Come gestire i rischi regionali in una catena di fornitura globale

Un quadro pratico per mappare i fornitori, confrontare l'esposizione al rischio nelle diverse regioni e trasformare le informazioni in decisioni operative.

Una catena di fornitura globale non ha un unico profilo di rischio. Ne ha tanti quanti sono i Paesi, i fornitori, le rotte, le normative e le dipendenze operative coinvolte.

Il World Economic Forum indica il confronto geoeconomico come il rischio con la maggiore probabilità di provocare una crisi globale rilevante nel 2026; il 68% degli esperti consultati prevede un ordine mondiale più frammentato o multipolare nel prossimo decennio. Allo stesso tempo, l'Allianz Risk Barometer 2026 conferma gli incidenti informatici come il principale rischio aziendale globale per il quinto anno consecutivo, con il 42% delle risposte. Solo il 3% delle aziende intervistate considera la propria catena di fornitura «molto resiliente».

In questo contesto, i team acquisti globali affrontano una sfida sempre più complessa: gestire catene di fornitura internazionali bilanciando rischi geopolitici, minacce informatiche, continuità operativa e requisiti normativi che variano da un Paese e da una regione all'altra.

> **Il concetto chiave**
>
> La gestione del rischio della catena di fornitura non consiste nel valutare tutti i fornitori allo stesso modo. Consiste nell'applicare il livello adeguato di visibilità, valutazione, convalida e monitoraggio in base all'impatto potenziale di ciascun fornitore e di ciascuna regione.

1. Inizia mappando l'attuale base fornitori

Prima di analizzare i rischi regionali, l'organizzazione deve disporre di una base dati coerente. La prima mappa non deve cercare di ricostruire l'intera catena estesa: deve organizzare le informazioni disponibili sui fornitori diretti e mettere in evidenza le lacune.

Come minimo, la gestione dei fornitori dovrebbe identificare:

- Paese e regione in cui opera il fornitore, non solo la sede fiscale.
- Categoria di acquisto, prodotti e servizi forniti.
- Livello di spesa, dipendenza e possibilità di sostituzione.
- Impatto su operatività, sicurezza, compliance e reputazione.
- Documentazione, certificazioni, qualifica e date di scadenza.
- Accesso a siti, sistemi, dati o infrastrutture critiche.
- Rotte logistiche e concentrazioni geografiche rilevanti.

> **Domanda di controllo**
>
> Sappiamo quali fornitori possono interrompere l'attività, causare non conformità o danni reputazionali in ogni regione e quali evidenze giustificano la classificazione?

2. Costruisci una matrice comparabile dei rischi regionali

Non tutti i rischi hanno lo stesso peso in ogni mercato. Una matrice efficace combina i fattori esterni del Paese o della regione con l'esposizione specifica del fornitore. In questo modo è possibile confrontare situazioni diverse con criteri coerenti, senza ridurre l'analisi a un generico punteggio di rischio Paese.

Dimensione	Cosa valutare
Rischio geopolitico	Conflitti, sanzioni, restrizioni commerciali, stabilità istituzionale e cambiamenti nelle alleanze regionali.
Rischio normativo	Conformità alla legislazione applicabile, licenze, autorizzazioni, requisiti di settore e modifiche normative.
Rischio operativo	Capacità di consegna, concentrazione, dipendenza da un unico fornitore, rotte, scorte e continuità del servizio.
Rischio finanziario	Solvibilità, liquidità, dipendenza economica, valuta, storico dei pagamenti e segnalazioni societarie.
Rischio ESG	Ambiente, condizioni di lavoro, etica, governance, salute e sicurezza e performance di sostenibilità.
Rischio informatico	Accesso ai sistemi, dati gestiti, controlli di sicurezza, incidenti, subappaltatori tecnologici ed esposizione digitale.
Rischio reputazionale	Notizie negative, controversie, contenziosi, sanzioni, liste di controllo e condotta aziendale.

L'OCSE raccomanda una due diligence basata sul rischio per identificare, prevenire, mitigare e monitorare gli impatti effettivi o potenziali sulle attività, le catene di fornitura e le relazioni commerciali. La conseguenza pratica è chiara: le risorse dedicate ad acquisti, compliance e audit devono concentrarsi dove impatto e probabilità sono maggiori.

3. Cambia prospettiva: rischi ricorrenti per regione

Una matrice globale richiede un contesto locale. Le esposizioni riportate di seguito sono indicative e devono essere adattate in base al Paese, al settore, alla categoria e al tipo di fornitore; non sostituiscono un'analisi specifica.

Regione	Esposizioni che richiedono generalmente maggiore attenzione	Cosa monitorare
Europa	Evoluzione della normativa ESG e di due diligence, protezione dei dati, cybersecurity, energia e continuità logistica.	Nuovi obblighi, requisiti di rendicontazione, sanzioni, scadenze documentali e rischi legati a terze parti digitali.
America Latina	Cambiamenti politici e normativi, corruzione, volatilità economica, sicurezza, infrastrutture e dipendenza logistica.	Liste di sanzioni, notizie negative, stabilità finanziaria, licenze, adempimenti fiscali e cambiamenti nelle condizioni operative.
Medio Oriente e Africa	Conflitti, sanzioni, rotte critiche, disponibilità di energia e acqua, diritti umani e stabilità istituzionale.	Restrizioni commerciali, chiusure delle rotte, condizioni di lavoro, continuità dei servizi ed esposizione a Paesi ad alto rischio.
Asia-Pacifico	Concentrazione dei fornitori, disastri naturali, tensioni commerciali, cybersecurity e dipendenza da componenti strategici.	Siti produttivi, subfornitori critici, capacità alternative, eventi climatici e controlli sui dati.
Nord America	Politica commerciale e tariffaria, minacce informatiche, divergenze normative, concentrazione tecnologica e rischi per la continuità.	Modifiche tariffarie, requisiti statali o di settore, incidenti informatici e dipendenza da fornitori unici.

4. Segmenta i fornitori per criticità e livello di rischio

Criticità e rischio non sono la stessa cosa. Un fornitore può operare in una regione a basso rischio ed essere critico perché non esistono alternative; un altro può trovarsi in una regione complessa, ma fornire un servizio facilmente sostituibile. La segmentazione deve combinare entrambe le variabili.

Livello	Profilo	Approccio consigliato
Critico	Un suo malfunzionamento può interrompere l'attività, compromettere la sicurezza, causare una non conformità o mettere a rischio un asset essenziale.	Due diligence completa, dati convalidati, monitoraggio continuo, audit ove opportuno e un piano di emergenza specifico.
Alto rischio	Esposizione rilevante a rischi ESG, finanziari, geopolitici, normativi o informatici.	Valutazione approfondita, convalida delle informazioni, monitoraggio continuo, avvisi, piani di miglioramento e audit basati su segnali o lacune.
Rischio medio	Dipendenza moderata o requisiti documentali rilevanti, con alternative disponibili.	Convalida dei dati critici, revisione strutturata, avvisi continui ed escalation in caso di modifica del profilo di rischio.
Basso	Basso impatto individuale e volume elevato di fornitori.	Analisi predittiva del rischio, valutazione dei dati esterni critici e monitoraggio senza coinvolgimento del fornitore; attivare l'escalation solo in presenza di segnali.

Questo approccio evita due errori comuni:

- Dedicare processi costosi a fornitori con una bassa esposizione senza migliorare la resilienza.
- Sottoporre i fornitori critici a verifiche documentali superficiali o sporadiche.

5. Estendi la visibilità oltre il fornitore diretto quando il livello di maturità lo consente

Una volta organizzata la base dei fornitori diretti, il passo successivo consiste nell'individuare le dipendenze nascoste tra fornitori di livello 2 e 3, stabilimenti, subappaltatori, componenti e rotte. Questa fase richiede la mappatura della supply chain, la collaborazione con i fornitori critici e, in alcuni casi, audit o verifiche aggiuntive.

L'Indagine globale sui rischi di Achilles 2026, condotta su oltre 2.800 organizzazioni, evidenzia l'ampiezza del divario: solo il 6% dichiara di avere una visibilità completa sui fornitori di livello 2 e 3, mentre quasi la metà ammette una visibilità limitata o nulla oltre la propria base diretta. Inoltre, solo il 18% si fida pienamente dell'accuratezza dei dati sulla sicurezza comunicati dai fornitori.

Per progredire senza cercare di mappare tutto in una volta:

- Inizia dai fornitori critici e dalle categorie per cui non esistono alternative.
- Individua materiali, ubicazioni, subappaltatori e rotte che concentrano l'esposizione.
- Dai priorità a Paesi, settori e componenti con un rischio intrinseco più elevato.
- Convalida le informazioni attraverso fonti esterne, documentazione, interviste o audit.
- Integra la mappa estesa nello stesso modello di avvisi e decisioni.

6. Monitora i segnali, non solo i documenti

Una certificazione valida oggi non elimina la possibilità di un'allerta finanziaria domani. Un fornitore qualificato può essere interessato da una sanzione, un attacco informatico, un conflitto, un cambio di proprietà o un evento climatico. Il monitoraggio deve rilevare i cambiamenti tra una valutazione e l'altra e attivare una risposta proporzionata.

Segnale	Perché è importante
Modifiche normative	Possono modificare i requisiti di qualifica, due diligence, contrattualizzazione o rendicontazione.
Allerte finanziarie	Anticipano problemi di capacità, liquidità, pagamenti o continuità.
Sanzioni e liste di controllo	Possono impedire un rapporto commerciale o richiedere controlli rafforzati.
Notizie negative e incidenti ESG	Incidono su reputazione, contratti, diritti umani e obblighi di legge.
Rischi informatici	Possono compromettere sistemi, dati, attività e terze parti collegate.
Eventi geopolitici o climatici	Modificano rotte, disponibilità, costi, tempi e accesso ai mercati.
Modifiche documentali o societarie	Rivelano scadenze, informazioni incomplete, acquisizioni o cambi di controllo.

7. Trasforma la mappa dei rischi in decisioni e piani di emergenza

La mappa genera valore solo se modifica le decisioni di acquisti aziendali, operations, compliance e management. Per ogni livello di rischio devono essere definiti azioni, responsabili, scadenze e criteri di escalation.

- Dare priorità agli audit ESG, agli audit di salute e sicurezza o di etica aziendale presso fornitori e regioni critiche.
- Richiedere piani di miglioramento con responsabili, evidenze e date di chiusura.

- Diversificare le fonti di approvvigionamento, le rotte o le ubicazioni in presenza di concentrazioni.
- Attivare un piano di emergenza per i fornitori che non possono essere sostituiti nell'immediato.
- Rafforzare i controlli contrattuali, documentali, informatici o finanziari.
- Sospendere nuove aggiudicazioni o attivare un'escalation verso l'ufficio legale e la compliance quando il rischio supera la soglia accettata.
- Sviluppare i fornitori strategici quando le azioni correttive sono più praticabili della sostituzione.

> **Regola decisionale**
>
> Ogni rischio rilevante dovrebbe rispondere a quattro domande: cosa può accadere? Quale impatto avrebbe? Chi deve intervenire? Entro quale termine?

8. Rivedi la mappa con una governance chiara

La gestione dei rischi regionali non è un esercizio annuale. Deve funzionare come un processo dinamico, con responsabili, soglie e una frequenza di revisione proporzionata alla criticità.

Come minimo, rivedi la mappa in caso di:

- Ingresso in una nuova regione o categoria.
- Inserimento o rinnovo di un fornitore critico.
- Modifica normativa, sanzione o restrizione commerciale.
- Incidente ESG, finanziario, operativo o informatico.
- Fusione, acquisizione o cambio di controllo.
- Perturbazione geopolitica, climatica o logistica.
- Peggioramento delle prestazioni o mancato rispetto di un piano di miglioramento.

Il DHL Global Connectedness Report 2026 evidenzia che il livello mondiale di globalizzazione si è mantenuto al 25% nel 2025, eguagliando il massimo storico registrato nel 2022. L'attività internazionale non sta scomparendo: si sta riconfigurando. Per questo, la resilienza della catena di fornitura dipenderà sempre più dalla capacità di individuare dove cambiano flussi e dipendenze.

Come Achilles può trasformare questo quadro in un processo operativo

Achilles consente di applicare diversi livelli di assurance all'intera base fornitori, da un primo livello di visibilità fino a valutazioni approfondite e audit. L'obiettivo non è aggiungere altre attività, ma concentrare gli sforzi dove possono ridurre maggiormente il rischio.

1

Ampia copertura con Achilles Risk Screening

Analisi predittiva e monitoraggio continuo, senza coinvolgimento del fornitore né questionari, per rilevare segnali ESG, finanziari, informatici e geopolitici, sanzioni, liste di controllo e notizie negative su grandi volumi di fornitori.

2

Processo di due diligence per i fornitori con maggiore esposizione

Valutazioni strutturate, dati e documenti convalidati e una visione comparabile delle prestazioni per supportare le decisioni di gestione dei fornitori e di acquisto.

3

Audit per ottenere un livello di affidabilità superiore

Audit documentali o in loco e, ove opportuno, interviste riservate ai lavoratori per verificare i controlli, individuare le lacune e definire azioni correttive.

4

Monitoraggio, avvisi e analisi in un'unica piattaforma

Informazioni aggiornate, dashboard e criteri configurabili per rilevare i cambiamenti, definire le priorità e condividere una visione comune tra acquisti, risk, compliance, ESG e operations.

5

Miglioramento e resilienza duraturi

Piani d'azione, monitoraggio delle non conformità e supporto ai fornitori per innalzare gli standard, ridurre l'esposizione e costruire una catena di fornitura sostenibile e pronta ad affrontare nuovi requisiti.

Scopri Achilles Risk Screening e l'approccio alla qualifica dei fornitori e alla gestione del rischio della catena di fornitura.

Checklist: valuta la maturità della gestione dei rischi regionali

Seleziona le azioni che la tua organizzazione svolge in modo sistematico. La checklist non sostituisce una valutazione formale, ma aiuta a individuare le lacune prioritarie.

Visibilità e segmentazione

☐ Abbiamo identificato i fornitori per Paese, regione, categoria, spesa e criticità.

☐ Sappiamo quali fornitori sono essenziali per continuità, compliance, sicurezza o reputazione.

☐ Distinguiamo la criticità operativa dal livello di rischio intrinseco.

Valutazione e due diligence

☐ Valutiamo i rischi geopolitici, normativi, finanziari, ESG, operativi e informatici per regione.

☐ Applichiamo diversi livelli di valutazione, convalida e audit in base all'impatto potenziale.

☐ Disponiamo di criteri di escalation per i fornitori il cui profilo di rischio cambia.

Monitoraggio e visibilità estesa

☐ Monitoriamo avvisi esterni, modifiche documentali e incidenti tra una valutazione e l'altra.

☐ Abbiamo visibilità sulle dipendenze di livello 2 o 3 nelle categorie critiche.

☐ Disponiamo di dati sufficientemente affidabili per prendere decisioni e giustificare il processo.

Azione e governance

☐ Definiamo piani di miglioramento, emergenza o sostituzione per i rischi rilevanti.

☐ Condividiamo le informazioni con acquisti, compliance, operations, ESG e management.

☐ Rivediamo la mappa quando cambiano fornitori, regioni, normative o condizioni operative.

Da 0 a 4 azioni	Livello iniziale: è opportuno organizzare la base fornitori e stabilire criteri di rischio comuni.
Da 5 a 8 azioni	Livello intermedio: esiste una base, ma mancano convalida, monitoraggio o coordinamento.
Da 9 a 12 azioni	Livello avanzato: l'organizzazione può concentrarsi su anticipazione, catena estesa e miglioramento continuo.

Conclusione: da una mappa statica a una gestione proattiva

Mappare i rischi regionali non significa accumulare dati. Significa costruire un'intelligence utilizzabile: sapere quale fornitore è importante, quale esposizione sta aumentando e quale decisione prendere prima che il rischio si trasformi in un'interruzione.

Le organizzazioni che combinano visibilità sui fornitori, criteri comparabili, dati convalidati, monitoraggio continuo e piani di miglioramento sono meglio preparate a operare in un contesto frammentato, regolamentato e in continua evoluzione. La resilienza inizia dalla capacità di individuare il rischio con sufficiente anticipo e trasformare questa visione in azione.

Domande frequenti sui rischi regionali e sui fornitori

Che cos'è la gestione del rischio della catena di fornitura?

È il processo di identificazione, valutazione, monitoraggio e riduzione delle minacce che, attraverso fornitori e terze parti, possono compromettere l'approvvigionamento, la compliance, la sicurezza, le finanze o la reputazione.

Come si devono segmentare i fornitori?

Combinando criticità e impatto con il rischio intrinseco. La spesa da sola non basta: occorre considerare anche la possibilità di sostituzione, l'accesso a sistemi o strutture, l'ubicazione, la normativa e l'effetto di un'interruzione.

Con quale frequenza deve essere rivista la mappa dei rischi?

I fornitori critici e ad alto rischio richiedono un monitoraggio continuo. Il quadro completo deve essere rivisto in caso di modifiche normative, incidenti, ingresso in nuove regioni, rinnovi contrattuali o cambiamenti rilevanti del fornitore.

Come migliorare la visibilità sui fornitori oltre il livello 1?

Dando priorità alle categorie e ai fornitori critici, richiedendo informazioni su subfornitori e ubicazioni, utilizzando fonti esterne e convalidando i punti di maggiore esposizione mediante mappatura della supply chain, due diligence o audit.