Oltre l'ESG: i rischi dei fornitori che possono bloccare la tua attività

Perché i dati ambientali, sociali e di governance sono necessari, ma non sufficienti, per proteggere la continuità operativa, la sicurezza e la reputazione di un'azienda.

Una catena di fornitura può presentare buoni indicatori ESG e, nonostante ciò, interrompersi domani.

La pressione normativa, alimentata da quadri come la CSRD e la CSDDD, dalla necessità di condurre analisi di doppia materialità, rendicontare le emissioni Scope 3 e rispondere alle aspettative di clienti e investitori, ha accelerato l'adozione di strumenti di analisi ESG. Questo progresso è necessario: consente di organizzare le informazioni sulla sostenibilità, confrontare i fornitori e migliorare la qualità della rendicontazione.

Il problema nasce quando queste informazioni vengono interpretate come una fotografia completa del rischio dei fornitori. Un fornitore può avere solide politiche ambientali e, allo stesso tempo, attraversare una crisi di liquidità. Può disporre di un codice etico e mantenere una vulnerabilità critica nel software con cui accede ai tuoi sistemi. Può rendicontare le proprie emissioni e presentare carenze nei controlli di qualità, nella sicurezza industriale o nella capacità operativa.

I dati più recenti mostrano perché questa distinzione è importante. Nel 2026, il 65% delle grandi imprese intervistate dal World Economic Forum ha indicato le vulnerabilità di terze parti e della catena di fornitura come il principale ostacolo alla resilienza informatica. Allianz ha classificato gli incidenti informatici come il principale rischio aziendale globale per il quinto anno consecutivo, con il 42% delle risposte.

CONCETTO CHIAVE

L'ESG è un livello informativo essenziale, non un sistema completo di controllo del rischio.

Una valutazione ESG aiuta a comprendere come un fornitore gestisce i propri impatti ambientali, sociali e di governance. La gestione dei rischi della catena di fornitura deve inoltre stabilire se il fornitore è in grado di continuare a consegnare, proteggere i dati, operare in sicurezza, rispettare i propri obblighi e resistere a un'interruzione.

1. Cosa mostra una valutazione ESG e cosa può lasciare fuori

Gli strumenti di analisi ESG strutturano dati che per anni sono rimasti frammentati: politiche ambientali, emissioni, diritti dei lavoratori, etica aziendale, diversità e governance. Aiutano inoltre a preparare la rendicontazione, individuare le lacune e avanzare verso una catena di fornitura sostenibile.

Tuttavia, il rischio dei fornitori non è suddiviso in compartimenti stagni. Alcuni fattori, come la salute e sicurezza o la cybersecurity, possono rientrare in un quadro ESG ampio, ma la loro gestione operativa richiede un livello di approfondimento molto maggiore rispetto a un indicatore generale o a un'autodichiarazione periodica.

Una valutazione ESG risponde generalmente a queste domande	La gestione integrata del rischio deve rispondere anche a queste domande
Quali politiche ambientali e sociali ha il fornitore?	Dispone della capacità finanziaria e operativa necessaria per rispettare il contratto?
Come misura e rendiconta le proprie emissioni?	Qual è il livello di dipendenza da quel fornitore, sito o subappaltatore?
Dispone di codici etici e di governance?	Ha accesso a sistemi, dati o infrastrutture critiche?
Dichiara di adottare pratiche in materia di salute e sicurezza?	Le qualifiche dei lavoratori, i permessi, le polizze e la documentazione sono ancora validi?
Soddisfa determinati criteri di sostenibilità?	Quali segnali indicano che il suo profilo di rischio sta cambiando in questo momento?

La differenza non sta nello scegliere tra ESG e gestione dei fornitori. Sta nell'integrare entrambi gli approcci in un modello multirischio, con dati verificati, segmentazione per criticità e monitoraggio continuo.

2. Rischio finanziario: anche un fornitore sostenibile può rimanere senza liquidità

La stabilità finanziaria è uno dei punti ciechi più evidenti di una valutazione incentrata esclusivamente sull'ESG. Insolvenza, deterioramento del flusso di cassa, dipendenza da pochi clienti o coperture assicurative insufficienti possono impedire a un fornitore di consegnare, mantenere il personale o rispettare gli impegni, anche quando le sue politiche di sostenibilità sono adeguate.

CASO REALE | Carillion: quando l'insolvenza diventa un'interruzione operativa

Cos'è successo. Il gruppo britannico Carillion è entrato in liquidazione nel gennaio 2018. Il suo crollo ha costretto il Governo del Regno Unito ad attivare misure di continuità per numerosi servizi e ha bloccato i lavori relativi a diversi contratti di costruzione, compresi due ospedali.

Cosa dimostra. La qualifica e i criteri ESG non sostituiscono il monitoraggio di solvibilità, liquidità, concentrazione dei ricavi, coperture assicurative e segnali di deterioramento. Senza queste informazioni, il rischio finanziario può concretizzarsi prima che la funzione acquisti disponga di un'alternativa pronta.

Per anticipare questo tipo di esposizione, la gestione dei rischi della catena di fornitura dovrebbe monitorare almeno:

- Cambiamenti nei rating finanziari, nei bilanci annuali e nei comportamenti di pagamento.
- Dipendenza economica da un cliente, un contratto o un mercato.
- Segnalazioni di insolvenza, contenziosi, pignoramenti o variazioni societarie.
- Validità e adeguatezza delle coperture assicurative.
- Disponibilità di fornitori alternativi e di un piano di emergenza.

3. Rischio informatico: ogni terza parte connessa amplia la superficie di attacco

La digitalizzazione della catena di fornitura ha moltiplicato le connessioni tra buyer, fornitori, piattaforme, operatori logistici e provider tecnologici. Questa efficienza crea anche dipendenze: una terza parte con accesso a dati, sistemi o credenziali può diventare il punto di ingresso di un incidente.

CASO REALE | SolarWinds: un fornitore affidabile trasformato in vettore di attacco

Cos'è successo. Nel 2020, la Cybersecurity and Infrastructure Security Agency degli Stati Uniti ha confermato lo sfruttamento attivo di versioni compromesse della piattaforma SolarWinds Orion. L'attacco ha utilizzato aggiornamenti software distribuiti da un fornitore legittimo per accedere alle organizzazioni clienti.

Cosa dimostra. La cybersecurity delle terze parti non può essere valutata soltanto all'inizio del rapporto. È necessario conoscere accessi, dipendenze tecnologiche, subappaltatori, controlli sugli aggiornamenti, risposta agli incidenti e variazioni del livello di esposizione.

Un questionario ESG può includere domande sulle politiche di protezione dei dati. Una gestione efficace del rischio deve andare oltre:

- Individuare quali fornitori accedono a sistemi, reti o informazioni sensibili.
- Valutare controlli, certificazioni, vulnerabilità e storico degli incidenti.
- Limitare i privilegi e riesaminare periodicamente gli accessi.
- Analizzare le dipendenze da software, cloud e fornitori di quarto livello.
- Definire protocolli di notifica, ripristino e continuità.

4. Qualità, capacità e sicurezza: rispettare le policy non garantisce una buona esecuzione

La continuità operativa dipende anche dalla capacità effettiva di un fornitore di produrre, installare, effettuare la manutenzione o erogare un servizio con la qualità e la sicurezza richieste. Sono quindi fondamentali competenza tecnica, tracciabilità, controllo delle modifiche, formazione, manutenzione, supervisione e storico degli incidenti.

CASO REALE | Alaska Airlines 1282: il costo della perdita di tracciabilità e del controllo di processo

Cos'è successo. Nel gennaio 2024, il pannello di chiusura di una porta di un Boeing 737-9 si è staccato durante il volo. Il rapporto finale della NTSB ha concluso che mancavano i bulloni di fissaggio e ha individuato come causa probabile l'inadeguatezza della formazione, delle istruzioni e della supervisione da parte di Boeing. Il componente aveva attraversato una catena di produzione e rilavorazione che coinvolgeva diverse organizzazioni e diversi team.

Cosa dimostra. I rischi di qualità e sicurezza richiedono evidenze operative: tracciabilità dei componenti, controlli delle modifiche, competenze, audit, registri di manutenzione e responsabilità chiare. Un buon indicatore ESG, da solo, non rileva un errore di processo.

La salute e la sicurezza richiedono un'ulteriore precisazione. Possono rientrare in una valutazione ESG, ma le aziende che impiegano appaltatori in siti critici necessitano di informazioni molto più specifiche: formazione obbligatoria, idoneità, permessi di lavoro, infortuni, assicurazioni, documentazione valida e controllo degli accessi.

Per questo motivo, in settori come energia, edilizia, utility, trasporti, marittimo e industria, la gestione documentale, il controllo di appaltatori e fornitori e, ove opportuno, una piattaforma per la gestione degli appaltatori fanno parte del sistema di prevenzione del rischio, non di un'attività amministrativa isolata.

5. Rischio normativo, geopolitico e reputazionale: il contesto può cambiare prima del fornitore

Un fornitore può mantenere esattamente le stesse pratiche e, nonostante ciò, vedere aumentare il proprio livello di rischio perché cambia il contesto. Una nuova sanzione, una restrizione commerciale, un conflitto, un'indagine, una modifica normativa o una notizia negativa possono influire sulla sua capacità di operare o sull'opportunità di mantenere il rapporto.

Questi rischi sono particolarmente difficili da gestire con valutazioni annuali. Richiedono il monitoraggio di liste di sanzioni, notizie negative, variazioni societarie, esposizione geografica, rotte logistiche e dipendenze da fonti uniche.

CAMBIO DI APPROCCIO

La qualifica indica se un fornitore soddisfaceva i requisiti in una data specifica.

Il monitoraggio continuo indica se continua a soddisfarli, se la sua esposizione è cambiata e se l'azienda deve intervenire prima che il problema raggiunga le attività operative.

6. Da fornitore qualificato a fornitore monitorato

La qualifica dei fornitori rimane una base necessaria. Consente di verificare i requisiti, organizzare la documentazione e stabilire una soglia di ingresso. L'errore consiste nel considerarla un punto di arrivo.

Il profilo di un fornitore cambia durante la validità del contratto. Può perdere una certificazione, subire un incidente informatico, ridurre il personale, cambiare proprietà, accumulare debiti, subappaltare un'attività critica o lasciare scadere la documentazione. Nessuno di questi cambiamenti è risolto dal fatto che il fornitore sia stato approvato dodici mesi prima.

Livello di controllo	Quali informazioni include	Quale decisione consente di prendere
Screening iniziale	Dati pubblici, ubicazione, attività, rischio intrinseco e segnali predittivi	Dare priorità ai fornitori che richiedono una due diligence più approfondita
Qualifica e convalida	Documenti, questionari, fonti esterne e requisiti del buyer	Approvare, approvare con riserva o rifiutare il rapporto
Valutazione specialistica	Finanza, cybersecurity, ESG, salute e sicurezza, assicurazioni, qualità e capacità	Attribuire un livello di rischio e controlli proporzionati
Audit	Evidenze relative al sistema di gestione, ai siti, ai processi e ai lavoratori	Confermare l'effettiva efficacia dei controlli e definire i miglioramenti
Monitoraggio continuo	Alert finanziari, sanzioni, notizie negative, scadenze, incidenti e variazioni societarie	Intervenire prima che il rischio provochi un'interruzione
Piani d'azione e di emergenza	Lacune, responsabili, scadenze, alternative e misure di continuità	Ridurre l'esposizione, sviluppare o sostituire i fornitori

7. Cosa dovrebbe includere una visione integrata del rischio dei fornitori

Una strategia solida non consiste nel richiedere più informazioni a tutti i fornitori indistintamente. Consiste nell'applicare il livello di controllo adeguato in base alla criticità, all'esposizione e al potenziale impatto.

- Visibilità sui fornitori: una base comune con ubicazione, categoria, spesa, criticità, accessi e dipendenze.
- Segmentazione del rischio: criteri coerenti per distinguere i fornitori critici, ad alto rischio, a medio rischio e a bassa esposizione.
- Analisi predittiva: un primo livello per individuare segnali nell'intera base fornitori, ancora prima di avviare processi di valutazione più approfonditi.
- Dati verificati: convalida documentale e confronto con fonti indipendenti, non soltanto autodichiarazioni.
- Valutazione multirischio: ESG, finanza, cybersecurity, salute e sicurezza, qualità, assicurazioni, compliance e continuità.
- Audit proporzionati: verifiche virtuali o in loco quando il livello di rischio richiede una maggiore assurance.
- Monitoraggio continuo: alert che rilevano i cambiamenti per l'intera durata del rapporto contrattuale.
- Piani di miglioramento e continuità: azioni con responsabili, scadenze, evidenze e alternative di fornitura.

Questo approccio migliora la resilienza perché trasforma le informazioni in decisioni: quali fornitori sviluppare, quali contratti rafforzare, dove effettuare audit, quando diversificare e quali rischi sottoporre a compliance, sicurezza, operations o direzione.

8. Come Achilles aiuta a collegare l'ESG a una gestione multirischio

Achilles consente di applicare diversi livelli di valutazione e assurance alla base fornitori. L'obiettivo non è sostituire l'analisi ESG, ma inserirla in una visione più completa del rischio e collegarla alle attività operative.

1	**Individuazione precoce del rischio** Analisi predittiva e segnali iniziali per dare priorità ai fornitori e individuare rischi nascosti in una base estesa.
2	**Valutazione e due diligence** Individuazione dei rischi e piani di mitigazione in base ai requisiti e al livello di criticità definito dal buyer.
3	**Assurance approfondita** Valutazioni specialistiche e audit per approfondire ESG, salute e sicurezza, qualità, etica, finanza e altri rischi.
4	**Monitoraggio e miglioramento** Audit, alert continui, analisi, piani d'azione e follow-up per mantenere aggiornate le informazioni e rafforzare la resilienza.

Scopri la piattaforma Achilles e il nostro approccio alla gestione integrata dei rischi dei fornitori.

Conclusione: l'ESG è essenziale, ma non è l'unico rischio

La sostenibilità deve continuare a far parte di qualsiasi strategia moderna di procurement e gestione dei fornitori. Tuttavia, un'azienda non protegge la propria catena di fornitura soltanto con indicatori ambientali, sociali e di governance.

La domanda decisiva non è soltanto se un fornitore è sostenibile. Occorre anche sapere se può continuare a consegnare, se è solvibile, se protegge i dati, se opera in sicurezza, se mantiene validi i propri requisiti e se l'organizzazione sarà in grado di reagire quando il suo profilo cambierà.

Una catena di fornitura resiliente si costruisce collegando l'ESG ai dati finanziari, informatici, operativi, documentali e di sicurezza, convalidando le informazioni e monitorando i segnali durante l'intero rapporto. È qui che il reporting smette di essere una fotografia e diventa una reale capacità di anticipazione.

MESSAGGIO FINALE

La valutazione migliore non è quella che raccoglie più dati, ma quella che permette di intervenire prima.

Quando procurement, sostenibilità, compliance, sicurezza e operations condividono una visione comune dei rischi dei fornitori, l'azienda può definire meglio le priorità, rafforzare i controlli e proteggere la continuità aziendale.

Domande frequenti

Che cos'è la gestione dei rischi della catena di fornitura?

È il processo di identificazione, valutazione, definizione delle priorità e monitoraggio dei rischi associati a fornitori, appaltatori, siti e dipendenze che possono influire sulla continuità, sulla compliance, sulla sicurezza o sulla reputazione di un'organizzazione.

Perché una valutazione ESG non è sufficiente?

Perché tende a concentrarsi sui fattori ambientali, sociali e di governance, mentre un fornitore può anche fallire per insolvenza, attacchi informatici, problemi di qualità, capacità insufficiente, documenti scaduti, sanzioni o incidenti di sicurezza.

Qual è la differenza tra qualificare e monitorare i fornitori?

La qualifica convalida i requisiti in un determinato momento. Il monitoraggio continuo rileva i successivi cambiamenti nel profilo finanziario, normativo, informatico, documentale o operativo del fornitore.

Tutti i fornitori richiedono lo stesso livello di valutazione?

No. Il livello di due diligence deve essere proporzionato alla criticità, al rischio intrinseco e al potenziale impatto. I fornitori a bassa esposizione possono iniziare con un'analisi predittiva, mentre quelli critici richiedono una convalida approfondita, audit e monitoraggio continuo.

Quale valore aggiunge un audit ESG all'interno di un approccio multirischio?

Fornisce evidenze sull'efficacia di determinati controlli ambientali, sociali e di governance. Deve essere integrato con altre valutazioni quando sono presenti rischi finanziari, informatici, operativi, di qualità o di salute e sicurezza.