Comment gérer les risques régionaux dans une chaîne d'approvisionnement mondiale

Un cadre pratique pour cartographier les fournisseurs, comparer l'exposition aux risques entre les régions et transformer les informations en décisions opérationnelles.

Une chaîne d'approvisionnement mondiale ne présente pas un profil de risque unique. Elle en présente autant qu'il existe de pays, de fournisseurs, d'itinéraires, de réglementations et de dépendances opérationnelles.

Le World Economic Forum identifie la confrontation géoéconomique comme le risque le plus susceptible de provoquer une crise mondiale majeure en 2026 ; 68 % des experts interrogés prévoient un ordre mondial plus fragmenté ou multipolaire au cours de la prochaine décennie. Parallèlement, l'Allianz Risk Barometer 2026 confirme que les cyberincidents constituent le principal risque pour les entreprises à l'échelle mondiale pour la cinquième année consécutive, avec 42 % des réponses. Seuls 3 % des entreprises interrogées estiment que leur chaîne d'approvisionnement est « très résiliente ».

Dans ce contexte, les équipes achats internationales font face à un défi de plus en plus complexe : gérer des chaînes d'approvisionnement mondiales tout en conciliant les risques géopolitiques, les cybermenaces, la continuité des activités et des exigences réglementaires qui varient d'un pays et d'une région à l'autre.

> **Le concept clé**
>
> La gestion des risques liés à la chaîne d'approvisionnement ne consiste pas à évaluer tous les fournisseurs de la même manière. Elle consiste à appliquer le niveau approprié de visibilité, d'évaluation, de validation et de suivi en fonction de l'impact potentiel de chaque fournisseur et de chaque région.

1. Commencez par cartographier votre base fournisseurs actuelle

Avant d'analyser les risques régionaux, l'organisation doit disposer d'une base de données cohérente. La première cartographie ne doit pas chercher à reconstituer l'ensemble de la chaîne étendue : elle doit structurer les informations disponibles sur les fournisseurs directs et mettre en évidence les lacunes.

Au minimum, la gestion des fournisseurs doit permettre d'identifier :

- Le pays et la région où le fournisseur exerce ses activités, et pas uniquement son siège fiscal.
- La catégorie d'achats ainsi que les produits et services fournis.
- Le niveau de dépenses, la dépendance et les possibilités de remplacement.
- L'impact sur les opérations, la sécurité, la conformité et la réputation.
- Les documents, certifications, qualifications et dates d'expiration.
- L'accès aux sites, systèmes, données ou infrastructures critiques.
- Les itinéraires logistiques et les concentrations géographiques significatives.

> **Question de contrôle**
>
> Savons-nous quels fournisseurs pourraient interrompre les activités, entraîner une non-conformité ou nuire à la réputation dans chaque région ? Et sur quelles preuves cette classification repose-t-elle ?

2. Construisez une matrice comparable des risques régionaux

Tous les risques n'ont pas le même poids sur chaque marché. Une matrice efficace combine les facteurs externes propres au pays ou à la région avec l'exposition spécifique du fournisseur. Elle permet ainsi de comparer différentes situations selon des critères cohérents, sans réduire l'analyse à un score générique de risque pays.

Dimension	Éléments à évaluer
Risque géopolitique	Conflits, sanctions, restrictions commerciales, stabilité institutionnelle et évolution des alliances régionales.
Risque réglementaire	Conformité à la législation applicable, licences, autorisations, exigences sectorielles et évolutions réglementaires.
Risque opérationnel	Capacité de livraison, concentration, dépendance à un fournisseur unique, itinéraires, stocks et continuité de service.
Risque financier	Solvabilité, liquidité, dépendance économique, devises, historique des paiements et alertes concernant l'entreprise.
Risque ESG	Environnement, conditions de travail, éthique, gouvernance, santé et sécurité, et performance en matière de durabilité.
Cyberrisque	Accès aux systèmes, données traitées, contrôles de sécurité, incidents, sous-traitants technologiques et exposition numérique.
Risque réputationnel	Informations négatives, controverses, litiges, sanctions, listes de surveillance et conduite des affaires.

L'OCDE recommande une due diligence fondée sur les risques afin d'identifier, de prévenir, d'atténuer et de suivre les impacts réels ou potentiels sur les activités, les chaînes d'approvisionnement et les relations commerciales. La conséquence pratique est claire : les ressources consacrées aux achats, à la conformité et aux audits doivent se concentrer là où l'impact et la probabilité sont les plus élevés.

3. Changez de perspective : les risques récurrents par région

Une matrice mondiale nécessite un contexte local. Les expositions présentées ci-dessous sont indicatives et doivent être adaptées au pays, au secteur, à la catégorie et au type de fournisseur ; elles ne remplacent pas une analyse spécifique.

Région	Expositions qui nécessitent généralement une attention accrue	Éléments à surveiller
Europe	Évolution de la réglementation ESG et de la due diligence, protection des données, cybersécurité, énergie et continuité logistique.	Nouvelles obligations, exigences de reporting, sanctions, échéances documentaires et risques liés aux tiers numériques.
Amérique latine	Évolutions politiques et réglementaires, corruption, volatilité économique, sécurité, infrastructures et dépendance logistique.	Listes de sanctions, informations négatives, stabilité financière, licences, obligations fiscales et évolution des conditions opérationnelles.
Moyen-Orient et Afrique	Conflits, sanctions, itinéraires critiques, disponibilité de l'énergie et de l'eau, droits humains et stabilité institutionnelle.	Restrictions commerciales, fermeture d'itinéraires, conditions de travail, continuité des services et exposition à des pays à haut risque.
Asie-Pacifique	Concentration des fournisseurs, catastrophes naturelles, tensions commerciales, cybersécurité et dépendance à des composants stratégiques.	Sites de production, sous-traitants critiques, capacités alternatives, événements climatiques et contrôles des données.
Amérique du Nord	Politique commerciale et tarifaire, cybermenaces, divergences réglementaires, concentration technologique et risques pour la continuité.	Évolutions tarifaires, exigences nationales ou sectorielles, cyberincidents et dépendance à des fournisseurs uniques.

4. Segmentez les fournisseurs selon leur criticité et leur niveau de risque

La criticité et le risque ne sont pas synonymes. Un fournisseur peut opérer dans une région à faible risque tout en étant critique faute d'alternative ; un autre peut se trouver dans une région complexe, mais fournir un service facilement remplaçable. La segmentation doit combiner ces deux variables.

Niveau	Profil	Approche recommandée
Critique	Une défaillance peut interrompre les activités, compromettre la sécurité, entraîner une non-conformité ou mettre en danger un actif essentiel.	Due diligence complète, données validées, suivi continu, audits le cas échéant et plan de continuité spécifique.
Haut risque	Exposition significative aux risques ESG, financiers, géopolitiques, réglementaires ou cyber.	Évaluation approfondie, validation des informations, suivi continu, alertes, plans d'amélioration et audits déclenchés par des signaux ou des lacunes.
Risque moyen	Dépendance modérée ou exigences documentaires significatives, avec des alternatives disponibles.	Validation des données critiques, révision structurée, alertes continues et escalade en cas d'évolution du profil de risque.
Faible	Faible impact individuel et grand nombre de fournisseurs.	Analyse prédictive des risques, évaluation des données externes critiques et suivi sans solliciter le fournisseur ; ne déclencher une escalade qu'en présence de signaux.

Cette approche permet d'éviter deux erreurs courantes :

- Consacrer des processus coûteux à des fournisseurs faiblement exposés sans améliorer la résilience.
- Soumettre les fournisseurs critiques à des contrôles documentaires superficiels ou ponctuels.

5. Étendez la visibilité au-delà des fournisseurs directs lorsque votre niveau de maturité le permet

Une fois la base de fournisseurs directs structurée, l'étape suivante consiste à identifier les dépendances cachées entre les fournisseurs de rang 2 et 3, les sites, les sous-traitants, les composants et les itinéraires. Cette phase nécessite de cartographier la chaîne d'approvisionnement, de collaborer avec les fournisseurs critiques et, dans certains cas, de réaliser des audits ou des vérifications complémentaires.

L'Enquête mondiale Achilles 2026 sur les risques, menée auprès de plus de 2 800 organisations, met en évidence l'ampleur de l'écart : seuls 6 % déclarent disposer d'une visibilité complète sur leurs fournisseurs de rang 2 et 3, tandis que près de la moitié reconnaissent avoir une visibilité limitée, voire inexistante, au-delà de leur base directe. En outre, seuls 18 % font pleinement confiance à l'exactitude des données de sécurité communiquées par leurs fournisseurs.

Pour progresser sans chercher à tout cartographier en une seule fois :

- Commencez par les fournisseurs critiques et les catégories pour lesquelles il n'existe aucune alternative.
- Identifiez les matériaux, les sites, les sous-traitants et les itinéraires qui concentrent l'exposition.
- Donnez la priorité aux pays, secteurs et composants présentant un risque intrinsèque plus élevé.
- Validez les informations à l'aide de sources externes, de documents, d'entretiens ou d'audits.
- Intégrez la cartographie étendue au même modèle d'alertes et de prise de décision.

6. Surveillez les signaux, pas seulement les documents

Une certification valide aujourd'hui n'exclut pas une alerte financière demain. Un fournisseur qualifié peut être touché par une sanction, une cyberattaque, un conflit, un changement de propriétaire ou un événement climatique. Le suivi doit détecter les évolutions entre deux évaluations et déclencher une réponse proportionnée.

Signal	Pourquoi est-ce important ?
Évolutions réglementaires	Elles peuvent modifier les exigences en matière de qualification, de due diligence, de contractualisation ou de reporting.
Alertes financières	Elles peuvent révéler en amont des problèmes de capacité, de liquidité, de paiement ou de continuité.
Sanctions et listes de surveillance	Elles peuvent empêcher une relation commerciale ou nécessiter des contrôles renforcés.
Informations négatives et incidents ESG	Ils ont une incidence sur la réputation, les contrats, les droits humains et les obligations légales.
Cyberrisques	Ils peuvent compromettre les systèmes, les données, les activités et les tiers associés.
Événements géopolitiques ou climatiques	Ils modifient les itinéraires, la disponibilité, les coûts, les délais et l'accès aux marchés.
Modifications documentaires ou sociétaires	Elles révèlent des échéances, des informations incomplètes, des acquisitions ou des changements de contrôle.

7. Transformez la cartographie des risques en décisions et plans de continuité

La cartographie ne crée de valeur que si elle influence les décisions des achats, des opérations, de la conformité et de la direction. Pour chaque niveau de risque, il convient de définir des actions, des responsables, des échéances et des critères d'escalade.

- Donner la priorité aux audits ESG, aux audits de santé et sécurité ou d'éthique des affaires auprès des fournisseurs et dans les régions critiques.
- Exiger des plans d'amélioration précisant les responsables, les preuves et les dates de clôture.
- Diversifier les sources d'approvisionnement, les itinéraires ou les sites en cas de concentration.
- Activer un plan de continuité pour les fournisseurs qui ne peuvent pas être remplacés immédiatement.
- Renforcer les contrôles contractuels, documentaires, cyber ou financiers.
- Suspendre les nouvelles attributions ou déclencher une escalade vers les services juridiques et conformité lorsque le risque dépasse le seuil accepté.
- Développer les fournisseurs stratégiques lorsque les mesures correctives sont plus réalistes qu'un remplacement.

> **Règle de décision**
>
> Chaque risque significatif doit répondre à quatre questions : que peut-il se passer ? Quel serait l'impact ? Qui doit intervenir ? Dans quel délai ?

8. Révisez la cartographie avec une gouvernance claire

La gestion des risques régionaux n'est pas un exercice annuel. Elle doit fonctionner comme un processus dynamique, avec des responsables, des seuils et une fréquence de révision proportionnée à la criticité.

Au minimum, révisez la cartographie dans les cas suivants :

- Entrée dans une nouvelle région ou catégorie.
- Intégration ou renouvellement d'un fournisseur critique.
- Évolution réglementaire, sanction ou restriction commerciale.
- Incident ESG, financier, opérationnel ou cyber.
- Fusion, acquisition ou changement de contrôle.
- Perturbation géopolitique, climatique ou logistique.
- Dégradation des performances ou non-respect d'un plan d'amélioration.

Le DHL Global Connectedness Report 2026 indique que le niveau de mondialisation s'est maintenu à 25 % en 2025, égalant le record historique atteint en 2022. L'activité internationale ne disparaît pas : elle se reconfigure. La résilience de la chaîne d'approvisionnement dépendra donc de plus en plus de la capacité à identifier où évoluent les flux et les dépendances.

Comment Achilles peut transformer ce cadre en processus opérationnel

Achilles permet d'appliquer différents niveaux de vérification à l'ensemble de la base fournisseurs, depuis un premier niveau de visibilité jusqu'aux évaluations approfondies et aux audits. L'objectif n'est pas d'ajouter des tâches, mais de concentrer les efforts là où ils peuvent réduire le plus efficacement les risques.

1. **Couverture étendue avec Achilles Risk Screening**
   Analyse prédictive et suivi continu, sans solliciter les fournisseurs ni utiliser de questionnaires, afin de détecter les signaux ESG, financiers, cyber et géopolitiques, les sanctions, les listes de surveillance et les informations négatives sur de grands volumes de fournisseurs.

2. **Processus de due diligence pour les fournisseurs les plus exposés**
   Évaluations structurées, données et documents validés, et vision comparable des performances afin d'éclairer les décisions de gestion des fournisseurs et d'achats.

3. **Audits pour obtenir un niveau de fiabilité supérieur**
   Audits documentaires ou sur site et, le cas échéant, entretiens confidentiels avec les travailleurs afin de vérifier les contrôles, d'identifier les lacunes et de définir des mesures correctives.

4. **Suivi, alertes et analyses sur une plateforme unique**
   Informations actualisées, tableaux de bord et critères configurables pour détecter les évolutions, définir les priorités et partager une vision commune entre les achats, les risques, la conformité, les équipes ESG et les opérations.

5. **Amélioration durable et résilience**
   Plans d'action, suivi des non-conformités et accompagnement des fournisseurs afin de renforcer les normes, de réduire l'exposition et de bâtir une chaîne d'approvisionnement durable, prête à répondre à de nouvelles exigences.

Découvrez Achilles Risk Screening ainsi que notre approche de la qualification des fournisseurs et de la gestion des risques liés à la chaîne d'approvisionnement.

Checklist : évaluez la maturité de votre gestion des risques régionaux

Cochez les actions que votre organisation réalise de manière systématique. Cette checklist ne remplace pas une évaluation formelle, mais elle aide à identifier les lacunes prioritaires.

Visibilité et segmentation

☐ Nous avons identifié les fournisseurs par pays, région, catégorie, dépenses et criticité.

☐ Nous savons quels fournisseurs sont essentiels à la continuité, à la conformité, à la sécurité ou à la réputation.

☐ Nous distinguons la criticité opérationnelle du niveau de risque intrinsèque.

Évaluation et due diligence

☐ Nous évaluons les risques géopolitiques, réglementaires, financiers, ESG, opérationnels et cyber par région.

☐ Nous appliquons différents niveaux d'évaluation, de validation et d'audit en fonction de l'impact potentiel.

☐ Nous disposons de critères d'escalade pour les fournisseurs dont le profil de risque évolue.

Suivi et visibilité étendue

☐ Nous suivons les alertes externes, les modifications documentaires et les incidents entre deux évaluations.

☐ Nous disposons d'une visibilité sur les dépendances de rang 2 ou 3 dans les catégories critiques.

☐ Nous disposons de données suffisamment fiables pour prendre des décisions et justifier le processus.

Action et gouvernance

☐ Nous définissons des plans d'amélioration, de continuité ou de remplacement pour les risques significatifs.

☐ Nous partageons les informations avec les achats, la conformité, les opérations, les équipes ESG et la direction.

☐ Nous révisons la cartographie lorsque les fournisseurs, les régions, les réglementations ou les conditions opérationnelles évoluent.

0 à 4 actions	Niveau initial : il est recommandé de structurer la base fournisseurs et d'établir des critères de risque communs.
5 à 8 actions	Niveau intermédiaire : une base existe, mais la validation, le suivi ou la coordination restent insuffisants.
9 à 12 actions	Niveau avancé : l'organisation peut se concentrer sur l'anticipation, la chaîne étendue et l'amélioration continue.

Conclusion : d'une cartographie statique à une gestion proactive

Cartographier les risques régionaux ne consiste pas à accumuler des données. Il s'agit de produire des informations exploitables : savoir quel fournisseur est important, quelle exposition augmente et quelle décision prendre avant que le risque ne se transforme en interruption.

Les organisations qui associent visibilité sur les fournisseurs, critères comparables, données validées, suivi continu et plans d'amélioration sont mieux préparées à évoluer dans un environnement fragmenté, réglementé et en constante mutation. La résilience commence par la capacité à détecter les risques suffisamment tôt et à transformer cette visibilité en actions.

Questions fréquentes sur les risques régionaux et les fournisseurs

Qu'est-ce que la gestion des risques liés à la chaîne d'approvisionnement ?

Il s'agit du processus qui consiste à identifier, évaluer, surveiller et réduire les menaces susceptibles, par l'intermédiaire des fournisseurs et des tiers, de compromettre l'approvisionnement, la conformité, la sécurité, les finances ou la réputation.

Comment segmenter les fournisseurs ?

En combinant la criticité et l'impact avec le risque intrinsèque. Les dépenses ne suffisent pas : il faut également prendre en compte les possibilités de remplacement, l'accès aux systèmes ou aux installations, la localisation, la réglementation et les conséquences d'une interruption.

À quelle fréquence la cartographie des risques doit-elle être révisée ?

Les fournisseurs critiques et à haut risque nécessitent un suivi continu. Le cadre complet doit être révisé en cas d'évolution réglementaire, d'incident, d'entrée dans une nouvelle région, de renouvellement contractuel ou de changement significatif concernant un fournisseur.

Comment améliorer la visibilité sur les fournisseurs au-delà du rang 1 ?

En donnant la priorité aux catégories et aux fournisseurs critiques, en demandant des informations sur les sous-traitants et les sites, en utilisant des sources externes et en validant les principaux points d'exposition au moyen de la cartographie de la chaîne d'approvisionnement, de la due diligence ou d'audits.