Au-delà de l'ESG : les risques fournisseurs qui peuvent aussi interrompre votre activité

Pourquoi les données environnementales, sociales et de gouvernance sont nécessaires, mais insuffisantes pour protéger la continuité opérationnelle, la sécurité et la réputation d'une entreprise.

Une chaîne d'approvisionnement peut afficher de bons indicateurs ESG et pourtant connaître une défaillance dès demain.

La pression réglementaire, portée par des cadres tels que la CSRD et la CSDDD, la nécessité de réaliser des analyses de double matérialité, de déclarer les émissions de Scope 3 et de répondre aux attentes des clients et des investisseurs, a accéléré l'adoption d'outils d'analyse ESG. Cette évolution est nécessaire : elle permet de structurer les informations de durabilité, de comparer les fournisseurs et d'améliorer la qualité du reporting.

Le problème survient lorsque ces informations sont interprétées comme une vision complète du risque fournisseur. Un fournisseur peut disposer de politiques environnementales solides et, dans le même temps, subir une crise de liquidité. Il peut avoir un code d'éthique tout en conservant une vulnérabilité critique dans le logiciel qui lui permet d'accéder à vos systèmes. Il peut déclarer ses émissions et présenter des défaillances en matière de contrôle qualité, de sécurité industrielle ou de capacité opérationnelle.

Les données récentes montrent pourquoi cette distinction est importante. En 2026, 65 % des grandes entreprises interrogées par le World Economic Forum ont cité les vulnérabilités liées aux tiers et à la chaîne d'approvisionnement comme principal obstacle à leur cyberrésilience. Allianz a classé les cyberincidents au premier rang des risques d'entreprise mondiaux pour la cinquième année consécutive, avec 42 % des réponses.

IDÉE CLÉ

L'ESG constitue une couche d'information essentielle, mais pas un système complet de maîtrise des risques.

Une évaluation ESG aide à comprendre comment un fournisseur gère ses impacts environnementaux, sociaux et de gouvernance. La gestion des risques de la chaîne d'approvisionnement doit également déterminer si ce fournisseur peut continuer à livrer, protéger les données, travailler en toute sécurité, respecter ses obligations et résister à une interruption d'activité.

1. Ce qu'une évaluation ESG montre, et ce qu'elle peut laisser de côté

Les outils d'analyse ESG structurent des données longtemps restées dispersées : politiques environnementales, émissions, droits des travailleurs, éthique des affaires, diversité ou gouvernance. Ils contribuent également à préparer le reporting, à identifier les lacunes et à progresser vers une chaîne d'approvisionnement durable.

Cependant, le risque fournisseur ne se divise pas en compartiments étanches. Certains facteurs, comme la santé et la sécurité ou la cybersécurité, peuvent s'inscrire dans un cadre ESG large, mais leur gestion opérationnelle exige un niveau d'analyse bien supérieur à celui d'un indicateur général ou d'une autodéclaration périodique.

Une évaluation ESG répond généralement aux questions suivantes	La gestion intégrée des risques doit également répondre aux questions suivantes
Quelles politiques environnementales et sociales le fournisseur applique-t-il ?	Dispose-t-il de la capacité financière et opérationnelle nécessaire pour exécuter le contrat ?
Comment mesure-t-il et déclare-t-il ses émissions ?	Quel est le niveau de dépendance à l'égard de ce fournisseur, de ce site ou de ce sous-traitant ?
Dispose-t-il de codes d'éthique et de gouvernance ?	A-t-il accès à des systèmes, des données ou des infrastructures critiques ?
Déclare-t-il appliquer des pratiques de santé et de sécurité ?	Les qualifications de ses travailleurs, ses permis, ses assurances et ses documents sont-ils toujours valides ?
Répond-il à certains critères de durabilité ?	Quels signaux indiquent que son profil de risque est en train d'évoluer ?

Il ne s'agit pas de choisir entre l'ESG et la gestion des fournisseurs, mais d'intégrer les deux approches dans un modèle multirisque reposant sur des données vérifiées, une segmentation par criticité et un suivi continu.

2. Risque financier : même un fournisseur durable peut manquer de liquidités

La stabilité financière est l'un des angles morts les plus évidents d'une évaluation centrée uniquement sur l'ESG. L'insolvabilité, la dégradation des flux de trésorerie, la dépendance à quelques clients ou une couverture d'assurance insuffisante peuvent empêcher un fournisseur de livrer, de maintenir ses effectifs ou de respecter ses engagements, même lorsque ses politiques de durabilité sont solides.

CAS RÉEL | Carillion : quand l'insolvabilité se transforme en interruption opérationnelle

Ce qui s'est passé. Le groupe britannique Carillion a été placé en liquidation en janvier 2018. Son effondrement a contraint le gouvernement britannique à mettre en place des mesures de continuité pour de nombreux services et a interrompu les travaux de plusieurs contrats de construction, dont deux hôpitaux.

Ce que cela montre. La qualification et les critères ESG ne remplacent pas le suivi de la solvabilité, des liquidités, de la concentration des revenus, des assurances et des signes de dégradation. Sans ces informations, le risque financier peut se matérialiser avant que les achats ne disposent d'une solution alternative prête.

Pour anticiper ce type d'exposition, la gestion des risques de la chaîne d'approvisionnement devrait au minimum suivre :

- Les évolutions des notations financières, des comptes annuels et des comportements de paiement.
- La dépendance économique à l'égard d'un client, d'un contrat ou d'un marché.
- Les alertes d'insolvabilité, les litiges, les saisies ou les changements d'entreprise.
- La validité et l'adéquation des couvertures d'assurance.
- L'existence de fournisseurs alternatifs et d'un plan de continuité.

3. Risque cyber : chaque tiers connecté élargit la surface d'attaque

La digitalisation de la chaîne d'approvisionnement a multiplié les connexions entre acheteurs, fournisseurs, plateformes, opérateurs logistiques et prestataires technologiques. Cette efficacité crée également des dépendances : un tiers ayant accès à des données, des systèmes ou des identifiants peut devenir le point d'entrée d'un incident.

CAS RÉEL | SolarWinds : un fournisseur de confiance devenu vecteur d'attaque

Ce qui s'est passé. En 2020, l'agence américaine de cybersécurité et de sécurité des infrastructures a confirmé l'exploitation active de versions compromises de la plateforme SolarWinds Orion. L'attaque a utilisé des mises à jour logicielles distribuées par un fournisseur légitime pour accéder aux organisations clientes.

Ce que cela montre. La cybersécurité des tiers ne peut pas être évaluée uniquement au début de la relation. Il faut connaître les accès, les dépendances technologiques, les sous-traitants, les contrôles des mises à jour, les procédures de réponse aux incidents et les évolutions du niveau d'exposition.

Un questionnaire ESG peut comporter des questions sur les politiques de protection des données. Une gestion efficace des risques doit aller plus loin :

- Identifier les fournisseurs qui accèdent aux systèmes, aux réseaux ou aux informations sensibles.
- Évaluer les contrôles, les certifications, les vulnérabilités et l'historique des incidents.
- Limiter les privilèges et réexaminer régulièrement les accès.
- Analyser les dépendances aux logiciels, au cloud et aux fournisseurs de quatrième rang.
- Définir des protocoles de notification, de reprise et de continuité.

4. Qualité, capacité et sécurité : respecter les politiques ne garantit pas une bonne exécution

La continuité opérationnelle dépend également de la capacité réelle d'un fournisseur à fabriquer, installer, entretenir ou fournir un service avec la qualité et la sécurité requises. La compétence technique, la traçabilité, la maîtrise des changements, la formation, la maintenance, la supervision et l'historique des incidents sont ici déterminants.

CAS RÉEL | Vol Alaska Airlines 1282 : le coût d'une perte de traçabilité et de maîtrise des processus

Ce qui s'est passé. En janvier 2024, le panneau d'obturation d'une porte d'un Boeing 737-9 s'est détaché en vol. Le rapport final du NTSB a conclu à l'absence de boulons de fixation et a identifié comme cause probable un manque de formation, d'instructions et de supervision adéquates de la part de Boeing. Le composant avait suivi une chaîne de fabrication et de reprise impliquant plusieurs organisations et équipes.

Ce que cela montre. Les risques liés à la qualité et à la sécurité exigent des preuves opérationnelles : traçabilité des composants, contrôles des changements, compétences, audits, dossiers de maintenance et responsabilités clairement définies. À lui seul, un bon indicateur ESG ne détecte pas une défaillance de processus.

La santé et la sécurité au travail nécessitent une précision supplémentaire. Elles peuvent figurer dans une évaluation ESG, mais les entreprises qui font intervenir des sous-traitants sur des sites critiques ont besoin d'informations beaucoup plus précises : formations obligatoires, habilitations, permis de travail, accidents, assurances, validité des documents et contrôle des accès.

C'est pourquoi, dans des secteurs tels que l'énergie, la construction, les services publics, le transport, le maritime et l'industrie, la gestion documentaire, le contrôle des sous-traitants et des fournisseurs et, le cas échéant, une plateforme de gestion des sous-traitants font partie du système de prévention des risques, et non d'une tâche administrative isolée.

5. Risques réglementaires, géopolitiques et réputationnels : le contexte peut changer avant le fournisseur

Un fournisseur peut conserver exactement les mêmes pratiques et néanmoins voir son niveau de risque augmenter parce que son environnement évolue. Une nouvelle sanction, une restriction commerciale, un conflit, une enquête, une modification réglementaire ou une information négative peuvent affecter sa capacité à exercer ses activités ou l'opportunité de maintenir la relation.

Ces risques sont particulièrement difficiles à gérer au moyen d'évaluations annuelles. Ils nécessitent le suivi des listes de sanctions, de la presse négative, des changements d'entreprise, de l'exposition géographique, des itinéraires logistiques et de la dépendance à des sources uniques.

CHANGEMENT D'APPROCHE

La qualification indique si un fournisseur répondait aux exigences à une date donnée.

Le suivi continu indique s'il continue d'y répondre, si son exposition a évolué et si l'entreprise doit agir avant que le problème n'affecte les opérations.

6. Du fournisseur qualifié au fournisseur suivi en continu

La qualification des fournisseurs reste une base nécessaire. Elle permet de vérifier les exigences, d'organiser les documents et de définir un seuil d'entrée. L'erreur consiste à la considérer comme un aboutissement.

Le profil d'un fournisseur évolue pendant la durée du contrat. Il peut perdre une certification, subir un cyberincident, réduire ses effectifs, changer de propriétaire, accumuler des dettes, sous-traiter une activité critique ou laisser expirer des documents. Aucun de ces changements n'est couvert par le simple fait que le fournisseur ait été approuvé douze mois auparavant.

Niveau de contrôle	Informations couvertes	Décision permise
Analyse initiale	Données publiques, implantation, activité, risque inhérent et signaux prédictifs	Prioriser les fournisseurs nécessitant une due diligence approfondie
Qualification et validation	Documents, questionnaires, sources externes et exigences de l'acheteur	Approuver, approuver sous conditions ou refuser la relation
Évaluation spécialisée	Finances, cybersécurité, ESG, santé et sécurité, assurances, qualité et capacité	Attribuer un niveau de risque et des contrôles proportionnés
Audit	Preuves relatives au système de gestion, aux sites, aux processus et aux travailleurs	Confirmer l'efficacité réelle des contrôles et définir les améliorations
Suivi continu	Alertes financières, sanctions, presse négative, échéances, incidents et changements d'entreprise	Agir avant que le risque ne provoque une interruption
Plans d'action et de continuité	Lacunes, responsables, délais, solutions alternatives et mesures de continuité	Réduire l'exposition, développer ou remplacer les fournisseurs

7. Ce que devrait inclure une vision intégrée du risque fournisseur

Une stratégie solide ne consiste pas à demander indistinctement davantage d'informations à tous les fournisseurs. Elle consiste à appliquer le niveau de contrôle approprié en fonction de la criticité, de l'exposition et de l'impact potentiel.

- Visibilité fournisseurs : une base commune regroupant l'implantation, la catégorie, les dépenses, la criticité, les accès et les dépendances.
- Segmentation des risques : des critères cohérents pour distinguer les fournisseurs critiques, à haut risque, à risque moyen et à faible exposition.
- Analyse prédictive : un premier niveau pour détecter des signaux dans toute la base fournisseurs, avant d'engager des évaluations approfondies.
- Données vérifiées : validation des documents et recoupement avec des sources indépendantes, et non de simples autodéclarations.
- Évaluation multirisque : ESG, finances, cyber, sécurité, qualité, assurances, conformité et continuité.
- Audits proportionnés : à distance ou sur site, selon le niveau de risque.
- Suivi continu : des alertes qui détectent les évolutions pendant toute la durée de la relation contractuelle.
- Plans d'amélioration et de continuité : responsables, délais, preuves et solutions alternatives.

Cette approche améliore la résilience en transformant l'information en décisions : quels fournisseurs accompagner, quels contrats renforcer, où réaliser des audits, quand diversifier et quels risques transmettre à la conformité, à la sécurité, aux opérations ou à la direction.

8. Comment Achilles aide à relier l'ESG à une gestion multirisque

Achilles permet d'appliquer différents niveaux d'évaluation et de vérification à la base fournisseurs. L'objectif n'est pas de remplacer l'analyse ESG, mais de l'intégrer dans une vision plus complète du risque et de la relier aux opérations.

1	**Détection précoce des risques** Analyse prédictive et signaux initiaux pour prioriser les fournisseurs et détecter les risques cachés dans une base étendue.
2	**Évaluation et due diligence** Identification des risques et plans d'atténuation en fonction des exigences et du niveau de criticité défini par l'acheteur.
3	**Vérification approfondie** Évaluations spécialisées et audits pour approfondir l'analyse ESG, la santé et la sécurité, la qualité, l'éthique, les finances et d'autres risques.
4	**Suivi et amélioration** Audits, alertes continues, analyses, plans d'action et suivi pour maintenir les informations à jour et renforcer la résilience.

Découvrez la plateforme Achilles et notre approche de la gestion intégrée des risques fournisseurs.

Conclusion : l'ESG est indispensable, mais ce n'est pas le seul risque

La durabilité doit rester au coeur de toute stratégie moderne d'achats et de gestion des fournisseurs. Mais une entreprise ne protège pas sa chaîne d'approvisionnement uniquement au moyen d'indicateurs environnementaux, sociaux et de gouvernance.

La question décisive n'est pas seulement de savoir si un fournisseur est durable. Il faut également déterminer s'il peut continuer à livrer, s'il est solvable, s'il protège les données, s'il travaille en toute sécurité, s'il maintient ses exigences à jour et si l'organisation pourra réagir lorsque son profil évoluera.

Une chaîne d'approvisionnement résiliente se construit en reliant l'ESG aux données financières, cyber, opérationnelles, documentaires et de sécurité, en validant les informations et en surveillant les signaux tout au long de la relation. C'est à ce stade que le reporting cesse d'être une photographie pour devenir une véritable capacité d'anticipation.

MESSAGE FINAL

La meilleure évaluation n'est pas celle qui collecte le plus de données, mais celle qui permet d'agir plus tôt.

Lorsque les achats, la durabilité, la conformité, la sécurité et les opérations partagent une vision commune du risque fournisseur, l'entreprise peut mieux prioriser ses ressources, renforcer ses contrôles et protéger la continuité de ses activités.

Questions fréquentes

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

Il s'agit du processus qui consiste à identifier, évaluer, hiérarchiser et suivre les risques liés aux fournisseurs, aux sous-traitants, aux sites et aux dépendances susceptibles d'affecter la continuité, la conformité, la sécurité ou la réputation d'une organisation.

Pourquoi une évaluation ESG ne suffit-elle pas ?

Parce qu'elle se concentre généralement sur les facteurs environnementaux, sociaux et de gouvernance, alors qu'un fournisseur peut également connaître une défaillance en raison d'une insolvabilité, d'une cyberattaque, de problèmes de qualité, d'une capacité insuffisante, de documents expirés, de sanctions ou d'incidents de sécurité.

Quelle est la différence entre qualifier et suivre les fournisseurs ?

La qualification valide les exigences à un moment donné. Le suivi continu détecte les évolutions ultérieures du profil financier, réglementaire, cyber, documentaire ou opérationnel du fournisseur.

Tous les fournisseurs nécessitent-ils le même niveau d'évaluation ?

Non. Le niveau de due diligence doit être proportionnel à la criticité, au risque inhérent et à l'impact potentiel. Les fournisseurs à faible exposition peuvent commencer par une analyse prédictive, tandis que les fournisseurs critiques nécessitent une validation approfondie, des audits et un suivi continu.

Quelle valeur un audit ESG apporte-t-il dans une approche multirisque ?

Il apporte des preuves de l'efficacité de certains contrôles environnementaux, sociaux et de gouvernance. Il doit être complété par d'autres évaluations lorsque des risques financiers, cyber, opérationnels, de qualité ou de santé et de sécurité sont présents.