaluations reflétaient invariablement le risque à un moment donné même si les visites étaient scrupuleuses et les questionnaires approfondis.

Si, cinq minutes après le départ de l'équipe du centre de données, une nouvelle mise à niveau logicielle compromettait soudainement l'intégrité des rapports financiers de l'entreprise, le rapport d'évaluation des risques ne rendrait pas compte de l'augmentation du risque.

Pour de nombreuses organisations, l'évaluation des risques a été renforcée pendant la pandémie. Les questionnaires envoyés par e-mail ont remplacé les inspections en personne. Les parties prenantes ont rempli les formulaires avec diligence, mais personne ne savait précisément quels appareils et logiciels les employés utilisaient à distance.

Existe-t-il une meilleure façon de mener des évaluations des risques ? Dans ma carrière, j'ai passé beaucoup de temps à me concentrer sur la pratique des évaluations de risques, et je pense qu'il y en existe une.

## Adapter l'évaluation des risques à l'ère du cloud computing et du télétravail (WFH)

La ponctualité est la première piste d'amélioration pour l'évaluation des risques. La plupart du temps, les rapports seront imprécis s'ils reposent sur des données collectées une fois par an.

La vie économique s'intensifie à un rythme inédit. Données, appareils, logiciels, relations commerciales : tout s'opère en flux continu. Les évaluations de risques doivent s'adapter à cette nouvelle réalité.

Les services informatiques disposent heureusement de nouveaux outils qui peuvent aider à améliorer la précision des évaluations de risques. Par exemple, la surveillance des endpoints en temps réel peut saisir l'emplacement, l'état du système informatique et de l'activité des endpoints, y compris dans les bureaux de télétravail. Cette surveillance fonctionne sur des connexions Internet standard sans nécessiter de VPN.

Grâce à ces outils modernes, les organisations informatiques peuvent collecter des données des endpoints toujours plus complètes, à jour et précises, alors qu'autrefois, la plupart des endpoints étaient encore sur des réseaux internes, surveillés sporadiquement par des outils traditionnels de gestion des endpoints.

Ensuite, il faut mesurer le risque au fil du temps. L'équipe de direction veut savoir si les mesures d'atténuation des risques qui ont été mises en place fonctionnent. Les équipes de gestion des risques doivent suivre les indicateurs qui précisent si l'entreprise atteint ou non ses objectifs en la matière.

Enfin, il faut mener des discussions avec l'équipe de direction sur le risque, données à l'appui. C'est là que les données plus à jour et plus complètes portent leurs fruits. En bénéficiant d'une meilleure visibilité sur vos endpoints et autres actifs informatiques, vous pouvez avoir une discussion plus pertinente sur les investissements qui fonctionnent et ou non.

## Quatre éléments clés de la gestion des risques

Voici quatre étapes pour gérer les risques dans une entreprise moderne en gardant à l'esprit les objectifs stratégiques de votre organisation.

### 1. Collecte des données

Désigne la collecte de toutes les données nécessaires pour mesurer les risques liés aux objectifs stratégiques de votre organisation. Cela inclut évidemment les données des endpoints, ainsi que les données environnementales et des utilisateurs.

### 2. Analyse

Une fois les données collectées, automatisez autant que possible leur analyse. Si votre analyse repose sur plusieurs feuilles de calcul Excel et impressions papier, elle prendra plus de temps et comportera davantage d'erreurs. Si vous avez créé des tableaux de bord pour évaluer les risques, les automatiser et faire de l'analyse un processus continu sera bien plus efficace qu'une capture d'écran une fois par an.

### 3. Rapports

Cette étape implique de synthétiser les indicateurs de risque et l'analyse des rapports au niveau exécutif. Ces rapports guideront les discussions de votre organisation sur les risques, les priorités, les décisions d'investissement, et bien plus. Dans ces rapports, cadrez l'analyse des risques vis-à-vis des objectifs stratégiques au cœur des préoccupations de votre direction et conseil d'administration.

### 4. Remédiation

Il existe deux types de remédiation des risques. Tout d'abord, les mesures prises au quotidien par le personnel de sécurité et des opérations informatiques pour répondre aux menaces comme l'infiltration de programmes malveillants. Ces actions ne nécessitent pas l'approbation de l'équipe de direction. Et ensuite, les mesures prises par les responsables informatiques et commerciaux en réponse aux rapports de la direction créés au fil des trois premières étapes de ce processus. Les entreprises doivent mettre en œuvre les deux formes de remédiation des risques.

L'année dernière, de nombreuses entreprises ont gagné en flexibilité et distribuent maintenant sur un territoire plus étendu. Désormais, les entreprises ont également la possibilité de réinventer leurs processus d'évaluation des risques.

Les entreprises peuvent à la fois réduire les risques et améliorer la sécurité de leurs travailleurs distants en tirant parti l'automatisation et des données en temps réel.

CHAPITRE 4 :

# L'importance de faire de l'évaluation des risques un processus continu

Mesurer le risque n'est pas une mince affaire. Heureusement, les nouvelles technologies peuvent vous aider à automatiser l'évaluation des risques.

Le risque concerne toutes les organisations, mais son évaluation est plus difficile que jamais. Dans ce chapitre, nous en expliquons les raisons, et vous présentons une approche descendante de la mesure des risques qui peut vous simplifier la tâche et aider les organisations à prendre de meilleures décisions.

## Pourquoi la mesure du risque est devenue plus difficile

Pourquoi la mesure du risque est-elle si difficile de nos jours ? Voici quatre raisons.

### Difficulté n°1 : Des actifs informatiques disparates et variés

Il y a vingt ans, les évaluations des risques informatiques consistaient principalement à compter les PC et les serveurs des employés dans les centres de données, à examiner les vulnérabilités probables pour divers modèles de matériel et à produire un rapport.

Aujourd'hui, les actifs informatiques à inventorier et à analyser peuvent être distribués dans 50 bureaux, 500 centres de données (la plupart appartenant à d'autres entreprises) et 10 000 réseaux domestiques. Une part significative de cette architecture distribuée (au moins 20 %, selon toute probabilité) est constituée d'« informatique fantôme » : des produits et services que les employés ont adoptés sans approbation officielle ni supervision continue par le service informatique.

Dans cet environnement informatique hautement distribué et difficile à cataloguer, les outils et approches traditionnels de mesure des risques ne fonctionneront tout simplement pas.

## Difficulté n°2 : Complexité informatique

La complexité informatique est une deuxième raison pour laquelle l'évaluation des risques est difficile. En plus du nombre élevé d'appareils, la façon dont le logiciel est conçu et fonctionne a changé.

L'ère des applications monolithiques de grande taille est terminée. L'infrastructure informatique d'aujourd'hui comprend de nombreux composants de petite et moyenne taille qui œuvrent de concert pour former un ensemble plus grand.

Par exemple, le fonctionnement d'une application bancaire mobile peut reposer sur 75 composants différents, du code de l'interface utilisateur à plusieurs bases de données back-end. Les risques associés à chacun de ces composants ont un impact sur les risques liés à l'application dans son ensemble. C'est pourquoi les entreprises doivent disposer d'une **nomenclature logicielle en temps réel.**

## Difficulté n°3 : Attaques de sécurité sophistiquées

Troisièmement, les entreprises sont attaquées par un nombre croissant de cybercriminels, dont beaucoup ont accès à des technologies hautement sophistiquées.

Il y a vingt ans, les pirates informatiques étaient principalement des malfaiteurs, des programmeurs informatiques qui souhaitaient trouver des moyens ingénieux de causer des problèmes. Aujourd'hui, des États, organisations criminelles et « script kiddies » malveillants sont prêts à dépenser 50 dollars sur le Dark Web pour acheter un programme malveillant ou un script de credential-stuffing et une liste d'informations d'identification corrompues.

## Difficulté n°4 : Responsabilités partagées

Une dernière difficulté ? Une tendance récente dans la gestion des risques exige un partage plus large des risques avec les unités commerciales. L'organisation informatique peut diriger le projet d'évaluation des risques d'une organisation. Les équipes de direction et les conseils d'administration demandent désormais aux dirigeants des unités commerciales de prendre des mesures et d'assumer la responsabilité des risques affectant leurs opérations.

Pour relever ces défis, adoptez une approche descendante pour mesurer les risques, comme mes collègues l'ont décrit dans les chapitres précédents de cet eBook. Identifiez les « chaînes d'approvisionnement » soutenant chaque objectif stratégique et récoltez autant d'informations que nécessaire en temps réel sur l'état de chaque chaîne d'approvisionnement.

## La mesure du risque est une activité stratégique continue

Comment savoir si votre approche de mesure des risques est efficace ? Si elle vous fournit des conseils en continu pour prendre vos décisions commerciales. Dans cette optique, les meilleures pratiques de mesure du risque sont les suivantes :

### Une mesure continue

Les évaluations des risques de votre organisation doivent être continuellement mises à jour avec des informations sur l'état actuel de votre environnement informatique. Si les données relatives aux risques sont à jour, vous avez la garantie de prendre des décisions en fonction de la technologie et des fournisseurs avec lesquels vous travaillez actuellement, et non plus de données obsolètes liées à vos partenaires passés.

### Une évaluation hiérarchisée

Votre approche de l'évaluation des risques devrait faciliter la hiérarchisation des risques et leur réduction pour atteindre les objectifs stratégiques de votre organisation. Vous avez mis en place une notation des risques afin de pouvoir comparer, par exemple, le risque de déplacer un référentiel de données de l'établissement vers un fournisseur cloud de confiance pour économiser de l'argent.

### Une évaluation accessible

Vous pouvez facilement accéder aux évaluations des risques lorsque vous en avez besoin. Inutile de parcourir une multitude de feuilles de calcul Excel pour trouver l'analyse que vous recherchez. Vous pouvez accéder rapidement aux rapports sur les risques dans le cadre des prises de décision continues de l'entreprise.

L'entreprise évolue plus rapidement que jamais. Les environnements informatiques sont vastes et complexes. Vous pouvez mettre en place la pratique de mesure des risques dont vous avez besoin pour guider votre organisation dans sa croissance et sa transformation dans les années à venir en adoptant une approche descendante pour mesurer les risques et en tirant parti de la collecte et de l'automatisation des données en temps réel.

## Guide : les fondamentaux de la mesure du risque

1. Consultez les dirigeants de votre entreprise pour comprendre leurs objectifs stratégiques à long terme pour l'entreprise.
2. Attribuez ces scores d'objectifs pour comprendre l'importance de chaque objectif.
3. Identifiez les personnes, les processus et les technologies qui soutiennent chaque objectif.
4. Analysez les incertitudes liées à chaque facteur de soutien dans la « chaîne d'approvisionnement » d'un objectif.
5. Dans la mesure du possible, faites confiance à l'automatisation pour collecter des données, telles que des données sur l'état de fonctionnement des endpoints.
6. Rencontrez les parties prenantes de différents services pour comprendre leurs préoccupations concernant les risques et travaillez ensemble à produire des recommandations pour les réduire.
7. Attribuez à chaque incertitude un score en termes d'importance et un pourcentage en termes de probabilité. Multipliez les scores par la probabilité de déduire un score de risque pour une personne ou une équipe, un processus ou une technologie spécifique dans la chaîne d'approvisionnement d'un objectif.
8. Notez les résultats de vos mesures et organisez-les de façon à associer chaque risque à un objectif stratégique.
9. Consultez à nouveau la direction de votre entreprise pour une discussion sur les risques, données à l'appui. Aidez-la à comprendre les risques existants et les décisions qui peuvent être prises pour les réduire.
10. Maintenant que vous avez mis en place un cadre de mesure des risques, continuez à le mettre à jour, en utilisant l'automatisation chaque fois que possible afin que les risques puissent être évalués en détail à tout moment.

Le risque, tel que défini par la *norme ISO 31000,* signifie une incertitude quant aux objectifs. Dans cet eBook, nous avons partagé nos connaissances sur les objectifs importants et la manière de mesurer leur incertitude pour obtenir le meilleur résultat possible : réduire les risques qui compromettent la mission d'une entreprise.

Les appareils d'endpoints de l'entreprise jouent un rôle important dans la gestion des risques. Grâce à la plateforme Tanium Converged Endpoint Management (XEM), les organisations peuvent mieux comprendre les mesures de sécurité à appliquer pour identifier les risques et les corriger en temps réel. Tanium Benchmark est la seule solution qui fournit des benchmarks de risques en temps réel aux entreprises d'un même secteur.

En savoir plus sur **Tanium Benchmark.**