

Anti-Financial Crime

Marzo 2026

a cura di:



Francesco Monini
Managing Director



Filippo Andrea Ravizza
Director



Emanuela Manzo
Manager

Dalla Finanza all'Industria della Difesa e Aerospazio: il modello di Risk Assessment Sanction, leva strategica per la Gestione del Rischio

Il settore della difesa e dell'aerospazio si confronta oggi con una crescente esposizione a rischi strategici che ne accrescono la complessità gestionale e la vulnerabilità.

Si consideri, ad esempio, il coinvolgimento in catene di fornitura globali, spesso caratterizzate da una complessa ricognizione geografica, la necessità di automatizzare l'analisi delle informazioni, dominare il cyberwarfare e la rapida evoluzione tecnologica nonché l'esigenza di un costante adeguamento ai frequenti pacchetti sanzionatori che incidono sulla libera circolazione delle merci. Ne consegue l'esigenza di gestire il rischio secondo un approccio strutturato che consideri non solo la conformità normativa ma la gestione dei big data, l'introduzione dell'AI nei modelli decisionali, una governance in grado di prendere decisioni consapevoli e veloci.

In tale prospettiva, l'implementazione di modelli strutturati per la valutazione e gestione di tali rischi – compresi quelli legati alle sanzioni internazionali, al riciclaggio, nonché i rischi reputazionali e di non conformità ai requisiti ESG – rappresenta oggi una prospettiva imprescindibile per assicurare la continuità operativa, la solidità strategica del comparto della difesa e aerospazio e la resilienza complessiva del comparto.

Premessa

Nel settore della difesa e aerospazio, la gestione dei rischi connessi alle sanzioni internazionali e al riciclaggio di denaro è diventata un elemento centrale della governance aziendale. La crescente complessità del quadro normativo, caratterizzato da regimi sanzionatori multilivello, dinamici e fortemente influenzati dal contesto geopolitico, impone l'adozione di presidi evoluti di compliance e risk management, capaci di garantire un costante allineamento ai requisiti legali e regolamentari.

Le sanzioni internazionali non si limitano alle tradizionali restrizioni commerciali e finanziarie, ma comprendono divieti settoriali, liste di soggetti designati, limitazioni sui beni dual use, tecnologie strategiche e servizi specialistici. L'introduzione delle sanzioni secondarie amplia ulteriormente il perimetro di esposizione, estendendo il rischio anche a soggetti terzi coinvolti indirettamente e rendendo necessario un controllo approfondito su controparti, clienti, fornitori e beneficiari finali.

La conferma della rilevanza di tali rischi è resa evidente dalla cronaca recente, che evidenzia un'attenzione crescente delle Autorità verso le violazioni in materia di export control, beni a duplice uso ed embarghi verso Paesi ad alto rischio. Numerose indagini hanno riguardato esportazioni illecite di componenti per droni e armamenti, trasferimenti societari sospetti e fenomeni corruttivi che hanno coinvolto imprese italiane e internazionali.

Negli anni Settanta, il caso che ha visto protagonista la [Lockheed Corporation](#), ha rappresentato il primo significativo momento di presa di coscienza della necessità di dotarsi di un framework di controlli interni solido e di garantire la compliance alle normative applicabili. La vicenda ha evidenziato in modo sistemico i rischi connessi a modelli operativi fondati sull'utilizzo di intermediari esteri, sull'operatività in giurisdizioni ad elevata esposizione geopolitica e su relazioni con controparti pubbliche. Proprio a partire da questo caso si è affermata l'esigenza di sviluppare presidi normativi e meccanismi di controllo oggi considerati imprescindibili, ponendo le basi per una visione integrata dei rischi di corruzione, riciclaggio e violazione dei regimi sanzionatori.

Un ulteriore precedente è rappresentato dal caso [Valsella Meccanotecnica](#), relativo all'esportazione di materiali militari verso l'Iran negli anni Ottanta. Pur collocandosi in un quadro geopolitico e regolamentare profondamente diverso da quello attuale, tale vicenda rappresenta un valido esempio delle ricadute di lungo periodo che la mancata osservanza dei vincoli all'export e degli embarghi internazionali può produrre, non solo sotto il profilo sanzionatorio, ma anche in termini politici, reputazionali e di credibilità istituzionale delle imprese coinvolte.

Anche in epoca più recente, indagini e procedimenti avviati dalle autorità nazionali hanno evidenziato come, nel comparto della difesa e delle tecnologie dual-use, possano emergere vulnerabilità operative legate alla gestione delle catene di fornitura internazionali, all'impiego di società intermedie e alla complessità dei flussi commerciali transfrontalieri verso Paesi caratterizzati da elevata sensibilità geopolitica e sanzionatoria.

Questi casi dimostrano come la gestione delle catene logistiche, l'attenzione alla **compliance normativa** nell'agire i propri processi di business e il controllo delle controparti/transazioni rappresentino fattori cruciali per la mitigazione del rischio nel comparto difesa e aerospazio. In tale contesto, l'adozione di modelli strutturati di Risk Assessment, mutuati dall'esperienza degli intermediari finanziari globali e adattati alle specificità del settore, consente di valutare in modo sistematico la probabilità e l'impatto dell'esposizione a sanzioni e flussi finanziari illeciti, rafforzando la resilienza operativa e la conformità alle normative nazionali e internazionali più stringenti. In sintesi: consente al management di prendere decisioni informate sulla base di rischi conosciuti e misurabili.

Riferimenti normativi

Il quadro giuridico disciplinante le sanzioni internazionali e le strategie di contrasto al riciclaggio nel settore della difesa e aerospazio è caratterizzato da un'operatività multilivello, coinvolgendo fonti multilaterali, europee e nazionali, oltre a raccomandazioni e best practice elaborate da organismi come il GAFI/FATF.

• Normativa Italiana

Il quadro nazionale è destinato a rafforzarsi significativamente con l'attuazione del Pacchetto AML/CFT europeo:

- Dal 2027 si applicherà il Regolamento AMLR (UE) 2024/1624, che estende obblighi uniformi di due diligence, governance e reporting anche a settori non finanziari ad alto rischio;
- L'Italia dovrà notificare entro il 2028 i settori ulteriori da assoggettare agli obblighi AMLR: il comparto difesa e aerospazio è un candidato naturale, data l'esposizione a supply chain sensibili, beni dual-use e controparti pubbliche estere. Ne deriva un rafforzamento atteso di KYC/KYD, screening sanzionatorio, controlli sui beneficiari effettivi, monitoraggio dei flussi finanziari e obblighi di segnalazione.

• Normativa UE

L'UE ha sviluppato un corpus normativo organico che integra sanzioni, export control, investimenti esteri e responsabilità penale:

- Il Regolamento Dual-Use (UE) 2021/821 impone programmi interni di compliance (ICP) e due diligence rafforzata su end-user e uso finale, recependo gli standard del Wassenaar Arrangement;
- Il Regolamento (UE) 269/2014 prevede asset freeze e divieti di messa a disposizione di risorse, estesi anche a entità controllate o interposte;
- La Direttiva 2009/43/CE disciplina i trasferimenti intra-UE di prodotti militari, rafforzando la tracciabilità delle supply chain;
- La Direttiva (UE) 2024/1226 armonizza le sanzioni penali per violazione delle misure restrittive.
- Il Regolamento FDI Screening (UE) 2019/452 e il Regolamento (UE) 833/2014 rafforzano il controllo su investimenti ed esportazioni verso la Russia e altri contesti sensibili.

• Normativa USA

La normativa USA esercita un impatto rilevante anche su operatori non statunitensi, per effetto della portata extraterritoriale delle sanzioni:

- CAATSA (2017) introduce sanzioni secondarie per soggetti che effettuino operazioni significative con il complesso militare-industriale russo, imponendo valutazioni rafforzate anche ai player europei;
- Le Sectoral Sanctions (OFAC Directives 3 e 4) limitano l'accesso a finanziamenti e vietano esportazioni verso soggetti della difesa russa;
- I regimi ITAR ed EAR disciplinano rispettivamente articoli militari e beni dual-use, richiedendo sistemi strutturati di classificazione, licensing, monitoraggio e audit;

- Gli Executive Orders (es. E.O. 14024) ampliano il perimetro delle restrizioni includendo entità collegate, anche indirettamente, a industrie strategiche o forze armate estere;
- Le raccomandazioni FATF qualificano il settore come ad alto rischio, imponendo controlli rafforzati, screening e obblighi di segnalazione.

Analisi dei rischi potenziali

Nel comparto della difesa, la mancata osservanza degli obblighi regolamentari citati espone a sanzioni non solo di natura amministrativa e penale (fino al 5% del fatturato globale, confisca dei beni impiegati o ottenuti tramite la violazione), ma anche al rischio di esclusione dai circuiti finanziari internazionali, all'interdizione da appalti pubblici alla perdita di affidabilità presso banche e assicurazioni e a gravi ripercussioni reputazionali e operative.

Nello specifico, le violazioni delle normative sanzionatorie possono assumere una **pluralità di forme**:

- **Violazione diretta**: coinvolgimento in operazioni con soggetti inseriti in liste sanzionatorie internazionali (ad esempio SDN List o Reg. UE 269/2014);
- **Istigazione e tentativo**: condotte penalmente rilevanti secondo la direttiva UE 2024/1226;
- **Mancata notifica**: omissione degli obblighi di comunicazione previsti dal DL 21/2012;
- **Non conformità alle condizioni imposte**: inosservanza delle prescrizioni tecniche contenute nei decreti autorizzativi;
- **Violazione indiretta** (compreso il rischio c.d. circumvention): utilizzo di triangolazioni attraverso paesi terzi o veicoli societari (SPV) per aggirare le restrizioni;
- **Rischio reputazionale e di vigilanza**: esposizione di intermediari finanziari e assicurativi coinvolti in operazioni critiche;
- **Inosservanza** delle tematiche ESG.

Ai fini della presente analisi, si approfondiscono i seguenti scenari di rischio:

- **Il rischio di circumvention**

Il fenomeno della circumvention rappresenta oggi uno dei profili di rischio più critici nell'applicazione dei regimi sanzionatori internazionali. Con tale termine si intende l'elusione indiretta delle restrizioni attraverso Paesi terzi che fungono da hub di transito o di riesportazione per beni e tecnologie soggetti a divieto.

Nel contesto post-2022, a seguito delle misure restrittive UE, USA e G7 contro la Russia, numerose analisi basate su dati Trade Map – ITC hanno evidenziato incrementi anomali dei flussi commerciali da parte di Paesi come Turchia, Emirati Arabi Uniti, Armenia, Georgia, Kazakhstan e Uzbekistan, che hanno significativamente aumentato le esportazioni di beni critici proprio mentre l'export diretto dall'Europa verso Mosca diminuiva.

La Commissione Europea, con le Guidance for EU Operators on Circumvention Risks del settembre 2023, ha invitato le imprese a implementare procedure di enhanced due diligence verso controparti localizzate in giurisdizioni considerate ad alto rischio, basandosi non solo su indicatori quantitativi di scambio commerciale, ma anche sulla natura dei beni coinvolti (e.g., dual use, avionica, semiconduttori, ottiche di precisione, etc.). Analoghe indicazioni provengono dagli Stati Uniti tramite il Russia Sanctions Evasion Global Advisory (2023) e il Tri-Seal Compliance Note (2024), che ribadiscono la responsabilità delle imprese – incluse quelle non statunitensi – nel prevenire triangolazioni o re-export vietati.

Sotto il profilo normativo, il rischio di circumvention è espressamente riconosciuto dalla Direttiva (UE) 2024/1226, che qualifica come reato non solo la violazione diretta delle misure restrittive, ma anche l'aiuto, l'istigazione e il tentativo di elusione. Ciò significa che un'impresa può incorrere in responsabilità anche laddove il bene non venga esportato direttamente verso un Paese sanzionato, ma raggiunga tale destinazione tramite un intermediario in una giurisdizione terza.

Per il comparto difesa e aerospazio, il rischio di circumvention è particolarmente rilevante poiché coinvolge beni ad alto impatto strategico e reputazionale. Componentistica avionica, droni, sistemi radar e semiconduttori figurano stabilmente tra gli articoli più ricercati attraverso canali di elusione, come confermato da diverse enforcement actions e dalle liste di beni critici stilate da UE, OFAC e G7. L'esposizione a tali schemi non comporta solo sanzioni finanziarie e penali, ma anche conseguenze reputazionali di lungo periodo, con possibili esclusioni da appalti NATO, bandi UE o progetti congiunti di ricerca e sviluppo.

In quest'ottica, la gestione del rischio circumvention non è solo un obbligo di conformità, ma un presidio strategico indispensabile per la tutela della posizione internazionale delle imprese del comparto difesa.

- **Il rischio reputazionale**

Il rischio reputazionale nel comparto difesa e aerospazio rappresenta un fattore critico che attraversa e amplifica tutte le dimensioni del rischio sanzionatorio e antiriciclaggio. A differenza di altri profili, non si limita a produrre impatti finanziari diretti: incide sulla credibilità istituzionale, sull'accesso ai mercati globali e sulla capacità di attrarre investitori, partner industriali e alleanze strategiche.

Le imprese del settore operano infatti sotto un livello di scrutinio pubblico e mediatico raramente riscontrabile in altri comparti. La sensibilità delle tecnologie coinvolte, la prossimità ai governi e il ruolo geopolitico delle forniture militari fanno sì che anche un singolo episodio di non conformità — fosse pure marginale, involontario o mediato da terzi (ad es. triangolazioni con Paesi soggetti a restrizioni, partnership con entità opache, utilizzo di subappaltatori non compliant) — possa tradursi in danni reputazionali profondi e duraturi. Le conseguenze vanno dalla revoca di licenze e dalla perdita di contratti, fino all'esclusione da gare internazionali e programmi congiunti di ricerca e sviluppo, con ripercussioni sulla stessa capacità dell'impresa di operare nei mercati strategici.

A ciò si aggiunge l'impatto sul rapporto con banche, assicurazioni e autorità di vigilanza: **un deterioramento reputazionale** può aumentare il costo del capitale, restringere l'accesso a linee di credito e innalzare la probabilità di controlli regolamentari. Anche la relazione con stakeholder non finanziari — fornitori, comunità locali, ONG e media — diventa vulnerabile, poiché la percezione di trasparenza e integrità è un elemento determinante per la sostenibilità operativa del settore.

In questo scenario, un ruolo crescente è svolto dal monitoraggio delle *negative news*: la semplice diffusione di notizie sfavorevoli su media internazionali o su banche dati specializzate può generare effetti reputazionali significativi, anche in assenza di accertamenti giudiziari definitivi.

In definitiva, la gestione del rischio reputazionale non è un accessorio né un'attività meramente cosmetica: è un vero abilitatore competitivo. Solo le imprese percepite come affidabili, trasparenti e pienamente conformi agli standard internazionali possono costruire relazioni solide e durature con governi, istituzioni multilaterali e partner industriali di primo piano.

• ESG e Risk Assessment

Infine, le tematiche ESG (*Environmental, Social, Governance*) stanno assumendo un ruolo sempre più rilevante anche nel comparto difesa e aerospazio, incidendo in modo diretto sia sulla valutazione del rischio sanzionatorio sia sulla percezione di affidabilità da parte degli stakeholder istituzionali e finanziari.

Sul versante ambientale, le imprese sono chiamate a dimostrare un approccio responsabile nella gestione delle risorse, nella riduzione delle emissioni e nell'adozione di pratiche sostenibili lungo l'intera catena di fornitura. La mancata conformità agli standard ambientali internazionali può infatti ampliare l'esposizione a rischi sanzionatori, soprattutto in ambiti tecnologici sensibili o basati su materiali critici.

Dal punto di vista sociale, assumono particolare rilievo i profili legati a potenziali violazioni dei diritti umani, all'impiego improprio di prodotti dual use o alla collaborazione con governi sottoposti a restrizioni internazionali. Tali fattori amplificano la probabilità di indagini e di danni reputazionali severi, rendendo indispensabile l'adozione di codici etici robusti e di procedure strutturate di *social due diligence*.

La dimensione della governance, infine, si intreccia in modo strutturale con la gestione del rischio sanzionatorio: assetti societari trasparenti, controlli efficaci sui beneficiari effettivi e consigli di amministrazione con responsabilità chiare in materia di compliance costituiscono elementi essenziali per prevenire violazioni, rafforzare la resilienza operativa e garantire credibilità nei confronti di investitori e istituzioni.

Integrare le considerazioni ESG nei modelli di *Sanctions Risk Assessment* non significa soltanto mitigare rischi legali e reputazionali, ma anche allinearsi alle aspettative di finanziatori, mercati e autorità di vigilanza, trasformando la compliance in un vantaggio competitivo concreto e duraturo.

Trasferibilità del modello di Risk Assessment Sanction dal contesto finanziario all'industria della Difesa e Aerospazio

Nel comparto della difesa e aerospazio, l'efficace gestione del rischio sanzionatorio rappresenta non solo una risposta ai requisiti normativi, ma anche una leva strategica per rafforzare la resilienza, la trasparenza e la competitività delle imprese.

Le imprese del settore della difesa e dell'aerospazio devono adottare un approccio proattivo e sistematico, basato su:

- Analisi preventiva delle controparti, dei beneficiari effettivi e della catena di fornitura;
- Valutazione del livello di esposizione ai rischi di sanzioni e riciclaggio per ciascuna operazione;
- Monitoraggio continuo dei flussi finanziari sospetti e revisione periodica dei modelli di controllo interno;
- Integrazione tra strumenti di screening, per individuare tempestivamente anomalie, tentativi di aggiramento o soggetti interposti;
- Formazione specifica del personale su tematiche sanzionatorie e antiriciclaggio.

In linea con gli elevati livelli di sensibilità del mercato e dai vincoli normativi internazionali stringenti, il Risk Assessment Sanction, si struttura su tre livelli, per garantire una valutazione dinamica e calibrata sulle specificità del settore:

1. **Rischio intrinseco (Intrinsic Risk):** tiene conto di fattori quali la presenza di programmi dual use, trasferimenti di tecnologie strategiche, rapporti con enti governativi o partner soggetti a restrizioni internazionali, e localizzazione geografica delle controparti, tipologia di canali distributivi e prodotti.

Per la gestione del rischio in operazioni con **prodotti dual use e materiali di armamento** (Regolamento UE 2021/821, Direttiva 2009/43/CE), gli operatori devono valutare non solo l'**end-user** ma anche l'**end-use** e i soggetti intermedi coinvolti nella catena di distribuzione. Operazioni dirette con Ministeri della Difesa o istituzioni governative offrono tracciabilità e autorizzazioni centralizzate, mentre l'impiego di rivenditori privati, subappaltatori o intermediari esteri comporta un maggiore rischio di **triangolazioni, re-esportazioni non autorizzate o diversioni verso Paesi soggetti a embargo**.

In merito alla **tipologia di prodotto**, la vendita di sistemi complessi (velivoli militari, satelliti, radar) è sottoposta a licenze rigorose e controlli multilivello (ITAR, autorizzazioni nazionali e licenze UE), fungendo da presidio di mitigazione. Al contrario, armi leggere, componenti modulari e munizionamento presentano un **rischio intrinseco più elevato** di deviazione verso soggetti non autorizzati, come evidenziato dalle FATF Typologies (2021) e dalle risoluzioni ONU sul traffico di armi leggere (UNSCR 2370/2017).

In sintesi, un **modello RA efficace** deve integrare:

- La mappatura dei **canali distributivi e dei livelli di intermediazione**;
- La **sensibilità del prodotto**, secondo normativa applicabile (e.g. ITAR, Reg. UE 2021/821);
- L'analisi dell'**end-user certificate** e dell'**uso finale dichiarato**.

L'adozione di **indicatori predittivi e scenari what-if** assume particolare rilievo nei contesti di rapido cambiamento geopolitico, come quelli legati ad aree di crisi o a mercati sotto embargo;

2. **Vulnerabilità (Vulnerability):** tiene conto della valutazione della robustezza dei presidi aziendali e include la verifica dei sistemi di controllo export, delle procedure di end-use/end-user, e dell'efficacia della formazione specifica per il personale. In particolare, test di robustezza e simulazioni di violazioni (e.g., red teaming su processi di fornitura e gestione supply chain, etc.) aiutano a identificare eventuali punti ciechi e a rinforzare la cultura del rischio, soprattutto in presenza di subappalti internazionali e forniture a soggetti pubblici;
3. **Rischio residuo (Residual Risk):** consente di evidenziare le aree di maggiore criticità che richiedono escalation immediata ai vertici aziendali o alle funzioni di compliance.

• Il modello di Risk Assessment

La valutazione del rischio su tre livelli è possibile attraverso l'utilizzo di un apposito **modello di calcolo** alimentato dai dati elementari che compongono gli indicatori di rischio (KRI). I KRI possono essere estratti e alimentati anche mediante il supporto di strumenti di intelligenza artificiale, che si rivelano particolarmente efficaci nell'analisi delle reti relazionali, nel monitoraggio continuo delle fonti di informazione (ad es., bad news), nell'analisi degli assetti proprietari e dei titolari effettivi (UBO), nonché nella gestione di volumi elevati di dati.

In tale prospettiva, l'intelligenza artificiale può supportare l'utente, affiancandolo nella fase di definizione e aggiornamento dei KRI attraverso l'individuazione di rischi emergenti. In particolare, l'utilizzo di approcci basati su grafi, integrati con modelli di intelligenza artificiale, consente di supportare la costruzione di scenari di rischio, anche mediante tecniche di intelligenza artificiale generativa, nonché di sviluppare capacità previsionali attraverso modelli avanzati, quali reti neurali. Tali strumenti permettono inoltre di simulare in modo continuativo scenari coerenti e plausibili (c.d. "simulazioni what-if"), in funzione dell'evoluzione dei fenomeni macroeconomici e geopolitici. Il modello prevede, inoltre, l'attribuzione di un peso a ciascun risultato – secondo scale di rischio semplici e intuitive (e.g. 1– 4) calcolate in base a misure statistico/matematiche, che generano oggettività nell'attribuzione delle misure e una corretta distribuzione dei pesi. Il peso attribuito a ciascun risultato contribuisce al calcolo del rischio finale, rappresentato all'interno di una matrice, utile a una lettura agevole per il Board e le funzioni di controllo. Rispetto al contesto finanziario, nel comparto della difesa e dell'aerospazio alcuni fattori di rischio devono assumere un **peso maggiore**. Tra questi rientrano, ad esempio, la filiera internazionale, la provenienza geografica delle controparti, l'esportazione di tecnologie dual use, l'adozione di sistemi di export control, le clausole sanzionatorie nei contratti, lo screening delle forniture indirette e le procedure per la gestione delle **sanzioni secondarie** (ad es. OFAC).

Di conseguenza, è essenziale considerare queste peculiarità nella selezione di un **dataset di indicatori di rischio**, sia qualitativi sia quantitativi, finalizzato a raccogliere informazioni relative, a titolo esemplificativo, a:

- **Presenza di relazioni con controparti estere:** oltre all'identificazione geografica delle controparti, è opportuno valutare se le stesse operino in giurisdizioni soggette a restrizioni dirette o indirette, anche in base a sanzioni secondarie (e.g. CAATSA); devono essere considerati i rischi connessi all'utilizzo di valute come il dollaro statunitense, che comportano automaticamente una competenza OFAC;
- **Operatività in Paesi soggetti a restrizioni:** la mappatura delle attività deve includere anche i canali di distribuzione e logistica, in quanto le triangolazioni con Paesi terzi possono costituire violazioni indirette (e.g. utilizzo di hub logistici in aree off-limits); è utile verificare l'esistenza di esenzioni o deroghe autorizzative connesse alle esportazioni dual-use;
- **Settore merceologico rilevante ai fini sanzionatori:** va condotta un'analisi aggiornata dei codici doganali (HS, CN, ECCN) per valutare se i prodotti siano soggetti a restrizioni ITAR, EAR o al Regolamento UE 2021/821; occorre tenere conto della combinazione di componenti: anche se il prodotto finale non è sanzionato, l'inclusione di sottosistemi controllati può esporre l'intera esportazione a violazioni;
- **Presenza di operazioni con soggetti pubblici esteri:** l'analisi deve considerare il grado di controllo statale sull'ente estero (es. >25% per la OFAC 50 Percent Rule) e valutare se sia incluso in liste di soggetti designati; è utile un controllo incrociato con banche dati ufficiali e l'adozione di meccanismi di enhanced due diligence in caso di PEP internazionali;
- **Partecipazione a joint venture o consorzi con partner esteri:** è utile mappare anche i rapporti indiretti di proprietà o influenza, per evitare violazioni derivanti da soggetti "nascosti" nei livelli societari;
- **Trasferimento di beni, tecnologie o know-how sensibili:** l'analisi deve includere anche i trasferimenti intangibili di tecnologia, ad esempio tramite licenze software, accesso a database o invii di documentazione tecnica; si raccomanda l'adozione di un Internal

Compliance Programme (ICP) conforme al Regolamento UE 2021/821 e l'integrazione nei flussi autorizzativi aziendali;

- **Presenza di clienti o fornitori con struttura societaria opaca:** è fondamentale accertare l'identità del titolare effettivo (UBO) e la presenza di eventuali trust, fondazioni o SPV che possano nascondere assetti proprietari; devono essere utilizzate fonti OSINT e database ufficiali per escludere collegamenti indiretti a soggetti designati o entità sanzionate;
- **Utilizzo di canali finanziari non trasparenti o ad alto rischio:** si deve verificare se i pagamenti transitano attraverso banche stabilite in giurisdizioni non cooperative o non conformi alle raccomandazioni FATF, o se vengono utilizzate modalità di pagamento frazionate, cash-based o con natura opaca; va prevista una segmentazione per valute e controvalori critici (ad es., soglia OFAC);
- **Esposizione a rischio reputazionale o investigativo:** è opportuno monitorare attivamente la presenza dell'ente o di suoi partner su banche dati di enforcement (es. OLAF, SIRENE, Procura, OFAC Enforcement Actions); l'adozione di una strategia di gestione proattiva delle crisi (inclusa comunicazione e risposta investigativa) rappresenta un fattore mitigante rilevante nel modello;
- **Presenza di esposizione contrattuale a terze parti (Third-party & Contractual Risk, AI-enabled):** oltre all'identificazione formale di fornitori, subappaltatori, agenti, distributori, partner di joint venture e system integrator, è opportuno valutare in che misura i contratti che regolano tali rapporti includano clausole efficaci in materia di sanzioni internazionali, export control, end-use, re-export, sub-contracting, audit e termination; a tal fine, l'utilizzo di soluzioni di Intelligenza Artificiale per l'analisi, l'indicizzazione e il monitoraggio continuo delle clausole contrattuali, consente di individuare lacune, incoerenze o variazioni di rischio derivanti dall'evoluzione dei regimi sanzionatori (UE, OFAC, ITAR, EAR, CAATSA) e prevenire violazioni indirette o fenomeni di circumvention tramite terze parti

Un modello preordinato alla raccolta di queste informazioni permette di facilitare l'esercizio e analizzare, più nel dettaglio, l'esposizione aziendale al rischio Sanction adottando le misure necessarie ad arginarlo.

Il modello di **Risk Assessment Sanction**, così strutturato, va oltre il semplice esercizio di compliance, configurandosi come uno **strumento di supporto decisionale** per il **Risk Appetite Framework (RAF)** aziendale. Misurando in modo sistematico il rischio intrinseco, le vulnerabilità e il rischio residuo, il Risk Assessment fornisce al management una rappresentazione oggettiva dei livelli di esposizione associati a specifiche giurisdizioni, settori merceologici o tipologie di controparti.

In questa prospettiva, i risultati del Risk Assessment diventano **input fondamentali** per definire le soglie di tolleranza al rischio (**risk tolerance**) e individuare le aree in cui l'impresa è disposta a sostenere determinati livelli di esposizione. Ciò consente al vertice aziendale di assumere **decisioni strategiche informate**, come ad esempio l'abbandono di mercati o geografie ritenuti troppo rischiosi sotto il profilo della compliance sanzionatoria, del rischio di circumvention o degli impatti reputazionali. Ciò risulta particolarmente rilevante se si considera che l'impiego di soluzioni di intelligenza artificiale consente di trasformare tale esercizio in un processo continuo, rafforzando la capacità dell'organizzazione di intercettare tempestivamente variazioni del profilo di rischio.

I modelli di Risk Assessment Sanction sono spesso integrati con l'intelligenza artificiale - algoritmi di machine learning possono essere addestrati su dataset specifici del settore difesa e aerospazio, utili ad analizzare pattern atipici nei flussi di materiali dual use, controllare la corrispondenza degli end-user dichiarati e automatizzare la verifica dei programmi di offset.

Conclusioni e supporto che Protiviti può fornire

In considerazione delle peculiarità del business e della dinamicità del contesto in cui l'intelligenza artificiale e i big data hanno un posto di spicco – la compliance non è solo un obbligo, ma un fattore abilitante di tutela del business, accesso a mercati, finanziamenti, gare internazionali e credibilità istituzionale cross border.

In questo contesto evolutivo, il nostro supporto alle aziende del settore difesa e aerospazio si concentra sulla progettazione e implementazione di framework di Sanctions Risk Assessment calibrati sulle specificità del business e sulle complessità delle catene di fornitura internazionali.

L'utilizzo di strumenti avanzati di analisi dei dati, il monitoraggio delle controparti e la valutazione delle relazioni indirette consentono di trasformare informazioni complesse in input significativi per i processi decisionali. Il Sanctions Risk Assessment si configura come leva strategica per la resilienza operativa, la sostenibilità reputazionale e la capacità di cogliere nuove opportunità di business anche in presenza di contesti strategici complessi.

Contatti

Francesco Monini

Managing Director
francesco.monini@protiviti.com

Cristina Peano

Managing Director
cristina.peano@protiviti.com

Enrico Ferretti

Managing Director
Enrico.Ferretti@protiviti.com

Filippo Andrea Ravizza

Director
filippoandrea.ravizza@protiviti.com

Emanuela Manzo

Manager
emanuela.manzo@protiviti.com