crime&tech TRANSCRIME Joint Research Centre on Innovation and Crime UNIVERSITÀ CATTOLICA del Sacro Cuore lab4 ems Università degli Studi di Palermo

La valutazione e gestione del rischio terze parti in Italia

Stato attuale e visione futura

Giugno 2024

La valutazione e gestione del rischio terze parti in Italia

Stato attuale e visione futura

Citazione suggerita: Crime&tech, Lab4Compliance e DEMS-Unipa, 2024, *La valutazione e gestione del rischio terze parti in Italia*, Milano: Crime&tech - Università Cattolica del Sacro Cuore

Con la collaborazione di:

Matteo Berbenni (Crime&tech/Transcrime)
Camilla Zupancich (Crime&tech/Transcrime)
Michele Riccardi (Crime&tech/Transcrime)
Antonio Bosisio (Crime&tech/Transcrime)
Marco Dugato (Crime&tech/Transcrime)
Andrea Merlo (DEMS - Unipa)
Enzo Bivona (DEMS - Unipa)
Costantino Visconti (DEMS - Unipa)
e associati di Lab4Compliance

ISBN: 978-88-99719-45-6

Progetto grafico : Ilaria Mastro

Crime&tech s.r.l.
Spin-off di Università Cattolica del Sacro Cuore (UCSC) - Transcrime
Largo Gemelli 1, 20123 Milano
Tel. +39 02 7234 3715/3716
info@crimetech.it
www.crimetech.it

Sommario

Transcrime (www.transcrime.it) è il Centro interuniversitario su criminalità e innovazione dell'Università Cattolica del Sacro Cuore, Alma Mater Studiorum Università di Bologna e Università degli Studi di Perugia. Fondato nel 1994, Transcrime è il principale hub di ricerca in Italia e in Europa per lo studio della criminalità organizzata e finanziaria. Ha condotto oltre 300 progetti a livello nazionale e internazionale, collaborando con enti di rilievo come le Nazioni Unite, la Commissione Europea, Europol, autorità di supervisione e forze di polizia a livello nazionale e internazionale. Sviluppa analisi dei fenomeni criminali complessi e applicazioni per le indagini finanziarie e la valutazione e prevenzione dei rischi associati alle terze parti per utenti pubblici e privati.

Crime&tech (www.crimetech.it) è lo spin-off universitario di Transcrime, che traduce le ricerche accademiche in analisi, soluzioni e strumenti per il settore pubblico e privato, per valutare, prevenire e ridurre i rischi di criminalità e per la sicurezza. È leader nella fornitura di indicatori di rischio per l'identificazione tempestiva di anomalie e imprese ad alto rischio e per la due diligence e il monitoraggio continuo di terze parti, come clienti e fornitori. Tramite l'impiego di approcci innovativi e AI, gli strumenti sviluppati da Crime&tech consentono la ricostruzione di strutture societarie e reti di relazioni complesse, la combinazione di banche dati e fonti non strutturate, e profilazione evoluta del rischio per lo svolgimento di indagini finanziarie e attività di due diligence sui partner commerciali.

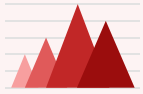
Lab4Compliance è la prima associazione in Italia composta esclusivamente da professionisti *in-house* della Compliance. Mission dell'associazione è quella di sostenere e promuovere la cultura dell'etica e della compliance e le relative best practices attraverso la creazione di molteplici occasioni di confronto, discussione e approfondimento nonché di supportare i professionisti del settore creando modelli, metodologie e best practices condivise e sempre più strutturate.

Il DEMS (Dipartimento di Scienze Politiche e Relazioni Internazionali) dell'Università di Palermo è un dipartimento interdisciplinare (cui afferiscono storici, giuristi, economisti, sociologi, psicologi e politologi) incentrato su di un obiettivo comune di ricerca: elaborare i diversi saperi che concorrono a delineare le "cornici cognitive" sottostanti al duplice processo di integrazione europea e di auspicabile creazione di un nuovo assetto internazionale fondato su principi universalistici. In questo orizzonte, assumono rilievo centrale -tra gli obiettivi di ricerca- le prospettive di integrazione/armonizzazione tra gli ordinamenti giuridici, incluse le strategie di contrasto della criminalità e progettazione di direttrici di politica criminale creati a livello sopranazionale. Il DEMS tra le altre cose supporta organizzazioni pubbliche e private nel disegno di politiche organizzative utili a prevenire fenomeni di criminalità organizzata, finanziaria e corruzione, con particolare riferimento al D.Lgs 231/2001 e altra disciplina rilevante in questo ambito

Executive Summary

Obiettivi dello studio

- Il presente studio nasce dalla collaborazione tra l'associazione **Lab4Compliance**, **Crime&tech** - spin-off company del centro di ricerca **Transcrime** dell'**Università Cattolica** del Sacro Cuore, e il dipartimento DEMS dell'**Università di Palermo**.
- L'obiettivo dello studio è approfondire un tema cruciale per gli operatori della compliance e della security di imprese, banche e pubbliche amministrazioni: la valutazione, la gestione, e la prevenzione dei **rischi legati alle terze parti** (*Third Party Risk Management - TPRM*).
- In particolare, lo studio si propone di:
  - Fornire una panoramica dei **principali ambiti normativi** che disciplinano, in maniera diretta ed indiretta, il TPRM: antiriciclaggio, anti-corruzione, codice degli appalti, 231/2001 e *corporate sustainability due diligence*;
  - Comprendere le **pratiche attuali** di TPRM di imprese e banche italiane, individuando i principali rischi e i tipi più ricorrenti di verifica su fornitori, sub-appaltatori, partner, clienti;
  - Analizzare gli **strumenti** e le **banche dati** più frequentemente utilizzate dagli operatori italiani per il TPRM;
  - Discutere le **criticità, le sfide e le opportunità future** nella valutazione e gestione dei rischi terze parti;
  - Elaborare un set di **raccomandazioni** per azioni future in questo ambito.
- Lo studio utilizza un approccio metodologico ibrido che combina:
  - **Analisi *desk***: rassegna della letteratura scientifica, istituzionale e delle fonti normative a livello italiano e internazionale;
  - ***Survey***: questionario somministrato ad oltre 50 imprese italiane attive in diversi settori, la maggior parte di esse (80%) con più di 1000 dipendenti;
  - **Interviste bilaterali e *focus group***: con esperti del settore, *compliance* manager, *security* manager, esperti di *internal audit* ed uffici acquisti, ricercatori accademici e rappresentanti di Lab4Compliance.



Principali risultati

Governance dei processi TPRM

- Rispetto al ciclo passivo (fornitori, sub-appaltatori), tra le imprese rispondenti del settore industriale e retail ogni anno in media vengono acquisite **400 nuove controparti**. Nel settore finanziario sono invece circa **950**.
- In media, di queste, il **31% è registrata all'estero o ha proprietà straniera** – il 25% nel settore finanziario.
- Nonostante questi numeri, e nonostante la maggior parte delle imprese italiane ne riconosca l'utilità, il 44% delle imprese interpellate non ha ancora adottato **regole o policy interne** che disciplinano il processo di TPRM.

- Il TPRM risulta un'attività spesso trasversale all'interno di un'azienda. Per il 38% delle imprese rispondenti è gestita **congiuntamente da diverse funzioni aziendali**, con una prevalenza di *compliance* e *security*.
- Se nel settore finanziario i controlli di TPRM sono diffusi su una percentuale elevata di terze parti, sia nel ciclo passivo che attivo, nel settore industriale e retail il 30% dei rispondenti effettua controlli, in media, solo su **un fornitore ogni quattro**.

Rischi

- Il **77% dei rispondenti** riporta di avere incontrato problematiche legate ai fornitori in almeno due aree di rischio.
- Le criticità più frequenti (50% dei rispondenti) riguardano la **sicurezza delle informazioni**, in termini di episodi di *data breach* e attacchi o tentativi di attacchi *cyber* subiti dalle terze parti.
- Al secondo posto, la **corruzione e i reati contro la pubblica amministrazione**, per circa un terzo dei rispondenti del settore finanziario (33%) e quasi la metà dei rispondenti negli altri settori (48%).
- Rilevanti anche gli incidenti sulle terze parti legati a **intermediazione illecita e sfruttamento del lavoro**, segnalati dal 39% dei rispondenti del settore non finanziario (54% considerando solo il mondo del lusso).
- Infine, se in media gli episodi di infiltrazione della **criminalità organizzata** sono stati rilevati sulle terze parti solo dal 10% dei rispondenti, questa percentuale sale al 66% per i rispondenti nel settore delle costruzioni e dell'energia.

Controlli, Banche dati, Strumenti

- Solo il 31% dei rispondenti adotta **controlli TPRM diversificati** a seconda dei rischi/reati presupposto, mentre il 69% adotta i medesimi controlli indipendentemente dai rischi valutati.
- I controlli si basano per la maggior parte sulle **cosiddette 'liste'**, ovvero sulla rilevazione del coinvolgimento di individui o società in casi precedenti di provvedimenti amministrativi o giudiziari ('*enforcement*') o in notizie di carattere negativo ('*adverse media*'), entrambe ricavate da fonti aperte e di stampa.
- Pur riconoscendone la validità, solo il 50% dei rispondenti del settore industriale e retail ricorre all'utilizzo di **indicatori di anomalia**, percentuale che aumenta in maniera significativa per banche ed altri soggetti obbligati anti-riciclaggio.
- Risulta diffuso l'utilizzo di banche dati e tool, con il 78% dei rispondenti che si avvale di strumenti forniti da provider terzi in modalità **'*software as a service*' (S-a-a-S)**. In generale, il ricorso a strumenti tecnologici appare più ampia per il settore finanziario che per quello industriale.
- La maggior parte dei rispondenti non risulta ancora pienamente soddisfatta degli strumenti in uso. Tra le esigenze più avvertite, la necessità di migliorare l'ampiezza della **copertura del dato** (48% dei rispondenti) e l'efficacia dei **sistemi di disambiguazione** dei *match* dei nominativi proposti (39% dei rispondenti).

Benefici, criticità e sfide future

- I **benefici** derivanti dai processi di TPRM rilevati dalle imprese italiane riguardano, in particolare, la protezione della reputazione aziendale; la prevenzione di provvedimenti legali o sanzioni amministrative o pecuniarie; la difesa della *business continuity* e il miglioramento della resilienza della *supply-chain*.
- Le principali criticità e le sfide future riguardano la **scarsa sensibilità aziendale** e la mancanza di processi aziendali chiari e strutturati per ciò che riguarda il TPRM. Un altro ostacolo rilevante riguarda la **frammentazione normativa** e la mancanza di una legislazione omogenea in questo ambito.

Conclusioni e raccomandazioni

- Lo studio propone anche delle riflessioni su come migliorare, in futuro, i processi di TPRM a livello di azienda e di sistema. In particolare, individua **10 temi chiave** su cui sono raccomandate azioni ed iniziative future, qui illustrate in sintesi (si veda il capitolo 'Conclusioni' per un'analisi approfondita).

1. TPRM come elemento chiave della valutazione dei rischi di un'organizzazione
2. TPRM come programma autonomo e trasversale su più ambiti normativi
3. TPRM come programma integrato tra diverse funzioni aziendali
4. TPRM come programma integrato e declinato nelle diverse aree di rischio
5. TPRM esteso al ciclo attivo anche nel mondo industriale? Dipende
6. TPRM oltre l'approccio basato sulle verifiche delle 'liste'
7. TPRM fondato su un approccio evoluto di indicatori di rischio e di anomalia
8. TPRM fondato sull'utilizzo di strumenti analitici avanzati
9. TPRM in una prospettiva 'glocal'
10. TPRM che guardi ai 'nuovi mondi': ESG e anti-riciclaggio allargato

Introduzione

Il presente studio è il risultato della collaborazione di tre attori:

Crime&tech, società spin-off del centro **Transcrime** di **Università Cattolica del Sacro Cuore**	l'associazione **Lab4Compliance**	il dipartimento **DEMS** dell'**Università di Palermo**

Lo studio nasce con l'obiettivo di approfondire un tema tanto cruciale nei processi gestionali di aziende (ed enti pubblici), quanto poco studiato e disciplinato: la **valutazione, gestione e prevenzione dei rischi delle terze parti** (TPRM = *Third Party Risk Management*).

Il concetto di **'terza parte'** (o controparte) è molto ampio e ricomprende qualsiasi persona fisica o giuridica, esterna ad un'azienda, con la quale un'azienda (o un ente pubblico) intrattiene, o potrebbe intrattenere, una relazione commerciale o di collaborazione. Inlcude, quindi, non solo la rete di fornitori, o di fornitori di fornitori (le cosiddette 'quarte parti') - ovvero il **'ciclo passivo'**, e la rete di clienti - ovvero il **'ciclo attivo'**-, ma anche altri soggetti come partner, concessionari, sponsor, *donor*, testimonial e altri intermediari. Ai fini di questo studio, ci concentreremo in particolare sulle terze parti del ciclo passivo (ad eccezione di quando espressamente citato).

Il processo, o l'insieme di processi, mediante il quale un'azienda o un ente pubblico identificano e gestiscono i rischi associati alle terze parti è detto ***Third Party Risk Management*** **(TPRM)**. Questo processo è generalmente (ma, come vedremo, non sempre) disciplinato da una policy interna che dovrebbe definire una governance della funzione e il *risk appetite* dell'organizzazione rispetto alle terze parti. Seguendo la classica logica dei processi di *risk management* così come prevista, tra gli altri, dallo standard ISO 31000, anche il TPRM si può strutturare in diverse fasi:

1. **Identificazione del rischio/i**: questa fase include l'identificazione delle terze parti da inserire nel perimetro della valutazione, e la natura dei rischi applicabili e associabili alle stesse. In questa fase viene dunque definito il *risk appetite* dell'organizzazione;

2. **Valutazione del rischio/i e classificazione delle terze parti**: in questa fase vengono valutati – ovvero misurati - i rischi applicabili alle terze parti, e vengono quindi classificate le terze parti dell'organizzazione in base al livello di rischio ad esse associato, che tenga conto sia delle criticità intrinseche alla controparte, che dell'impatto eventuale sull'organizzazione stessa.

3. **Gestione e mitigazione del rischio**: in questa fase vengono disegnate ed implementate alcune misure di mitigazione del rischio, proporzionate al livello di criticità della controparte e ai rischi per cui si è proceduto alla valutazione. Le misure implementate possono variare dall'introduzione di clausole a livello contrattuale, a forme di audit o *due diligence* rafforzate, fino a decisioni più drastiche, come la sospensione dei rapporti con la controparte in questione e – in taluni casi (ad esempio nel mondo dell'anti-riciclaggio) la segnalazione alle autorità competenti.

4. **Monitoraggio nel continuo**: una volta avvenuto l'*on-boarding* (ovvero letteralmente l' 'imbarco') di una terza parte, a seconda delle policy aziendali un'organizzazione può procedere ad un monitoraggio nel continuo della stessa, così da valutare se il suo livello di rischio rimane costante nel tempo.

Sebbene questo processo possa applicarsi a qualunque tipo di rischio associabile ad una terza parte, compresi

i rischi finanziari, di credito, o di continuità operativa, il TPRM si riferisce generalmente ai **rischi in ambito *legal* e *compliance***, nei casi di non conformità alle norme. Questo si traduce nella possibilità che la relazione con una terza parte possa causare a un'organizzazione "*sanzioni penali, amministrative, ammende, perdite finanziarie o danni reputazionali e di immagine conseguenti al mancato rispetto delle norme di legge vigenti, di regolamenti o codici di condotta*" (ANRA, 2024). A volte, queste fattispecie sono anche ricomprese sotto l'ombrello concettuale del **'rischio reputazionale'**, per quanto (come sarà discusso nel capitolo 3) non esista un consenso generalizzato sul significato operativo di quest'ultima nozione.

Se il processo di TPRM sulla carta appare chiaro e lineare, nella pratica pone **numerosi interrogativi**, sui quali ancora manca un ragionamento organico, soprattutto per quanto concerne la realtà italiana. Se si considera il contesto nazionale, la letteratura sul tema è virtualmente assente, con l'eccezione di alcune iniziative che hanno indagato aspetti specifici senza però dare vita ad alcun lavoro strutturato che possa fungere da guida per i professionisti in questo campo (Deloitte, 2021). Molti dei lavori citati in questo studio si riferiscono perciò al mondo anglosassone o a quello statunitense, che tuttavia possono solo in minima parte essere di orientamento per le imprese italiane – considerando le ampie divergenze normative e di cultura e *governance* aziendale.

Il presente studio intende cominciare ad affrontare questo gap conoscitivo, e a porre le basi per una riflessione condivisa sul tema, che unisca il mondo della **ricerca accademica** e quello delle **imprese e degli intermediari finanziari** e che possa produrre, nel lungo periodo, delle raccomandazioni e linee guida utili a tutti gli operatori in questo settore. In particolare, questo documento prova a rispondere alle seguenti domande:

- Perché il TPRM è importante per un'impresa?
- Quali sono gli ambiti normativi di riferimento per il TPRM?
- Come definire il rischio di una terza parte? Quali sono i tipi di rischio delle terze parti più rilevanti per le imprese italiane?
- Quali pratiche di TPRM sono più comuni tra le imprese italiane?
- Quali le strutture di governance del TPRM più frequenti?
- In che misura vengono usate banche dati e strumenti tecnologici per il TPRM?
- Quali le principali criticità e sfide presenti e future? E quali i benefici?
- Quali sono i temi chiave su cui impostare delle raccomandazioni per gli operatori?

Per affrontare queste domande di ricerca, il gruppo di lavoro si è avvalso di un approccio metodologico combinato, che ha integrato:

analisi desk di letteratura scientifica, istituzionale e di fonti normative, a livello italiano ed internazionale;

interviste bilaterali e *focus group* con esperti del settore - *compliance e security* manager, ed esperti legali di alcune tra le principali aziende italiane e in rappresentanza del Lab4compliance;

un questionario strutturato a cui hanno risposto più di 50 imprese italiane, attive in diversi settori, la maggior parte delle quali (80%) con più di 1000 dipendenti[1].

Le imprese rispondenti appartengono ai seguenti settori: food e GDO, retail e lusso (37%), attività finanziarie ed assicurative (17%), manifatturiero (14%), energy & utility (9%), trasporti (6%). Al questionario, che è stato disseminato su invito, era possibile rispondere in forma anonima.

Lo studio è strutturato come segue: il capitolo 2 tratteggia il contesto socio-economico e geopolitico in cui si innestano i processi di TPRM, e illustra i principali ambiti normativi, a livello nazionale, di riferimento; il capitolo 3 illustra le principali pratiche di valutazione e gestione del rischio terze parti in Italia, toccando temi legati alla governance del TPRM, agli ambiti di applicazione e alle modalità di valutazione, agli strumenti e alle banche dati utilizzate, ai benefici e criticità del processo; il capitolo 4 avanza delle prime riflessioni su temi chiave sui quali elaborare delle raccomandazioni e linee guida future.

2. Background e contesto

2.1. Il contesto socio-economico e geopolitico

In un'economia interconnessa e globalizzata come quella odierna, gestire il rischio associato alle terze parti è diventato imperativo per le aziende (OECD, 2018; Associazione Italiana Internal Auditors, 2019). Se da un lato il ricorso ad una ***supply-chain*** **sempre più ampia ed internazionale** è ormai necessario per aumentare la produttività, dall'altro abbattere i costi ed espandere i mercati aumenta in maniera esponenziale i rischi per l'organizzazione che se ne avvale.

La necessità di avere un processo efficace di TPRM è ancora più evidente alla luce del **contesto socio-economico e geopolitico** attuale, caratterizzato dal susseguirsi di eventi non sempre prevedibili. A partire dal 2020 la pandemia da Covid-19 ha comportato l'interruzione parziale o totale delle catene di fornitura, o comunque una completa revisione delle stesse, una rivoluzione delle modalità di consumo o di *delivery*. Secondo alcuni studi, le aziende che avevano destinato meno risorse al processo di TPRM sono quelle che hanno registrato gli incidenti di business *continuity* a più alto impatto (Deloitte, 2021).

Con il crescere delle tensioni geopolitiche, prima fra tutte l'**invasione russa dell'Ucraina**, e, più recentemente, l'inasprirsi del conflitto in **Medio Oriente** (con l'impatto sulle rotte commerciali, ad esempio nel Mar Rosso), il TPRM ha assunto un ruolo ancora più centrale nella buona *governance* aziendale. A partire dal 2014, in corrispondenza dell'invasione russa della Crimea, l'Unione Europea e diverse autorità a livello nazionale – innanzitutto gli Stati Uniti, tramite l'Office of Foreign Assets Control (OFAC) - hanno emanato una serie di **pacchetti sanzionatori** nei confronti di individui ed entità considerate legate al governo russo o comunque con un ruolo di supporto all'invasione in Ucraina.

Le misure restrittive imposte dall'Unione Europea, dall'OFAC e dalle altre autorità possono assumere diverse forme – tra cui restrizioni ai viaggi, alle esportazioni ed importazioni di particolari categorie merceologiche, congelamento dei beni – ma, dal punto di vista del TPRM, assumono particolare rilevanza quegli obblighi che comportano il **blocco dei fondi e delle risorse economiche** messe a disposizione delle persone presenti nelle 'liste sanzioni', o delle entità ad esse riconducibili, anche quando queste ultime non sono esplicitamente incluse negli elenchi sanzionatori: il cosiddetto principio del *sanctioned by extension* (Nicolazzo et al., 2024). La presenza di questi obblighi vincola qualunque operatore economico, impresa o banca, a valutare attentamente le relazioni con le proprie terze parti per verificare che queste non siano ricomprese all'interno di **liste sanzioni** e non siano **controllate da soggetti sanzionati** (per quanto la nozione di 'controllo' non sia sempre di facile determinazione pratica, soprattutto per quanto concerne la disciplina UE)[2].

2. Su questo tema si veda il progetto di ricerca europeo KLEPTOTRACE (www.transcrime.it/kleptotrace), coordinato da Transcrime, che ha di recente organizzato una formazione online su come individuare e tracciare catene di controllo di imprese e terze parti riconducibili a entità sanzionate dall'Unione Europea o dall'OFAC negli Stati Uniti. Il video del training è disponibile a questo link: https://transcrime.it/kleptotrace/second-kleptotrace-training-for-public-and-private-organisations/.

Accanto a questi eventi globali, vanno ricordati alcuni fenomeni tipici della realtà nazionale (benché non esclusivamente nazionali) che hanno storicamente esposto le imprese italiane, soprattutto di alcune regioni, a rischi considerevoli. In particolare, l'infiltrazione della **criminalità organizzata**, soprattutto mafiosa, e la **corruzione** rappresentano le principali minacce non solo da un punto di vista del riciclaggio di denaro (secondo quanto ribadito dall'ultima valutazione nazionale dei rischi AML/CFT – Comitato di Sicurezza Finanziaria, 2019), ma anche in termini di inquinamento della *supply-chain* e del tessuto imprenditoriale nazionale. Questi rischi risultano ancora più amplificati dall'evoluzione del fenomeno mafioso verso **forme più sottili e non violente di infiltrazione**, con un utilizzo sempre più frequente da parte delle organizzazioni criminali delle imprese come copertura per commettere reati fiscali, finanziari, fallimentari, e per riciclare denaro (DIA, 2023). Se a livello europeo l'86% delle reti criminali utilizza regolarmente le imprese (Europol, 2024), ciò significa che la possibilità che un fornitore o un'altra terza parte possano essere ricondotte a soggetti o schemi criminali deve essere contemplata in maniera seria e valutata con un processo di TPRM sistematico ed efficace.

2.2. Il contesto normativo

Ad oggi **non esiste una normativa specifica** applicabile universalmente in materia di controlli sulle terze parti. Nonostante la rilevanza del tema, le pratiche di TPRM si fondano su una spiccata **frammentarietà regolamentare**, in cui obblighi e prescrizioni derivanti da ambiti normativi diversi si intrecciano e sovrappongono, provocando spesso confusione tra gli operatori economici – e duplicazioni e sprechi di risorse (Associazione Italiana Internal Auditors, 2019).

Uno degli obiettivi di questo lavoro è proprio quello di sistematizzare, seppur in maniera sintetica, questo *corpus normativo* e offrire una **panoramica di tutti i principali ambiti regolamentari** che, a vario modo, incidono sulle pratiche di TPRM in Italia. In particolare:

- Antiriciclaggio e contrasto al finanziamento del terrorismo (AML/CFT);

- Anticorruzione;

- Responsabilità amministrativa degli enti (D.Lgs 231/2001);

- Normativa sugli appalti pubblici;

- Normativa sulla corporate *sustainability* due diligence (CSDDD).

I prossimi paragrafi illustreranno in estrema sintesi i principali obblighi e raccomandazioni in materia di valutazione del rischio delle terze parti previsti da ciascuno di questi ambiti normativi, elencati anche in maniera sinottica e comparata nella Tabella 1 di seguito.

	AML/CFT	Anticorruzione	Codice degli appalti	Responsabilità amministrativa enti ex D.lgs 231/2001	Diritti umani e norme ambientali (CSDDD)
Riferimenti normativi	*Tra gli altri*: Raccomandazioni FATF/GAFI; Direttiva UE/2018/843; D.lgs. 231/2007; D.Lgs 90/2017 e ss. modifiche.	*Tra gli altri*: L. 190/2012; Piano Nazionale Anticorruzione (ultimo aggiornamento 2022, e allegati); Linee Guida ANAC; UNI ISO 37001:2016;	*Tra gli altri*: Codice dei contratti pubblici (d.lgs. 36/2023)	D.Lgs. 231/2001	Corporate Sustainability Due Diligence Directive (CSDDD)
Terze Parti nel perimetro	Clienti	Clienti, fornitori, altre terze parti	Clienti, fornitori, altre terze parti	Clienti, fornitori, altre terze parti	Fornitori e 'quarte parti'
Valutazione del rischio	Sì	Sì, ma non esplicita sulle terze parti	Sì, ma non esplicita sulle terze parti	Sì, ma non esplicita sulle terze parti	Sì
Soggetti obbligati	Per elenco completo: • Art. 3, D.Lgs. 90/2017 e ss. modifiche. (si veda anche l'elenco in corso di aggiornamento secondo il nuovo pacchetto AML UE).	• Enti privati a controllo pubblico • Ordini professionali • Società a controllo pubblico	Tutti gli operatori economici (cfr. art. 65 d.lgs. 36/2023) affidatari di un appalto, di un contratto pubblico o di una concessione	Per l'elenco completo dei soggetti cui si applica il D.Lgs. 231/2001 si veda l'art. 1	• Grandi società europee • Imprese extra UE che rientrano nelle categorie precedenti
Obblighi concernenti la valutazione del rischio e i controlli sulle terze parti	• Identificazione del cliente e del titolare effettivo; • Comprensione dello scopo e la natura del rapporto; • Monitoraggio continuo del rapporto; • Monitoraggio delle transazioni;	Nessun obbligo esplicito sulla valutazione terze parti. Desumibile da analisi del rischio relativo a: • Contesto interno; • Contesto esterno.	Nessun obbligo esplicito sulla valutazione delle terze parti ma affidamento sulle capacità del contraente di selezionare al meglio i soggetti con cui intrattiene relazioni (art. 2 – principio della fiducia)	Nessun obbligo esplicito sulla valutazione terze parti	Verifica in materia di sostenibilità e diritti umani.

Tabella 1: Ambiti normativi e valutazione del rischio delle terze parti
Fonte: elaborazione Crime&tech

2.2.1 Antiriciclaggio e contrasto al finanziamento del terrorismo (AML/CTF)

La legislazione AML/CTF è stata la prima a definire chiaramente una serie di obblighi relativi alla valutazione dei rischi legati alle terze parti, focalizzati però esclusivamente sui clienti. Il cardine di questa normativa è l'approccio basato sul rischio (*risk based approach*), che deve guidare il comportamento dei cosiddetti 'soggetti obbligati' (ad esempio banche, professionisti, società di *gaming* – si veda più sotto) nei confronti della loro clientela: a maggiori rischi corrispondono obblighi con le terze parti più stringenti ed onerosi. In questo ambito intervengono tre diversi livelli:

- **Internazionale**: con gli *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation*, meglio conosciuti come '40 Raccomandazioni', elaborate dal Gruppo d'Azione Finanziaria Internazionale (GAFI/FATF), non normativamente vincolanti, ma con un carattere di *soft law*;
- **Comunitario**: con il novero di Direttive e Regolamenti emessi a partire dal 1991, ed in costante evoluzione (si veda il Box 1 per gli ultimi sviluppi in termini di pacchetto AML/CFT);
- **Nazionale**: con la legislazione risultante dal recepimento degli standard europei ed internazionali.

Per quanto riguarda il contesto italiano, il cuore della normativa AML/CTF è rappresentato dal d.lgs. 231/2007, dal d.lgs. 109/2007 e dal d.lgs. 90/2017 e successive modifiche. Oltre a prevedere un obbligo di monitoraggio delle transazioni e di conservazione delle informazioni al fine di consentire la tracciabilità dei flussi finanziari, questi testi normativi hanno introdotto un obbligo di **adeguata verifica della clientela** o *customer due diligence* (CDD), a volte meno precisamente definita come *know your customer* (KYC). L'articolo 18 del d.lgs. 90/2017 disciplina gli obblighi di adeguata verifica, tra cui:

- **L'identificazione e verifica dell'identità del cliente e del titolare effettivo**: attraverso la verifica del documento di identità o di altri documenti ottenuti da fonte affidabile e indipendente;
- **L'acquisizione di informazioni sullo scopo e la natura del rapporto**: tra le quali, in presenza di rischio elevato, anche quelle relative alla situazione economico-patrimoniale del cliente;
- **Il monitoraggio continuo del rapporto con il cliente**: attraverso l'aggiornamento continuo delle informazioni raccolte, della funzione di rischio associata al cliente e la verifica continua dei fondi e delle risorse nella disponibilità del cliente.

La quinta Direttiva UE AML/CFT (2018/843) ha ampliato il novero dei soggetti obbligati, che ora ricomprende, tra gli altri, **banche** ed altri intermediari finanziari, **professionisti**, e operatori non finanziari (tra cui **società di scommesse** e *virtual asset service providers*/**VASP**) e **pubbliche amministrazioni**[3]. Il nuovo pacchetto AML in discussione amplierà ulteriormente l'elenco (si veda Box 1 di seguito). Tuttavia, aldilà di questi aggiornamenti, questa disciplina continua a rimanere **settoriale**, non comportando obblighi per la gran parte delle imprese registrate in Italia ed altrove. Tuttavia, molte delle attività di valutazione sulla clientela condotte dai soggetti obbligati in ambito AML/CFT possono essere fonte di ispirazione anche per l'attività di TPRM di altre organizzazioni al di fuori dello stretto perimetro antiriciclaggio.

Alcune novità AML/CFT, con riflessi sul TPRM, verranno introdotte dal nuovo pacchetto legislativo su cui Consiglio e Parlamento europeo hanno raggiunto un accordo a gennaio 2024 (Consiglio dell'UE, 2024), e quindi votate dal Parlamento nell'aprile 2024 (Box 1).

3. Nello specifico, la lista di soggetti obbligati ora ricomprende: (a) Intermediari bancari, finanziari e assicurativi tra cui banche, istituti di pagamento, imprese di assicurazioni, società di intermediazione mobiliare, società di consulenza finanziaria, fiduciarie, mediatori creditizi, agenti che esercitano attività di cambio valuta; (b) Professionisti tra cui notai, avvocati, dottori commercialisti, revisori contabili, soggetti che forniscono servizi da periti, consulenti che svolgono attività in materia di contributi e contabilità; (c) Operatori non finanziari tra cui prestatori di servizi relativi a società e trust, soggetti che commerciano in opere d'arte o oro, attività di recupero crediti per conto terzi, prestatori di servizi relativi all'utilizzo di valuta virtuale, prestatori di servizi di gioco.

Box 1: Il nuovo pacchetto comunitario in materia AML/CFT

Il nuovo Regolamento e la nuova Direttiva AML/CFT andranno a costituire, tra gli altri, il cosiddetto "corpus normativo unico" in ambito AML/CFT, con l'obiettivo di armonizzare le norme in materia in tutta l'Unione. Tutte le norme applicabili direttamente al settore privato verranno trasferite nel regolamento, mentre la direttiva conterrà prescrizioni relative ai sistemi AML/CFT istituzionali degli stati membri. Tra le novità, alcune avranno un impatto significativo anche in materia di TPRM:

Soggetti obbligati

viene esteso l'elenco dei soggetti obbligati, facendovi rientrare anche le società e gli agenti operanti nel settore del calcio professionistico e i soggetti che commerciano in beni di lusso. Tra questi ultimi figurano commercianti di pietre e metalli preziosi, gioielli, orologi (sopra i 10.000 euro), auto di lusso (sopra i 250.000 euro), aerei e yacht (sopra i 7,5 milioni di euro).

Misure rafforzate di adeguata verifica

vengono introdotte misure rafforzate di adeguata verifica per i rapporti di corrispondenza transfrontalieri per i prestatori di servizi per le cripto-attività e per i rapporti d'affari con persone ad alto patrimonio netto.

Pagamenti in contanti

viene stabilito un limite massimo di 10.000 euro per i pagamenti in contanti in tutta l'UE. Inoltre, i soggetti obbligati dovranno identificare e verificare l'identità di persone che effettuano operazioni in contanti superiori ai 3.000 euro.

Titolarità effettiva

vengono armonizzate le norme sulla titolarità effettiva, fissando la soglia per l'identificazione del titolare effettivo a 25% e disciplinando l'accesso ai registri dei titolari effettivi nei paesi UE.

Paesi terzi ad alto rischio

i soggetti obbligati dovranno applicare misure rafforzate di adeguata verifica alle operazioni occasionali e ai rapporti d'affari che coinvolgono paesi terzi ad alto rischio, valutati sulla base degli elenchi del GAFI/FATF.

2.2.2 Anticorruzione

Il secondo ambito che prevede degli obblighi in materia TPRM è quello dell'anticorruzione. Il perno nel quadro normativo anticorruzione in Italia è rappresentato dalla **Legge n.190 del 2012**, che prevede degli obblighi specifici per un novero ristretto di organizzazioni – per quanto, per quelle non direttamente interessate, permangano gli obblighi anticorruzione derivanti dal D.Lgs. 231/01 (si veda sotto). La 190/2012 si applica ad una platea piuttosto ristretta di soggetti:

- Enti pubblici;
- Ordini professionali;
- Società a controllo pubblico;
- Enti di diritto privato con un bilancio superiore ai 500.000 euro le cui attività sono state finanziate prevalentemente da pubbliche amministrazioni per almeno due esercizi consecutivi nell'ultimo triennio.

Questi soggetti sono tenuti ad adottare – ad integrazione delle misure previste dal modello di organizzazione e gestione (MOG) 231 – un piano di prevenzione della corruzione fondato su una attenta valutazione dei rischi. Pur non includendo obblighi specifici relativi al controllo delle terze parti, la L. 190/2012 e il Piano Nazionale Anticorruzione (PNA) prevedono che le organizzazioni interessate effettuino una **mappatura puntuale dei rischi** che caratterizzano il **contesto esterno ed interno** dell'organizzazione ed i **processi** ad essa collegati, al fine di meglio individuare e prevenire i fenomeni di tipo corruttivo. Ne consegue, in senso lato, che una valutazione dei rischi corruttivi non può prescindere da una consapevole mappatura dei rischi dei soggetti - tra cui le terze parti (fornitori o beneficiari) - con cui le organizzazioni interessate si relazionano.

Per le pubbliche amministrazioni, i presidi anti-corruzione sulle terze parti sono da intendersi anche a **completamento degli obblighi AML/CFT** a cui anch'esse sono tenute ai sensi dell'art. 10 del D.Lgs 231/2007. È la stessa Autorità Nazionale Anti Corruzione (ANAC) che, con il Piano Nazionale Anticorruzione (PNA) 2022 e in un'ottica di integrazione funzionale[4], rileva che i presidi AML/CFT "*al pari di quelli anticorruzione, sono volti a fronteggiare il rischio che l'amministrazione entri in* ***contatto con soggetti coinvolti in attività criminali*** *soprattutto nell'impiego fondi del PNRR. Per questo, in più parti del PNA, sono stati evidenziati i raccordi necessari che è opportuno sussistano fra anticorruzione e antiriciclaggio*" (ANAC, 2023).

Un ulteriore importante riferimento proposto dal PNA, già nel 2016, è quello allo standard **UNI ISO 37001:2016**, la cui adozione viene riconosciuta come idonea a soddisfare le prescrizioni della L. 190/2012 (ANAC, 2017) e in cui si fa esplicito riferimento alla necessità di valutazione del rischio delle terze parti (Box 2).

Box 2: Anti-bribery Management System – ISO 37001:2016

La norma **UNI ISO 37001:2016** è uno standard volontario che definisce delle linee guida per aiutare le organizzazioni a prevenire, individuare e rispondere al rischio corruzione e a conformarsi alle legislazioni nazionali in materia di anticorruzione. Esso si applica a qualunque organizzazione, indipendentemente dalla tipologia e dalla natura delle attività svolte, e adotta una definizione piuttosto ampia di 'terze parti' che, oltre a fornitori e clienti, ricomprende anche i cosiddetti *business associate*, come:

Venditori e distributori

Agenti e rappresentanti

Partner in joint-venture e consorzi

4. Seguendo lo spirito del Piano integrato di organizzazione e attività (PIAO).

Lo standard prevede che l'organizzazione debba **identificare le terze parti rilevanti** e fornisce indicazioni su come effettuare la *due diligence* nelle aree individuate come a maggior rischio. In particolare, le imprese devono raccogliere una serie di informazioni utili ai fini della valutazione, tra le quali:

- Documenti relativi all'iscrizione al registro delle imprese, registrazioni delle scritture contabili, eventuali quotazioni in borsa;
- Verifica dei requisiti professionali e delle risorse necessarie per condurre l'attività oggetto del rapporto;
- Valutazione del sistema di gestione della corruzione (se presente);
- Valutazione di eventi e notizie negative relative alla controparte;
- Verifica dell'identità dei vertici aziendali.

2.2.3. Normativa sugli appalti pubblici e Codice degli appalti

Il "nuovo" **Codice dei contratti pubblici** (d.lgs. 36/2023) **non prevede specifici obblighi** di qualificazione delle terze parti ed è anzi improntato al **principio della fiducia** (art. 2), che si traduce anche in un generalizzato affidamento sulle capacità del contraente di selezionare al meglio i soggetti con cui intrattiene relazioni. Tale circostanza, tuttavia, non comporta il venir meno della esigenza di una corretta procedura di valutazione delle terze parti. Piuttosto, il nuovo testo normativo sembra rinviare a un sistema in cui tale pratica appartiene alle consuete **prassi aziendali** delle imprese intenzionate a restare nella filiera – breve o lunga che sia – delle forniture della pubblica amministrazione.

Va infatti considerato che una delle caratteristiche principali del nuovo codice dei contratti pubblici consiste - almeno per quel che qui rileva – nel venir meno della maggior parte dei limiti al subappalto (cfr. art. 119) e nella reintroduzione dell'appalto integrato (art. 44). Tale alleggerimento regolatorio, tuttavia, ha come risvolto un aumento del rischio per le imprese di trovarsi coinvolte in **filiere opache** che possono legittimare l'attivazione delle misure di **prevenzione patrimoniali** di cui al Codice antimafia (D.lgs 159/2011). Si allude, in particolare alle misure **dell'Amministrazione giudiziaria** e del **Controllo giudiziario**, istituti rispettivamente previsti dagli art. 34 e 34 bis Cod. ant, con i connessi contraccolpi sul versante gestionale e reputazionale.

Sicché, diviene cruciale per le imprese dotarsi di efficaci procedure per **TPRM** (possibilmente integrate nel Modello di organizzazione di cui al d.lgs 231/231: si veda paragrafo successivo), specie con riferimento alla commissione dei **reati-catalogo di cui al Codice antimafia**. Si segnala a tal proposito che, oltre ai reati di **criminalità organizzata** e a quelli **contro la pubblica amministrazione**, il reato di **sfruttamento del lavoro** è divenuto in certi distretti giudiziari uno dei principali presupposti applicativi della misura dell'amministrazione giudiziaria. Con riferimento a quest'ultima fattispecie, va peraltro considerato che il Codice degli appalti prevede specifici **oneri per gli operatori economici** di "garantire le stesse tutele economiche e normative per i lavoratori in subappalto rispetto ai dipendenti dell'appaltatore e contro il lavoro irregolare" (art. 102). Tale garanzia dev'essere oggetto di una specifica comunicazione da inserire nell'offerta circa "le modalità con le quali intende adempiere". In altri termini, **sotto l'aspetto delle tutele dei lavoratori, l'operatore economico deve chiarire in che modo seleziona i subappaltatori**. Il mancato assolvimento dell'onere appena descritto, tuttavia, non va incontro a precise sanzioni, atteso che la mancata qualificazione dei subappaltatori non è inserita nell'elenco tassativo (la tassatività è affermata all'art. 11) delle cause di eslusione obbligatorie o facoltative (previste rispettivamente agli artt. 94 e 95).

Una qualche forma qualificazione delle terze parti è infine accennata all'art. 119 del Codice dei contratti pubblici, nell'ambito della disciplina del subappalto, laddove si prevede la possibilità per la stazione appaltante di limitare l'esecuzione dell'appalto al solo aggiudicatario "in ragione dell'esigenza di rafforzare […] il controllo delle attività di cantiere e più in generale dei luoghi di lavoro o di garantire una **più intensa tutela delle condizioni di lavoro e**

della salute e sicurezza dei lavoratori ovvero di prevenire il rischio di infiltrazioni criminali". Il Codice prevede che tali limitazioni possano essere superate qualora i "subappaltatori siano **iscritti nell'elenco dei fornitori, prestatori di servizi ed esecutori di lavori** di cui al comma 52 dell'articolo 1 della legge 6 novembre 2012, n.190, oppure **nell'anagrafe antimafia degli esecutori** istituita dall'articolo 30 del decreto-legge 17 ottobre 2016, n. 189, convertito, con modificazioni, dalla legge 15 dicembre 2016, n. 229". Anche in questo caso va tuttavia specificato che la mancata qualificazione dei subappaltatori non è inserita nell'elenco tassativo delle cause di esclusione.

2.2.4. La responsabilità amministrativa degli enti: il D.lgs. 231/2001

Tra gli ambiti normativi che contengono, esplicitamente o non, previsioni sui controlli relativi alle terze parti, quello afferente al decreto legislativo 8 giugno 2001, n. 231 (di seguito decreto 231/2001), appare sicuramente il più completo, sia per il perimetro di applicazione ad una **vasta gamma di soggetti**, sia per l'ampio **catalogo di reati presupposto** coperti (si veda sotto).

Il decreto 231/2001 attribuisce agli enti una responsabilità amministrativa – del tutto equiparabile ad una responsabilità penale – per i reati commessi nel loro interesse/vantaggio da soggetti qualificati interni all'organizzazione, e specificatamente da **soggetti apicali** (ad esempio amministratori, manager, direttori) o persone sottoposte alla loro direzione o vigilanza. In particolare, l'ente può essere ritenuto responsabile se, prima della commissione del reato da parte di uno di questi soggetti qualificati, non si era dotato di un **modello di organizzazione e gestione** (MOG) capace di prevenire questi reati.

Destinatari del decreto 231 sono "*gli enti forniti di personalità giuridica, le società fornite di personalità giuridica e le società e le associazioni anche prive di personalità giuridica*" (art. 1, comma 2), categoria ampia di soggetti che ricomprende, seguendo anche le più recenti pronunce giurisprudenziali (per una rassegna si veda Confindustria 2021):

- **Imprese**: indipendentemente dalla dimensione, dal settore economico, dal controllo (privato, pubblico, o misto pubblico-privato) in cui operano[5];
- **Associazioni** e organizzazioni senza scopo di lucro;
- **Fondazioni** ed enti con scopi benefici o sociali.

Nonostante l'ampio perimetro di applicazione, l'adozione di un Modello 231 è comunque volontaria per la maggior parte degli enti. Fanno eccezione le **imprese quotate sul segmento STAR** di Borsa Italiana (Borsa Italiana, 2024), e, per prassi ormai consolidate, le imprese che devono accreditarsi in alcuni settori specifici (come quello sanitario o formativo, perlomeno di alcune regioni italiane). Come anticipato, il catalogo dei reati presupposto 231 (artt. 24 e ss.) ha negli anni subito un significativo ampliamento e ricomprende ora numerose categorie, tra le quali i **reati corruttivi e contro la pubblica amministrazione** e il suo patrimonio (artt. 24 e 25), i reati di **criminalità organizzata** (art. 24-ter), reati di ricettazione, **riciclaggio**, auto-riciclaggio e impiego di denaro (art. 25-octies), **reati ambientali** (art. 25-undecies), reati legati a **immigrazione clandestina** (art. 25-duodecies), **reati tributari** (art. 25-quinquesdecies) e numerosi altri.

Venendo alle implicazioni in termini di **TPRM**, è utile sottolineare che il decreto 231/2001 non prevede esplicitamente un obbligo di valutazione del rischio e controllo delle terze parti; tuttavia si può affermare che questa attività discenda da un'efficace attuazione del MOG, posto che quest'ultimo deve prevedere, tra le altre cose, "*misure idonee a garantire lo svolgimento dell'attività nel rispetto della legge e a* ***scoprire ed eliminare tempestivamente situazioni di rischio***" (art. 7, comma 3). Considerato che l'attività di un'organizzazione non si svolge in un ambiente asettico, bensì è per sua natura permeata di relazioni con soggetti terzi (clienti, fornitori, partner, intermediari), un'efficace prevenzione dei rischi rispetto ai reati presupposto 231 deve passare necessariamente da una attenta valutazione dei rischi delle terze parti.

5. Fanno eccezione le imprese individuali, perchè, secondo alcune pronunce giurisprudenziali, la disciplina 231 è applicabile solo ai soggetti collettivi (si veda, tra gli altri Cass., VI sez. pen., 30085/2012).

Questo assume ancora più importanza considerando che la responsabilità dell'ente può sussistere anche qualora il soggetto qualificato, autore dell'illecito, abbia concorso nella sua realizzazione con **soggetti terzi esterni** all'organizzazione, tra i quali, a titolo di esempio, società appaltatrici, partner, *contractor* o *sub-contractor*, e altri intermediari. L'ipotesi di concorso è ravvisabile anche nei casi in cui l'organizzazione abbia adottato **procedure carenti nella selezione delle terze parti**, ad esempio in termini di:

- Omessa valutazione preliminare circa la sussistenza di requisiti di legge in capo ai fornitori/società appaltatrici, o dei requisiti di onorabilità e professionalità;
- Mancato utilizzo di alcuni parametri e indici di valutazione delle terze parti previsti dalla legge (o dalle prassi consolidate), come ad esempio l'iscrizione in albi o liste rilevanti (es. iscrizione della terza parte in *white list* prefettizie antimafia);
- Procedure carenti in termini di criteri economici di aggiudicazione di lavori e servizi in appalto, e mancata valutazione della congruità dei costi (ad esempio in termini di salute e sicurezza sul lavoro) (Confindustria, 2021);

È importante sottolineare che le carenze dei modelli 231 in termini di valutazione delle terze parti sono stati recentemente richiamate, in più occasioni, anche dall'autorità giudiziaria come elemento discriminante per l'applicazione di misure di **Amministrazione Giudiziaria** ex Art. 34 Codice Antimafia (D.lgs 159/2011) (si veda un esempio nel Box 3). Alla luce di queste considerazioni, un processo efficace di TPRM appare non solo come un approccio auspicabile per una piena implementazione della logica sottostante la disciplina 231/2001, ma come una **componente essenziale di qualsiasi MOG 231**. Semmai, la questione è come declinare i processi di TPRM rispetto all'ampio catalogo di reati presupposto – e di terze parti – previsti dal perimetro del D.lgs. 231/2001, ovvero se debba prevedersi un processo unico o articolato rispetto agli stessi. Questo tema sarà discusso nel capitolo 3 e 4.

Box 3: Amministrazione giudiziaria, TPRM e criticità nei modelli di organizzazione e gestione ex 231/2001

In un recente caso relativo ad una società di grandi dimensioni, quotata in borsa, proprio le criticità riscontrate nel MOG 231 rispetto ai processi di approvvigionamento e di qualifica fornitori hanno costituito un elemento essenziale per l'Autorità Giudiziaria al fine di rilevare la rimproverabilità colposa della medesima organizzazione rispetto ai tentativi di infiltrazione della criminalità organizzata nella *supply-chain*:

> *È emerso che il Modello 231 e i presidi di controllo presenti all'interno delle procedure organizzative cui gli attori del processo dovevano far riferimento per il processo approvvigionamenti, in particolare per la qualifica e la selezione dei fornitori, non fossero completamente idonei a prevenire le suddette fattispecie di reato. In particolare è stato rilevato […] che le procedure non contemplavano tutti i* ***presidi di controllo suggeriti dalle*** **best practices** *di riferimento in materia di sistema di controllo interno […]. In concreto: non erano disciplinate le modalità con cui* ***verificare l'onorabilità dei fornitori****; non erano disciplinati controlli in merito al* ***mantenimento dei requisiti di onorabilità e professionalità*** *dei c.d. "fornitori storici", ovvero quei fornitori con cui erano maturati rapporti consolidati nel tempo e caratterizzati da particolare apprezzamento della fornitura ricevuta; i criteri previsti per determinare l'affidamento senza effettuare una "esplorazione" di mercato risultavano generici, lasciando quindi discrezionalità agli attori del processo; […] le procedure non facevano riferimento a verifiche di controparte relativamente ai* ***subappaltatori****; analogamente nelle procedure non erano richiesti, indicati e/o specificati i controlli da espletare per poter autorizzare il subappalto. Si evidenzia, inoltre, come le* ***procedure non risultassero tra loro coordinate****, anche per effetto dell'utilizzo di denominazioni discordanti e richiami generici, lasciando, per alcuni aspetti, un'ampia incertezza applicativa.*

(Decreto di revoca dell'Amministrazione Giudiziaria per la società OMISSIS, p. 6-7).

2.2.5. Diritti umani e norme ambientali: la *Corporate Sustainability* Due Diligence Directive (CSDDD)

Negli ultimi anni ha assunto particolare rilievo il dibattito rispetto ai cosiddetti principi **ESG – *Environmental, Social, Governance*** – che dovrebbero fungere da orientamento per imprese, banche, enti pubblici nel raggiungimento di un'attività sostenibile dal punto di vista ambientale, sociale ed etico [6]. In base a questi principi, un'impresa dovrebbe essere in grado di disegnare in maniera sostenibile la propria attività e la rete di relazioni con le sua intera catena di fornitura. Tuttavia, nonostante l'ampio consenso attorno a questo paradigma, a questo dibattito è raramente seguita una riflessione concreta su come declinare i principi ESG nell'attività operativa di un'organizzazione, in particolare nel rapporto con le sue terze parti.

Questo dibattito dovrebbe però trovare una ricaduta concreta già nei prossimi mesi, con l'entrata in vigore della Direttiva (UE) relativa alla *due diligence* di sostenibilità delle imprese, meglio conosciuta come **CSDDD - *Corporate Sustainability Due Diligence Directive*** che mira ad armonizzare gli obblighi di adeguata verifica riguardo la sostenibilità delle attività operative delle imprese e della loro *supply-chain*. In particolare, la proposta di Direttiva si propone di definire i requisiti di *due diligence* che le aziende saranno tenute ad adottare lungo l'intera catena di fornitura al fine di individuare, mitigare, prevenire e porre fine ai rischi delle proprie attività (e quelle dei suoi fornitori e 'quarte parti') in termini di violazione dei diritti umani e delle norme ambientali (European Commission, 2022; Eurosif et al., 2023). L'obiettivo della Direttiva è quello di armonizzare i requisiti di *due diligence* in materia di sostenibilità in tutta l'Unione, sostituendo il mosaico di normative ad oggi vigenti.

Dopo un primo apparente arenamento, dovuto al mancato accordo tra Consiglio e Parlamento europeo, il 24 aprile 2024 il Parlamento europeo ha approvato il **testo definitivo della CSDDD** con alcune modifiche (su spinta di alcuni paesi membri, tra cui Italia e Germania) che hanno riguardato principalmente una riduzione del suo ambito di applicazione (Council of the European Union, 2024)[7]. Come esito finale della negoziazione, una volta formalmente adottata dal Consiglio Ue, la CSDDD si applicherà alle:

Società nei paesi membri UE con almeno **1.000 dipendenti**;

Società nei paesi membri UE con almeno **450 milioni di euro** di fatturato globale;

Società **extra UE**, con dimensioni e fatturato generato nell'UE in linea con le precedenti categorie[8].

6. Il termine *Environmental* fa riferimento ad alcuni criteri utili per valutare come un'azienda opera da un punto di vista di sostenibilità ambientale; il termine Social afferisce all'impatto sociale di una organizzazione con il suo contesto sociale, ed in particolare il territorio, i dipendenti, le terze parti e la comunità di relazioni con cui interagisce; il termine *Governance* fa riferimento a criteri di 'sana' gestione aziendale, sia in termini etici e di compliance normativa, che di altri principi legati al rispetto di dipendenti e stakeholders, trasparenza delle politiche aziendali, retribuzione dei dipendenti, rispetto delle minoranze.

7. Il testo sarà pubblicato nella Gazzetta Ufficiale della UE entro l'autunno e i paesi membri avranno un periodo di due anni per recepire il testo a livello nazionale.

8. Nella proposta originaria, si trattava di società europee con oltre 500 dipendenti e più di 150 milioni di euro di fatturato; società europee di medie dimensioni (con oltre 250 dipendenti e 40 milioni di euro di fatturato) però esposte a rischi particolari in virtù delle attività svolte.

I servizi finanziari sono al momento esclusi dall'ambito di applicazione, così come le piccole e medie imprese – che però vi potrebbero rientrare indirettamente in quanto coinvolte in qualità di **fornitori e sub-fornitori** all'interno delle *supply-chain* delle società obbligate.

La CSDDD pone una serie di obblighi, per quanto (ancora) generici, che mirano a promuovere la sostenibilità aziendale e la responsabilità sociale, sottolineando l'importanza di una gestione oculata dei rischi legati alle attività aziendali, in particolare alle relazioni con le terze parti (Peta, 2024). Gli obblighi nel particolare coprono:

1. **Integrazione del dovere di diligenza**: le aziende devono integrare il dovere di diligenza nelle politiche e nei sistemi di gestione del rischio, illustrando l'approccio aziendale e come vengono implementate *due diligence* e verifica della conformità.

2. **Individuazione e valutazione degli impatti negativi**: le imprese interessate devono realizzare una mappatura e valutazione approfondita delle operazioni per identificare le aree di rischio.

3. **Adozione di strumenti di segnalazione**: le aziende devono stabilire strumenti di segnalazione e canali di reclamo accessibili e trasparenti per coloro che esprimono preoccupazioni legittime sugli impatti negativi, sia potenziali che effettivi.

4. **Coinvolgimento efficace delle parti interessate**: le aziende devono impegnarsi in consultazioni trasparenti ed efficaci con dipendenti, sindacati, consumatori e altre entità il cui interesse potrebbe essere influenzato dalle operazioni aziendali.

5. **Prevenzione degli impatti negativi**: le imprese interessate devono adottare misure appropriate (richieste di conformità contrattuale o sviluppo di piani di azione) per prevenire, arrestare o minimizzare gli impatti negati sui diritti umani o sull'ambiente.

6. **Verifica, monitoraggio e valutazione**: le imprese devono effettuare valutazioni periodiche delle misure di *due diligence* per valutare l'implementazione e l'efficacia dei sistemi di identificazione, prevenzione e mitigazione degli impatti negativi.

7. **Rendicontazione**: le aziende devono rendere conto della politica e delle misure di due diligence in conformità alle disposizioni legislative pertinenti.

Le nuove disposizioni di *due diligence* rappresentano un significativo spostamento verso una maggiore responsabilità sociale e ambientale da parte delle imprese. Tuttavia, è importante riconoscere che l'attuazione efficace di queste misure richiede tempo, risorse e un impegno costante da parte delle imprese.

3. Le pratiche di valutazione e gestione del rischio terze parti in Italia

Alla luce dell'assenza di un unico riferimento regolamentare per ciò che concerne il TPRM e della frammentarietà regolamentare, con obblighi dispersi su più ambiti normativi, risulta ancora più importante capire **come le imprese italiane hanno implementato, nella prassi, i processi di valutazione e gestione del rischio delle terze parti**. In questa sezione vengono presentati i risultati dell'indagine svolta sulle pratiche di TPRM più diffuse a livello italiano, integrando la letteratura sul tema con quanto emerso dai *focus group* con gli esperti in materia e dal questionario compilato da 50 delle principali aziende italiane[9].

3.1. La governance della funzione TPRM

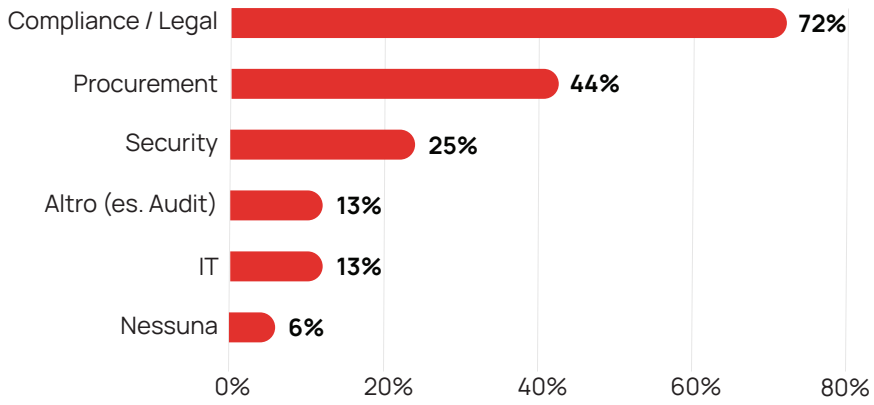
I pochi studi a livello internazionale che ad oggi hanno indagato le dinamiche di governo della funzione TPRM sono concordi nell'individuare l'eccessiva **decentralizzazione e frammentazione dei processi di valutazione delle terze parti** come una delle principali problematiche della *compliance* aziendale (Deloitte, 2022; McKinsey & Company & ORIC International, 2017); criticità che talvolta si suggerisce di affrontare semplicemente tramite l'*outsourcing* del TPRM a società specializzate. Dall'analisi svolta sul campione di imprese che hanno partecipato al questionario emerge che una parte consistente (**44% dei rispondenti**) **non ha adottato regole o policy interne** che disciplinano il processo di TPRM. Tale percentuale scende al 22% se si considerano le aziende che hanno un modello di organizzazione e gestione (MOG) ex 231/2001.

Come già sottolineato da studi precedenti, la quantità di risorse umane destinate al processo di TPRM varia molto a seconda della dimensione dell'organizzazione analizzata (Ernst & Young, 2018). La survey conferma questa tendenza, con il 60% delle aziende con più di 1.000 dipendenti in cui la funzione di TPRM è supportata da **più di 10 addetti**, che diventano **meno di 5** per le imprese sotto i 1.000 dipendenti.

Le risorse umane dedicate al TPRM possono essere afferenti a più aree funzionali. Nel campione analizzato, la *due diligence* delle terze parti viene **gestita da più funzioni nel 38% dei casi,** denotando quindi la natura 'trasversale' del TPRM nei processi e aree aziendali. In Figura 1 sono rappresentate le aree funzionali più coinvolte nella fase di *due diligence*. Se la funzione compliance è coinvolta nel 72% dei casi, il *procurement* e la *security* risultano coinvolte rispettivamente per il 44% e il 25% dei rispondenti.

9. Come ricordato sopra, al questionario, che è stato disseminato su invito attraverso la rete di contatti in imprese e banche di Crime&tech, Transcrime e Lab4Compliance, era possibile rispondere in forma anonima.

Figura 1: Coinvolgimento delle funzioni aziendali nella due diligence delle terze parti
Fonte: elaborazione Crime&tech



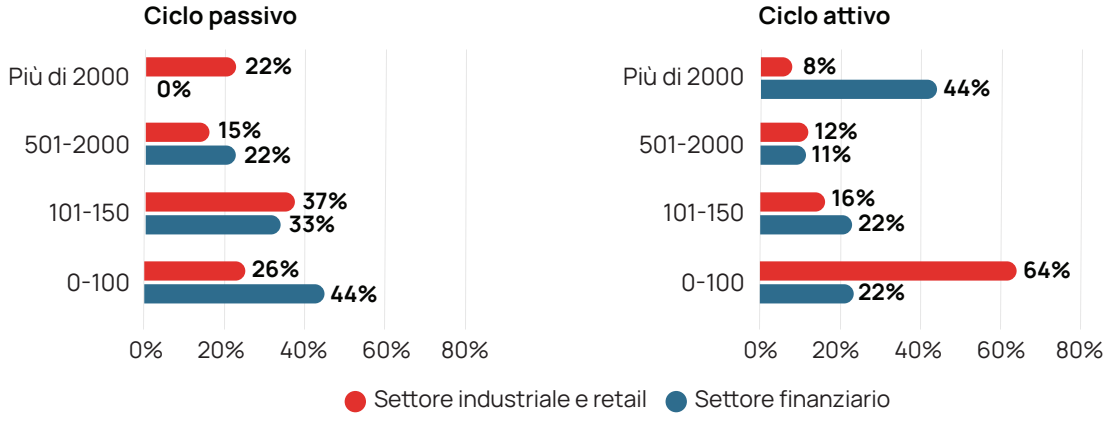
3.2. Ambiti di applicazione e processi di valutazione

Come anticipato sopra, uno degli aspetti fondamentali per comprendere le pratiche più diffuse di TPRM tra le aziende italiane è quello di esaminare il **perimetro di applicazione dei controlli** messi in atto da queste imprese. Fino ad oggi, non ci sono stati studi in Italia che abbiano cercato di distinguere tra i diversi tipi di terze parti, indagando a quali rischi espongono l'organizzazione e come questa **adatti i suoi controlli in base alla controparte esaminata**. Inoltre, benché vi sia consenso sulla necessità di estendere la *due diligence* anche al ciclo attivo e alle cosiddette 'quarte parti', manca una riflessione organica sul tema (KPMG, 2022).

L'importanza di questi controlli diventa ancora più chiara dal momento in cui si analizzano i numeri delle nuove controparti con cui le imprese italiane si interfacciano ogni anno. In termini assoluti, il numero medio di nuove controparti nel settore industriale e retail è pari a circa 400, mentre in quello finanziario a circa 980 (ciclo passivo). Per quanto riguarda invece il ciclo attivo, i numeri tendono a crescere: nel settore industriale e nel retail i rispondenti dichiarano di acquisire circa 4.100 nuove controparti all'anno, mentre nel settore finanziario circa 14.900[10].

Andando più nel dettaglio, i risultati della survey rilevano che per quanto riguarda il ciclo passivo, nel settore industriale e nel retail, il 22% delle organizzazioni intervistate dichiara di avere più di 2.000 nuove controparti ogni anno, il 15% tra le 500 e le 2.000, e il 27% tra le 100 e le 500. Per quanto riguarda il settore finanziario, facendo riferimento al ciclo attivo il 44% dei rispondenti dichiara di acquisire più di 20.000 nuove controparti ogni anno.

Figura 2: Nuove controparti con le quali le aziende si interfacciano ogni anno
Fonte: elaborazione Crime&tech



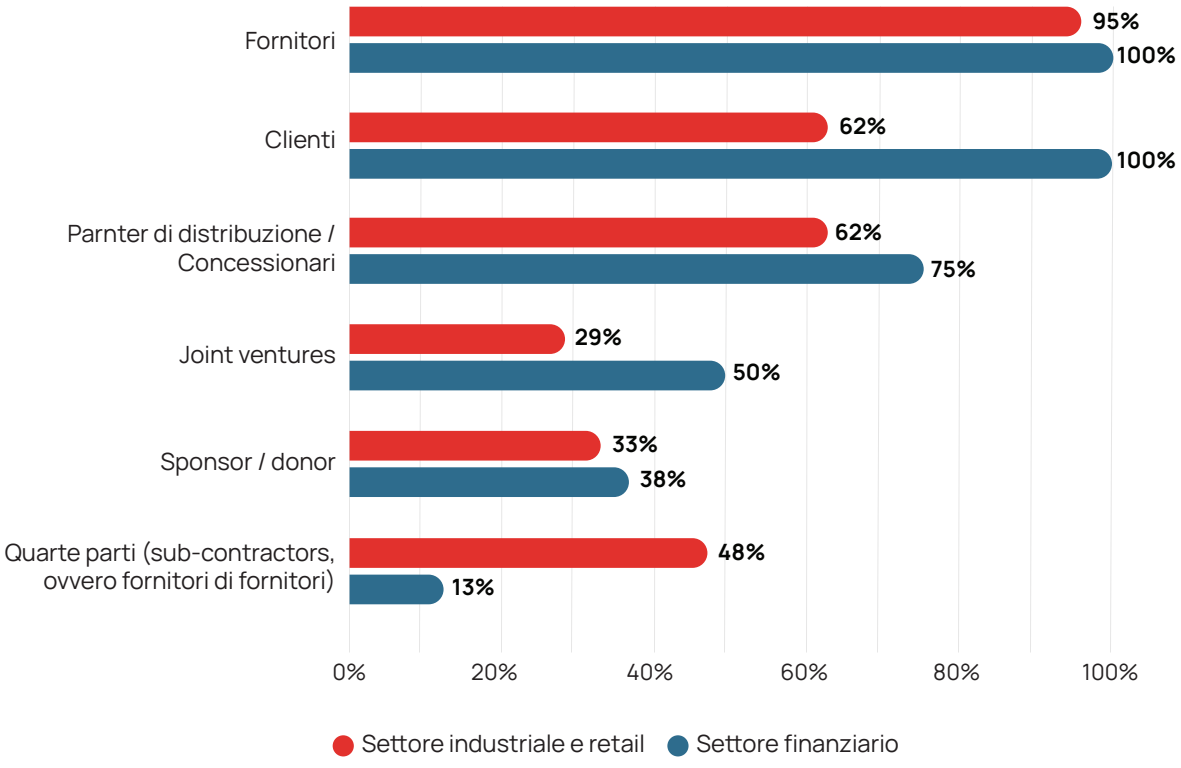
10. Il numero medio di controparti è stato ottenuto calcolando la mediana di ciascun range di valori e successivamente moltiplicandola per la percentuale totale dei rispondenti per ogni range.

Degno di nota è anche il fatto che una quota rilevante di controparti con le quali le imprese italiane si interfacciano sono **estere o hanno proprietà estera**, rispettivamente circa il 31% nel settore industriale e retail e il 25% in quello finanziario.

La prima parte del questionario si è quindi concentrata sul tipo di terze parti oggetto di valutazione, i rischi esaminati e i tipi di controlli effettuati.

Come visibile in Figura 3, le controparti più coperte dai processi di TPRM in Italia sono i **fornitori**, valutati rispettivamente dal 100% dei rispondenti operanti nel settore finanziario e dal 95% di quelli operanti nel settore industriale. Le differenze settoriali si ampliano soprattutto con riguardo al ciclo attivo. Se la totalità degli istituti finanziari interpellati esegue **controlli di TPRM sui clienti** – come lecito immaginare considerati gli obblighi di adeguata verifica della clientela in ambito AML/CFT (vedi sopra) – sorprende la percentuale elevata (62%) di rispondenti degli altri settori[11] che eseguono valutazione sui clienti (probabilmente guidata da operatori nel settore del lusso e del manifatturiero di alta gamma). Ancora bassa, invece, la percentuale dei rispondenti che effettua controlli sulle **quarte parti** – poco meno della metà nel settore industriale e retail, e solo il 13% in ambito finanziario.

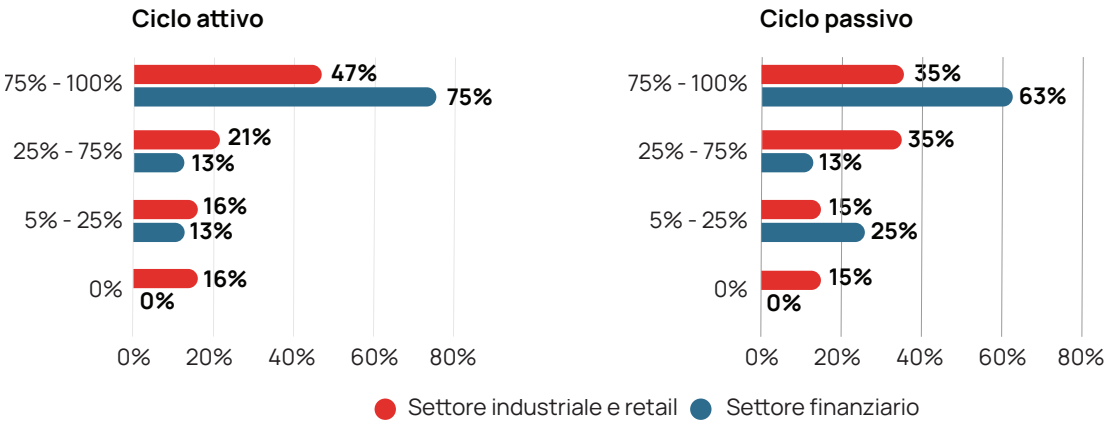
Figura 3: Terze parti rientranti nel perimetro di controllo TPRM delle imprese italiane
Fonte: elaborazione Crime&tech



La maggiore propensione del settore finanziario alla sistematicità dei controlli delle terze parti, soprattutto sul ciclo attivo, è desumibile anche da quanto riportato in Figura 4, che riporta la porzione di controparti soggette ai controlli di TPRM. Più interessante notare, invece, che il 30% dei rispondenti del settore non finanziario effettua controlli solo su un **massimo del 25% del ciclo passivo**: significa che, in media, solo 1 su 4 fornitori è soggetto a qualche genere di verifica o *screening*.

11. Sono inclusi nella categoria 'settore industriale' operatori afferenti a segmenti variegati tra cui food e grande distribuzione, settore del lusso, manifatturiero, energy & utility e trasporti.

Figura 4: Percentuale di terze parti soggette a controlli di TPRM
Fonte: elaborazione Crime&tech



Questi dati si scontrano con l'esposizione effettiva dei rispondenti ai diversi tipi di rischio. Prendendo come riferimento una versione ridotta del catalogo dei reati presupposto 231/2001, abbiamo chiesto al nostro campione di imprese italiane quali **problematiche legate alle terze parti sono state sperimentate negli ultimi due anni**. I risultati sono riportati in Tabella 2[12]. Solo un rispondente ha dichiarato di non aver riscontrato incidenti, mentre, in media, il 77% dei rispondenti riporta di avere incontrato problematiche in due o più aree di rischio. Le problematiche più frequenti hanno riguardato la **sicurezza delle informazioni** (in termini di *data breach*, attacchi o tentativi di attacchi cyber), che hanno interessato più del 50% delle imprese in entrambi i settori.

Al secondo posto la **corruzione e i reati contro la pubblica amministrazione**, per circa un terzo dei rispondenti del settore finanziario e quasi la metà dei rispondenti negli altri settori (48%). Particolarmente significativi per il settore finanziario i rischi relativi ai reati di **riciclaggio, finanziamento del terrorismo** e alle **sanzioni internazionali** - probabilmente questi ultimi 'trainati' dai controlli AML/CFT, per quanto tutti gli operatori economici in qualunque settore siano esposti a queste fattispecie (si veda il tema del '*sanctioned by extension*' discusso sopra). Interessante invece notare il peso degli incidenti legati a **intermediazione illecita e sfruttamento del lavoro**, segnalati dal 39% dei rispondenti nel settore non finanziario (e da nessuno in quello finanziario), percentuale che sale però al **54% considerando solo il mondo del lusso**. Importante il peso anche dei rischi legati a violazioni dei diritti umani, segnalati dal 22% dei rispondenti nel settore non finanziario. Sebbene in termini assoluti i numeri siano relativamente bassi, è interessante notare come le questioni legate alla **criminalità organizzata** (10% in media) siano più frequenti nei settori che hanno stretti legami con la pubblica amministrazione, come quello delle costruzioni e dell'energia (66%).

Alla varietà degli incidenti a cui sono state esposte le imprese del campione, sopra illustrata, non corrisponde una varietà di controlli e presidi: solo il 31% dei rispondenti adotta controlli TPRM diversificati a seconda dei rischi/reati presupposto, **mentre il 69% adotta i medesimi controlli indipendentemente dai rischi valutati**[13]. Per tutti coloro che declinano i controlli in base al tipo di rischio, a fare la differenza è il livello di profondità dell'analisi (intervento dell'analista vs. controllo automatizzato) e per un numero minore le modalità di controllo (audit in situ vs. controllo da remoto).

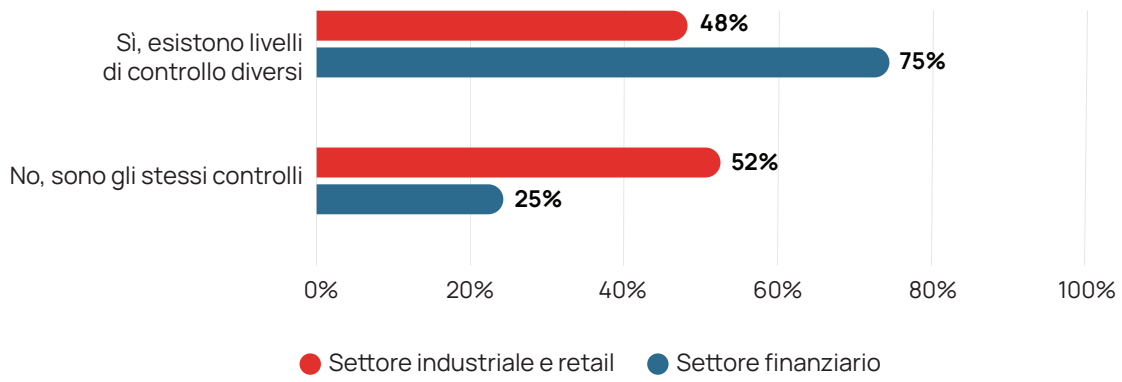
Per quanto riguarda invece la diversificazione dei controlli in base alla tipologia di terze parti, la panoramica appare leggermente migliore. Dai risultati della survey emerge chiaramente che una quota considerevole di aziende – 48% settore industriale e retail e 75% settore finanziario - adotta una differenziazione nei controlli (Figura 5). Nonostante questo, è importante sottolineare che una quota altrettanto elevata – **rispettivamente 52% e 25%** - non adotta questa politica.

12. Sono da intendersi 'problematiche' non solo gli incidenti verificati con terze parti aventi relazioni contrattuali già in essere (es. clienti o fornitori già acquisiti) ma anche quelli riscontrati su terze parti in fase di on-boarding pertanto prima dell'eventuale instaurazione di relazioni contrattuali.
13. Questa domanda si riferisce esclusivamente a controlli sul 'ciclo passivo'.

Tabella 2: Percentuale di rispondenti che hanno subito incidenti significativi legati alle controparti
Fonte: elaborazione Crime&tech

Incidenti legati alle controparti	Settore finanziario	Settore industriale e retail
Riciclaggio di denaro e finanziamento del terrorismo	22%	4%
Corruzione e reati contro la PA	33%	48%
Infiltrazione della criminalità organizzata	11%	9%
Reati tributari (ex art 25-quinquesdecies, D.Lgs. 231/01)	11%	30%
Sicurezza IT e delle informazioni (e.g. data breach e attacchi cyber)	56%	57%
Reati societari (ex art 25-ter, D.Lgs. 231/01)	33%	26%
Reati ambientali (ex art 25-undecies, D.Lgs. 231/01)	22%	26%
Sanzioni internazionali	33%	9%
Intermediazione illecita e sfruttamento del lavoro	0%	39%
Violazione dei diritti umani	0%	22%

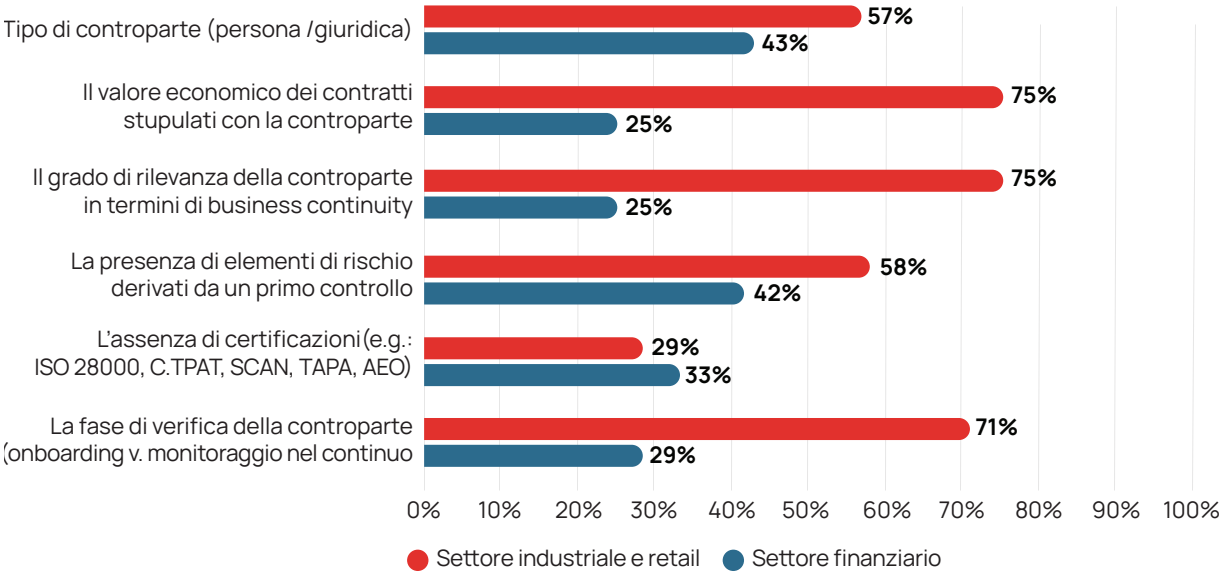
Figura 5: Variazioni dei controlli in base alle controparti
Fonte: elaborazione Crime&tech



Questi risultati sollevano importanti interrogativi sulla gestione dei rischi e sulla sicurezza delle transazioni aziendali. Le diverse controparti, infatti, possono presentare rischi specifici e unici, e la mancanza di una differenziazione può esporre l'organizzazione a diverse vulnerabilità.

Inoltre, andando più nello specifico emerge che ci sono delle variabili che fanno scattare dei controlli diversificati (Figura 6), e che queste risultano molto diverse in base al macrosettore che si analizza. Nel settore industriale e del retail l'attenzione è posta in particolare alla tipologia di controparte (se fisica o giuridica) e alla presenza di fattori di rischio dopo un primo controllo (paese o forma legale); nel settore finanziario invece i rispondenti indicano come variabili incisive il valore del contratto da stipulare con la terza parte, e il grado di rilevanza in termini di *business continuity*.

Figura 6: Variabili incisive nella decisione di intraprendere controlli più rigorosi
Fonte: elaborazione Crime&tech



Ma quali sono i metodi di *screening* di TPRM più frequenti tra le imprese italiane? Sia nel settore finanziario che in quello non finanziario si riscontra una **prevalenza nell'utilizzo delle cosiddette 'liste'**, ovvero di database, spesso forniti da *provider* terzi, quasi sempre ricavati da fonti aperte, che riguardano il coinvolgimento di individui o società in casi precedenti di provvedimenti amministrativi o giudiziari (spesso riferiti come casi di '*enforcement*'), o menzionati in notizie di tenore negativo - i cosiddetti '*adverse media*' (Figura 4). Il ricorso agli ***'adverse media'*** si osserva per l'88% dei rispondenti nel settore finanziario, e per il 71% degli altri rispondenti. La totalità degli intermediari finanziari interpellati si affida poi agli elenchi di **persone politicamente esposte (PEP)** e alle **liste di soggetti sanzionati** (ad esempio da Nazioni Unite, Unione Europea, e US OFAC); molto utilizzate in questo settore anche le cosiddette liste di ***'enforcement'*** (88%). Questi ultimi due controlli – sanzioni ed *enforcement* – appaiono invece molto meno utilizzati dai rispondenti del settore non finanziario – rispettivamente 48% e 52%.

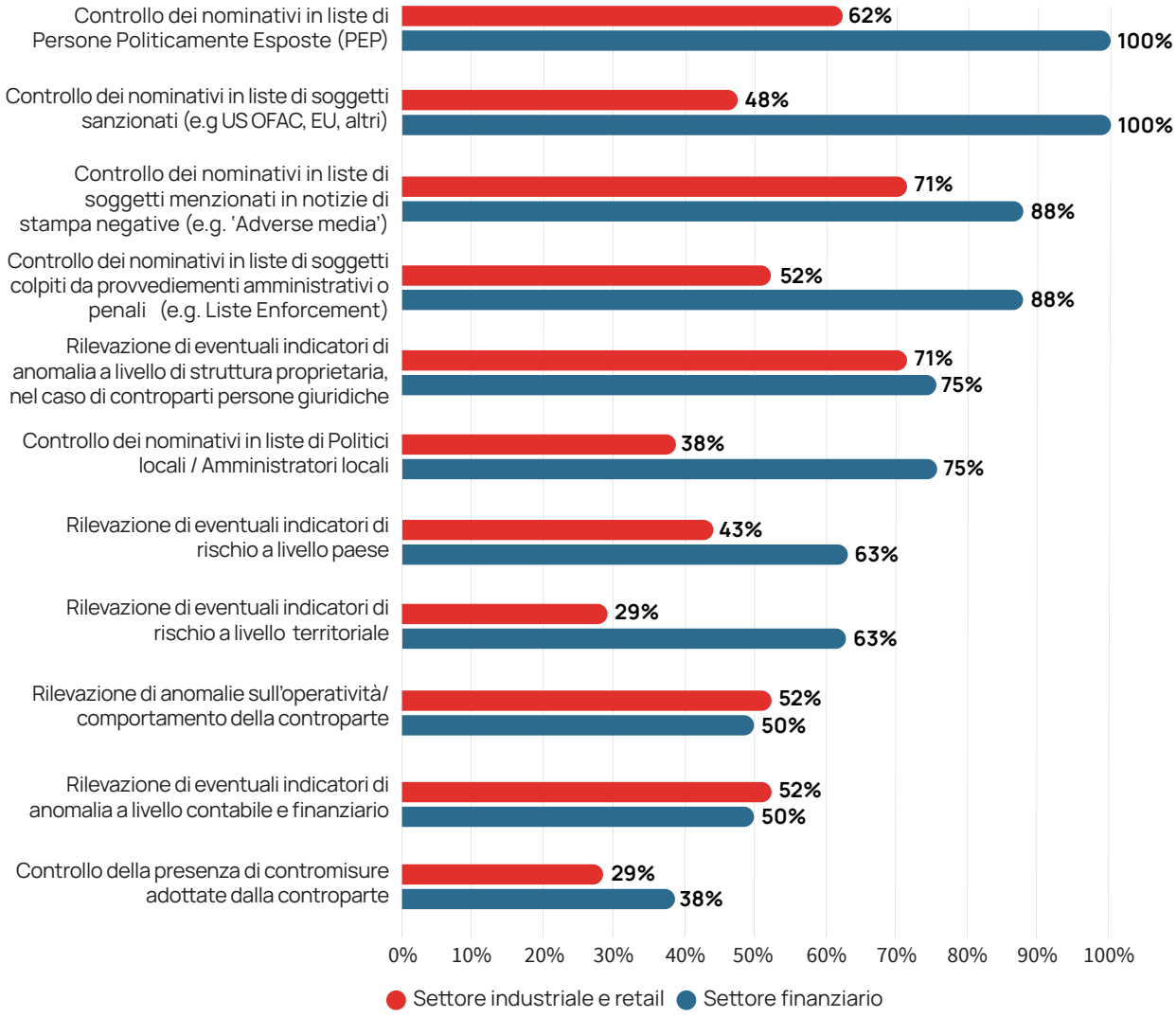
In generale, il settore industriale mostra una maggiore variabilità nei controlli, dovuta anche all'eterogeneità delle attività svolte dalle imprese ricomprese in questa categoria. E, in sintesi, il campione appare molto più sbilanciato sulle 'liste' che sul ricorso ai cosiddetti **indicatori di anomalia**, o di rischio. Negli ultimi anni la necessità di utilizzare un approccio più evoluto, basato su **indicatori di rischio**, nei processi di valutazione delle controparti, è stata più volte sottolineata da istituzioni nazionali ed internazionali, sia in ambito industriale (OECD, 2018) che ancora di più in ambito finanziario, con particolare riguardo alle attività di *due diligence e risk assessment* AML/CFT (EBA, 2022; FATF, 2014, 2023).

La spinta del regolatore AML/CFT o delle autorità competenti in questo ambito (si pensi, in Italia, ai '*Modelli e schemi di comportamenti anomali*' pubblicati periodicamente dall'Unità di Informazione Finanziaria) e il miglioramento significativo in termini di **disponibilità di dati e di strumenti tecnologici avanzati**, anche basati sull'**intelligenza artificiale**, ha aumentato a dismisura le possibilità per banche ed imprese di mappare in maniera sistematica i fattori di rischio legati alle terze parti, sia di natura soggettiva che oggettiva – ovvero relativi alle transazioni ad esse collegati (Crime&tech e SAS, 2021). Anche il mondo della ricerca accademica si è recentemente dedicato allo sviluppo di **modelli predittivi**, anche validati empiricamente, utilizzabili per l'*early detection* di imprese – comprese potenzialmente le terze parti – ad alto rischio (si veda Box 4).

Tuttavia, nonostante questi sviluppi, l'utilizzo di indicatori di rischio e approcci 'evoluti' **non sembra particolarmente diffuso** nei processi di TPRM delle imprese italiane. In media, le aziende che utilizzano indicatori di anomalia per la valutazione delle controparti sono solo il 60% dei rispondenti per il settore finanziario ed il 50% per il settore industriale. Fatta eccezione per le *red-flags* legate alla **struttura proprietaria** delle imprese, utilizzate da circa il 70% dei rispondenti (ma che tuttavia nella pratica si riferiscono essenzialmente alla individuazione di collegamenti con *trust*, fiduciarie e altri veicoli societari più critici), l'utilizzo di indicatori di rischio a livello **contabile e finanziario**

(es. rilevazione di 'società cartiere') e a livello **territoriale**, sia locale che internazionale (es. collegamenti con comuni o con giurisdizioni ad alto rischio), appare minoritario, soprattutto tra i rispondenti del settore non finanziario. Allo stesso modo, la sussistenza di contromisure e presidi presso la terza parte – ad esempio **certificazioni**, iscrizione in ***white list* antimafia, rating di legalità** – è verificata solo da circa il 30% dei rispondenti.

Figura 7: I metodi di controllo TPRM adottati dalle imprese italiane
Fonte: elaborazione Crime&tech



Box 4 – Ricerca accademica e modelli per l'identificazione di terze parti ad alto rischio

Crime&tech, spin-off company del centro Transcrime di Università Cattolica del Sacro Cuore, ha sviluppato dei **modelli e indicatori di anomalia** utilizzabili per la profilazione del rischio delle terze parti, ad esempio da parte di banche e altri soggetti obbligati per finalità di **anti-riciclaggio**, o da imprese nel settore industriale, retail o dalle pubbliche amministrazioni per la valutazione dei rischi della ***supply-chain*** e la ***procurement integrity***.

Gli indicatori si fondano sugli approcci analitici evoluti di Transcrime, che impiegano diversi metodi di ***machine learning*** (es. naïve Bayes e algoritmi *tree-based*) e **intelligenza artificiale**, anche applicata all'**analisi testuale** (es. *Large language models, Named entity recognition*) e di **rete** (e.g. *transductive* e *inductive link prediction*), per la raccolta e l'elaborazione dei dati sulle controparti.

Gli indicatori coprono diverse dimensioni di rischio, tra le quali: (i) anomalie nella **struttura proprietaria** e nella **governance delle imprese** (es. complessità anomala, collegamenti con veicoli opachi); (ii) **esposizione territoriale e settoriale** verso aree ad alto rischio (a livello internazionale e locale, es. soggetti apicali provenienti da comuni ad alto rischio; (iii) anomalie nella **struttura contabile e finanziaria**; (iv) anomalie nel **ciclo di vita** dell'impresa (es. rotazioni e concentrazioni anomale); (v) assenza di **contromisure** (es. mancata iscrizione in whitelist, assenza di attestazioni SOA, etc).

Gli indicatori sono validati empiricamente (per testare la capacità predittiva di rilevare imprese e controparti ad alto rischio) e istituzionalmente, essendo utilizzati anche da **autorità, in Italia e in Europa**, in indagini e attività di intelligence su criminalità organizzata, finanziaria e anti-corruzione.

In conclusione, lo sviluppo di questi modelli rappresenta una soluzione innovativa per l'identificazione precoce delle terze parti ad alto rischio, consentendo di rilevare situazioni di anomalia anche **quando non sono presenti segnali provenienti dalle 'liste'**, ovvero da media avversi e precedenti giudiziari.

Per maggiori informazioni: Crime&tech e Tom-The Ownership Monitor

3.3. Strumenti e banche dati

I tipi di controllo effettuati sulle terze parti trovano chiaro riflesso negli **strumenti** e nelle **banche dati** utilizzati per il TPRM[14]. Dall'analisi della letteratura esistente e dagli input ricevuti durante i *focus group* emerge chiaramente una domanda per strumenti tecnologici in grado di facilitare il lavoro di TPRM, con particolare riferimento alla fase di *due diligence* e a quella di monitoraggio nel continuo (Deloitte 2022; 2021; McKinsey & Company and ORIC International 2017). Non stupisce che la quasi **totalità delle imprese interpellate si avvalga di banche dati o di strumenti tecnologici** e che la maggior parte dei rispondenti veda l'adozione di questi ultimi come una priorità strategica e miri ad aumentarne l'uso nei prossimi anni.

Per quanto riguarda le banche dati, l'83% dei rispondenti dichiara di utilizzare *repository* con **copertura globale**. In linea con i controlli effettuati (vedi precedente paragrafo), le banche dati più comunemente utilizzate sono quelle riguardanti '*Enforcement*' e '*Adverse Media*', così come quelle contenenti informazioni societarie e camerali (Tabella 3).

Tabella 3: Banche dati utilizzate nei controlli di TPRM
Fonte: elaborazione Crime&tech

Banche dati utilizzate per i controlli TPRM	% dei rispondenti
Banche dati di "Enforcement" e "Adverse Media"	78%
Banche dati contenenti informazioni societarie e camerali	78%
Banche dati contenenti liste di soggetti sanzionati	65%
Banche dati di persone politicamente esposte (PEP)	65%
Banche dati relative a certificazioni societarie	48%
Banche dati di informazioni legate a protesti/pregiudizievoli	48%

14. Si intendono qui come 'banche dati' i sistemi informatici di raccolta, archivio e gestione delle informazioni relative a terze parti, e come 'strumenti' le tecnologie, anche dotate di interfacce utente, appositamente sviluppate per aggregare dati provenienti da fonti diverse al fine di valutare il rischio associato alle terze parti. Non sempre è possibile elaborare una chiara distinzione tra i due servizi, e pertanto la differenza qui riportata è da ritenersi indicativa.

Considerato il maggiore interesse per le controparti del ciclo attivo, i rispondenti del settore finanziario utilizzano in maniera più sistematica di quelli del settore industriale i *repository* **con prevalente copertura su persone fisiche**, ovvero quelli sui PEP e sui soggetti sanzionati – rispettivamente 100% contro 47%. Viceversa, è interessante notare che la percentuale di utilizzatori di banche dati contenenti informazioni camerali o certificazioni societarie sia più elevata per il settore industriale che quello finanziario (rispettivamente 80% vs. 75%, e 53% vs. 38%).

Passando alle tecnologie, la maggioranza delle imprese (78%) si appoggia a **strumenti sviluppati da *provider* esterni** e forniti alle imprese in modalità ***software-as-a-service* (SaaS)**. Come visibile in Tabella 4, la funzione più diffusa messa a disposizione da questi strumenti è quella dell'individuazione dei soggetti apicali (es. soci, amministratori) di una società. Il 74% dei rispondenti dichiara di essere in grado, grazie a questi strumenti, di **individuare i titolari effettivi** delle proprie controparti anche quando queste sono registrate all'estero o sono controllate tramite società intermediarie registrate all'estero. Tuttavia questa funzione è molto meno utilizzata dalle imprese in ambito non finanziario (53%). Altre funzioni particolarmente diffuse sono quelle della combinazione di informazioni provenienti da fonti diverse, come il *matching* dei nominativi tramite l'integrazione delle banche dati di cui sopra (es. match tra liste PEP o liste sanzioni e i nomi di soci o amministratori).

In generale, la *survey* mostra un **più limitato ricorso a strumenti tecnologici per le imprese del settore industriale** che per quelle in ambito finanziario – ad esempio, come anticipato, in termini di servizi per la ricostruzione delle catene di controllo, di *matching* di nominativi e fonti diverse, di monitoraggio nel continuo. Gli unici due servizi che appaiono più diffusi in ambito non finanziario sono da un lato l'automatizzazione dei processi/questionari di *on-boarding*; e dall'altro, l'utilizzo di strumenti in grado di generare in maniera automatica ***rating* di rischio reputazionale** delle controparti (40%).

Tabella 4: Funzioni e servizi degli strumenti tecnologici utilizzati per il TPRM
Fonte: elaborazione Crime&tech

Funzioni degli strumenti di TPRM	Settore finanziario	Settore industriale e retail
Individuazione dei titolari effettivi (soci, amministratori e altre persone fisiche) collegati alla controparte	100%	53%
Raccolta, combinazione e armonizzazione di informazioni da fonti diverse	75%	67%
Individuazione e mappatura dei collegamenti tra le controparti presenti nel suo portafoglio	50%	47%
Matching dei nominativi delle controparti e dei soggetti ad esse collegati con le banche dati	63%	53%
Produzione di un rating di rischio reputazionale delle controparti	25%	40%
Automatizzazione di compilazione di questionari di on-boarding	0%	7%
Servizi di monitoraggio del rischio nel continuo	50%	27%

Tuttavia, nonostante l'ampio utilizzo di tecnologie nel TPRM, la maggioranza delle imprese intervistate **non è ancora soddisfatta dei risultati** in termini di valutazione del rischio offerti da questi strumenti, come peraltro già evidenziato da studi precedenti a livello internazionale (KPMG 2022). Tra le esigenze più avvertite troviamo la necessità di migliorare l'ampiezza della **copertura del dato** (segnalata dal 48% dei rispondenti) e l'efficacia dei **sistemi di disambiguazione** dei *match* dei nominativi proposti dalle piattaforme TPRM in uso (39% dei rispondenti). Non sembra invece particolarmente pressante la necessità di contenere i costi di licenza di questi strumenti. Tuttavia, questo risultato è probabilmente influenzato dalla natura del campione analizzato, composto principalmente da grandi imprese con maggiori risorse a disposizione.

Box 5 – TPRM e 'rischio reputazionale'

Come anticipato nell'introduzione, la valutazione del rischio legato alle terze parti è talvolta denominata, in alternativa, valutazione del 'rischio reputazionale'. Tuttavia, **non esiste un consenso** su cosa significhi esattamente questo concetto, e tantomeno sui fattori che concorrono a determinarlo. La maggior parte degli studi disponibili si limita a parlare di 'rischio reputazionale' in maniera generica, o a considerarlo come una categoria molto ampia che può essere alimentata da diversi tipi di rischio (si veda, a titolo di esempio, Moody's Analytics 2023).

Anche nel campione intervistato il 'rischio reputazionale' è prevalentemente interpretato come una **fattispecie già ricompresa all'interno delle categorie di rischio** afferenti, in linea di massima, al catalogo dei reati presupposto ex 231/2001 elencati in Tabella 2. Nonostante il 93% dei rispondenti dichiari di coprire il rischio reputazionale nel proprio processo di TPRM, solamente il **22% lo considera una fattispecie di rischio a sé stante** ed ha sviluppato delle **metriche o modelli di *scoring* specifici** per valutarlo. Nella maggior parte dei casi, invece, il rischio reputazionale è valutato affidandosi a controlli di '*adverse media*' tramite lo screening di fonti aperte.

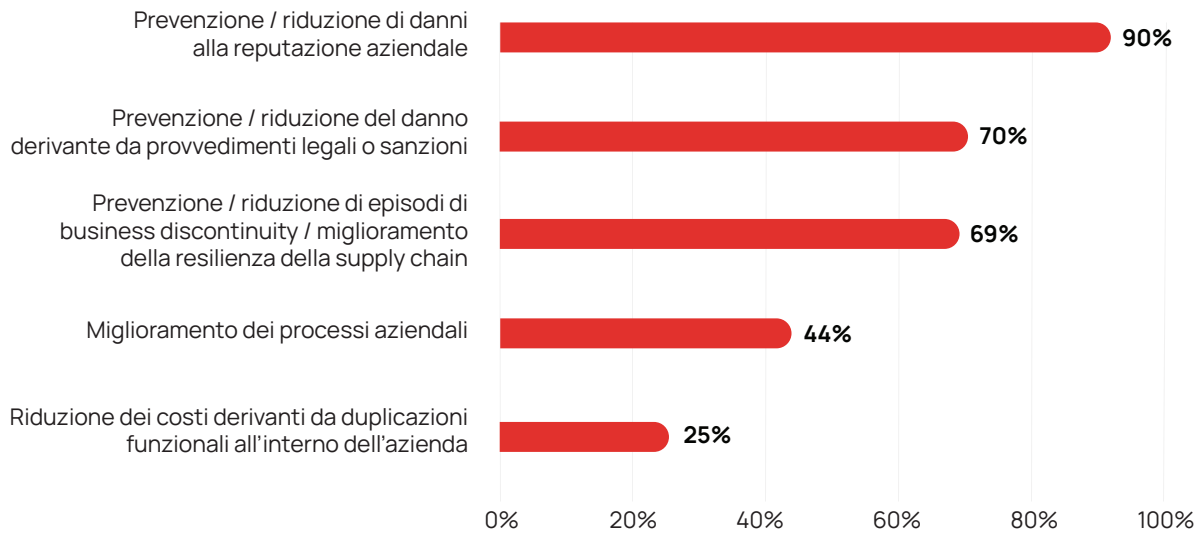
I rispondenti che concepiscono il 'rischio reputazionale' come una fattispecie distinta dagli altri rischi tendono a legarlo, più che ad una dimensione di non conformità normativa, a delle **valutazioni etiche** su un comportamento tenuto o caratteristiche di una controparte non conformi alla **cultura o identità aziendale e ai suoi valori**. In particolare, questa visione si applica soprattutto, più che al ciclo passivo, all'*assessment* di determinati clienti o di altro genere di terze parti come *testimonial, partner, sponsor,* soprattutto nei casi di marchi con maggiore visibilità. Non è un caso che, tra le poche aziende che considerano il rischio reputazionale come una fattispecie a sé stante, la maggior parte sia attiva nel settore del **lusso**.

3.4. Benefici e criticità nei processi di TPRM

In sintesi, nonostante le sfide e le complessità sopra illustrate, c'è un **consenso ampio circa i benefici** apportati ad imprese, banche ed enti pubblici dall'introduzione di processi strutturati di TPRM (Figura 7). In particolare, nel campione interpellato, prevale la convinzione che il TPRM possa soprattutto difendere l'azienda da **danni alla reputazione aziendale**, prima ancora di quelli derivanti da eventuali **provvedimenti legali o sanzioni amministrative o pecuniarie**.

La prevenzione di questi ultimi è considerata alla stregua dei benefici operativi in termini di ***business continuity*** e di miglioramento della **resilienza della *supply-chain***, come ricordato nell'introduzione. Il miglioramento dei processi aziendali, così come emerso nei *focus group*, non è da intendersi esclusivamente come riduzione/razionalizzazione dei costi (all'ultimo posto tra i benefici percepiti), ma anche come miglioramento della *performance* aziendale, ad esempio in termini di efficientamento della catena di approvvigionamento e di maggiore responsività alle esigenze del mercato.

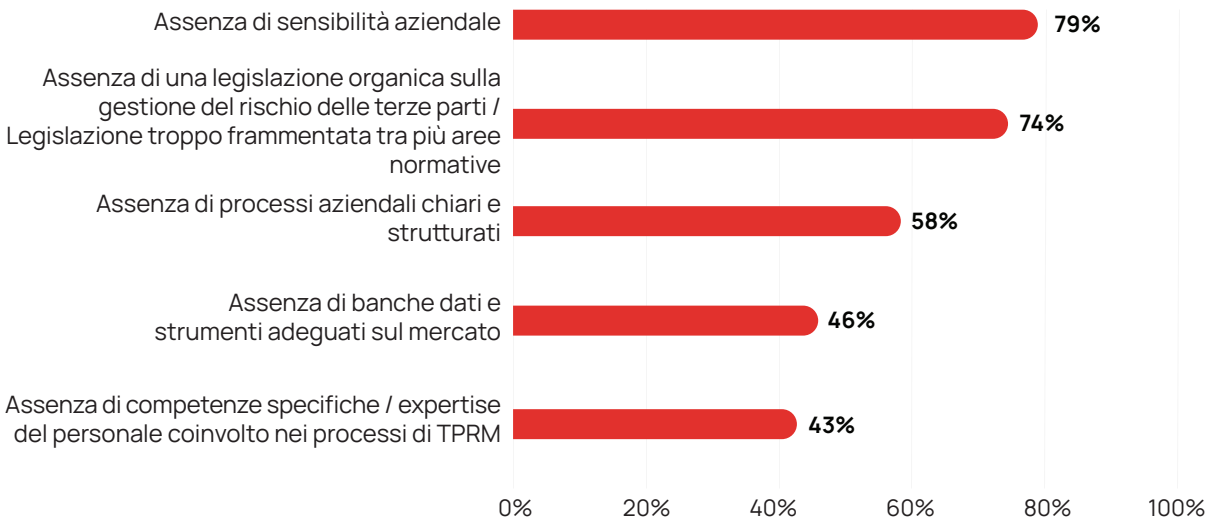
Figura 8: Benefici percepiti dai rispondenti in relazione ai processi di TPRM
Fonte: elaborazione Crime&tech



D'altra parte, le imprese intervistate sottolineano alcune **criticità chiave** che inficiano un'efficace implementazione dei processi di TPRM. Prima ancora che le carenze in termini di **strumenti/banche dati** o di **competenze specifiche** delle risorse umane (agli ultimi due posti secondo le risposte alla *survey*), le principali criticità riguardano la cultura interna dell'organizzazione. In particolare si rileva la percezione diffusa di una **scarsa sensibilità aziendale** sull'esigenza e sui benefici derivanti dal TPRM, essendo le scelte sulle terze parti orientate prevalentemente in una logica di profitto. La scarsa sensibilità si manifesta poi anche in termini di **assenza di processi aziendali chiari e strutturati**. Come ricordato sopra, il TPRM è spesso a cavallo di diverse aree aziendali (*compliance, procurement, security, internal audit*) e richiede un'integrazione – spesso complessa - di diverse funzioni, team, sistemi operativi e tecnologici.

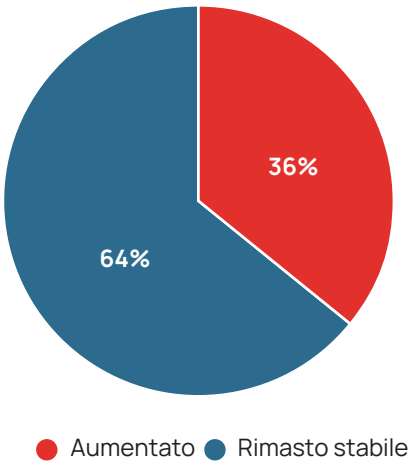
Allo stesso tempo, come già discusso, **l'assenza di riferimenti legislativi univoci, e la frammentarietà regolamentare**, con obblighi di valutazione distribuiti su più ambiti normativi, costituiscono un ostacolo importante alla definizione di un processo di TPRM organico e lineare. Questa è proprio una delle ragioni che hanno portato alla redazione di questo studio e ad aprire la riflessione sulle pratiche di valutazione del rischio terze parti delle imprese italiane.

Figura 9: Criticità percepite in relazione ai processi di TPRM
Fonte: elaborazione Crime&tech



Nonostante le criticità evidenziate dagli intervistati, l'aumento della complessità e delle minacce globali hanno reso il TPRM una **priorità strategica** per le imprese desiderose di proteggere i propri interessi. Questa consapevolezza ha spinto molte organizzazioni a riconoscere l'importanza di dedicare risorse significative a questo processo. Di conseguenza, dalla *survey* emerge che il **budget dedicato a questo processo nel 36% dei casi è aumentato**, mentre nel restante 64% è rimasto stabile, e in nessun caso è diminuito.

Figura 10: Budget stanziato per il TPRM nel 2023
Fonte: elaborazione Crime&tech



4. Conclusioni e raccomandazioni

Dall'analisi svolta risulta evidente che, per le imprese italiane ma non solo, la **valutazione e la gestione del rischio** delle terze parti sia una attività centrale nel panorama della ***compliance*** e ***security*** aziendale. Tuttavia, si tratta di un ambito complesso, variegato, eterogeneo e sotto studiato. L'esigenza di avere un processo efficace di TPRM è chiara, ma i benefici apportati alle organizzazioni non sono sempre parimenti compresi da tutte le funzioni aziendali.

Riteniamo sia possibile stilare un **decalogo di 10 temi chiave** che possono fungere da spunti utili ad orientare una riflessione futura su **come migliorare i processi di TPRM** e come implementarli efficacemente in un'organizzazione. Sono brevemente discussi di seguito.

1. TPRM come elemento chiave della valutazione dei rischi di un'organizzazione

- Sebbene solo alcuni degli ambiti normativi sopra ricordati prevedano in maniera esplicita degli obblighi di TPRM, da tutti discende la necessità di avere dei controlli strutturati delle terze parti.
- Imprese, intermediari finanziari, enti pubblici non vivono in ambienti asettici, bensì **permeati di relazioni con soggetti esterni**: clienti, fornitori, partner, 'quarte parti'.
- Ne consegue che una valutazione comprensiva dei rischi di un'organizzazione non può limitarsi alla mappatura dei processi interni e delle aree funzionali, ma debba **estendersi anche alle terze parti**.
- In questo senso, un presupposto essenziale al TPRM è una conoscenza sistematica delle controparti, che **devono essere censite** tramite una mappatura sistematica, completa, formalizzata ed aggiornata.

2. TPRM come programma autonomo e trasversale su più ambiti normativi

- Come ampiamente ricordato, **non esiste un unico riferimento normativo** per i processi di TPRM: esistono obblighi diversi afferenti a più ambiti regolamentari, che spesso si sovrappongono ed incrociano - anche in assenza di raccordi formali.
- Da qui l'esigenza che il TPRM sia disegnato all'interno di un'organizzazione come un **programma autonomo** capace di rispondere, in maniera trasversale, agli obblighi che emergono dai diversi ambiti normativi.
- È necessario abbandonare l'idea che il TPRM sia semplicemente **parte di una *policy*** di gestione del rischio sanzioni, anticorruzione o antiriciclaggio: deve essere trattato come un'entità distinta, ma capace di dialogare con tutti questi ambiti.
- In questo modo si possono minimizzare le duplicazioni e i costi ridondanti e massimizzare le economie di scala tra le diverse aree normative sotto l'ombrello della compliance aziendale.

3.TPRM come programma integrato tra diverse funzioni aziendali

- Da questa convinzione conseguono due implicazioni. La prima è che il TPRM debba essere disegnato in **maniera integrata** tra le diverse funzioni aziendali.
- Dall'analisi svolta emerge che il TPRM non è quasi mai appannaggio di un'unica area: nel 38% dei casi è gestito tra ***compliance***, ***procurement***, ***security*** ed ***internal audit***.
- I compiti di ciascuna funzione devono essere chiari – così come devono essere disciplinati i flussi informativi sulle terze parti, standardizzati e disegnati in maniera tale da consentire una **piena integrazione funzionale e tecnologica** (ad esempio dei sistemi utilizzati da ciascuna area per gestire i rapporti con le terze parti).

4. TPRM come programma integrato e declinato nelle diverse aree di rischio

- La seconda implicazione è che il TPRM deve essere disegnato così da rispondere, in maniera integrata, a **tutte le aree di rischio** a cui è esposta un'organizzazione – così come identificate secondo il *risk appetite* aziendale.
- Come riferimento, un'organizzazione può prendere in maniera indicativa il catalogo dei **reati presupposto ex 231/2001** – eventualmente raggruppati così da essere più funzionali rispetto ai processi aziendali.
- È utile che **ogni terza parte sia valutata rispetto a ciascuna delle aree di rischio** rilevanti così identificate.
- Ciò non significa che i controlli delle terze parti debbano essere gli stessi indipendentemente dall'area di rischio; anzi, è auspicabile che siano **declinati e articolati rispetto ad esse** – ad esempio in termini di diversi tipi di verifiche, profondità dell'analisi, fonti informative, indicatori di anomalia e di strumenti o banche dati.
- In questo senso, è auspicabile un'**estensione del concetto di *risk based approach*** – perno nell'adeguata verifica della clientela a fini AML/CFT – anche alla valutazione del rischio delle **terze parti del ciclo passivo**, e oltre l'ambito antiriciclaggio.

5. TPRM esteso al ciclo attivo anche nel mondo industriale? Dipende

- In questo senso, seguendo proprio una logica di *risk based approach*, non è opportuno né includere **né escludere a priori** la valutazione delle terze parti afferenti al ciclo attivo (es. clienti).
- Prima di tutto, è necessario **mappare i processi interni** e, sulla base sia del modello di business in questione che del *risk appetite* aziendale, valutare se esistano dei rischi rilevanti anche per le terze parti del ciclo attivo.
- In questo senso, aldilà degli obblighi normativi già presenti (es. antiriciclaggio, o programmi sanzioni), i **controlli sulla clientela** devono essere effettuati in base ai rischi effettivamente individuati per il business.

6. TPRM oltre l'approccio basato sulle verifiche delle 'liste'

- Secondo quanto emerge dall'analisi svolta, la maggior parte delle imprese e banche italiane si limita, per finalità TPRM, ai **controlli sulle 'liste'** – elenchi di soggetti sanzionati, PEP, adverse media, enforcement.
- Riteniamo che questo approccio non sia efficace – e lo sarà sempre meno – per diverse ragioni. In primo luogo perché, per definizione, i controlli delle liste sono in grado di verificare solo **istanze di pericolo passate e già accertate**, ma non future.
- In secondo luogo, anche alla luce delle recenti evoluzioni normative (es. GDPR e 'Riforma Cartabia'), l'accesso dei media ai documenti giudiziari sarà sempre più ristretto, e pertanto la disponibilità di 'nomi' sulle fonti aperte sarà sempre inferiore.
- Infine, l'evoluzione dei fenomeni criminali – in primo luogo quelli di criminalità organizzata ed economica – porta a forme di **infiltrazione nella *supply-chain*** sempre meno visibili (ad esempio nelle forme di reati fallimentari, fiscali, finanziari) che risultano anche meno attrattivi – e quindi visibili – sulla stampa locale e tantomeno internazionale.

7. TPRM fondato su un approccio evoluto di indicatori di rischio e di anomalia

- In questo senso, è auspicabile un TPRM 'evoluto' che si possa fondare – ispirato anche dalle evoluzioni osservate negli ultimi anni a livello AML/CFT – su un'analisi avanzata di **indicatori di anomalia e rischio** associabili alle terze parti.
- Questo avrebbe diversi vantaggi. In primo luogo consentirebbe di rilevare situazioni di rischio **non già accertate o mappate** dalle autorità competenti (e quindi riprese dalle fonti aperte).
- In secondo luogo consentirebbe anche di superare, o perlomeno mitigare, i rischi in termini di uso improprio di dati personali (e categorie speciali degli stessi), anche in un'ottica di ***data minimization***.
- Anche seguendo gli esiti delle ultime ricerche scientifiche in questo ambito, gli indicatori di rischio dovrebbero guardare a diverse dimensioni dell'operatività aziendale – dalla **struttura proprietaria, a quella contabile-finanziaria, all'esposizione territoriale** (a livello locale ed internazionale) o al ciclo di vita di un'impresa.

8. TPRM fondato sull'utilizzo di strumenti analitici avanzati

- Per fare ciò, è auspicabile che i processi di TPRM facciano pieno uso degli **strumenti analitici avanzati** ora disponibili (anche a basso costo) sul mercato, a cominciare da quelli basati sull'**intelligenza artificiale**.
- Questo consentirebbe di utilizzare al meglio l'ampio patrimonio informativo a disposizione delle aziende (sia nel contesto interno che in quello esterno) e di affrontare alcuni problemi rilevanti segnalati dalle imprese interpellate – a cominciare da quelli di **disambiguazione e *matching*** dei nominativi 'a rischio'.

9. TPRM in una prospettiva 'glocal'

- Nella valutazione dei rischi delle terze parti è sempre più evidente la necessità di coniugare una **dimensione globale** con una **dimensione locale**.
- *Globale* perché da un lato le catene di approvvigionamento – soprattutto in alcuni settori e per alcune imprese italiane – sono **significativamente esposte all'estero**, e dall'altro perché la proprietà di molte terze parti è ora in mano a soggetti stranieri (anche attraverso complesse catene societarie di controllo transnazionali).
- *Locale* perché molti dei rischi e fenomeni criminali da cui le imprese italiane si vogliono difendere hanno una **dimensione molto locale** – ad esempio legata alla presenza di attori criminali sui singoli comuni, o quartieri, o di vulnerabilità territoriali specifiche.
- È auspicabile pertanto, in ottica TPRM, il ricorso a banche dati con copertura globale (ad esempio in termini di informazioni sulla struttura societaria), e l'utilizzo di **indicatori di rischio a livello territoriale** capaci sia di coprire la dimensione paese, che quella locale dei singoli comuni italiani – se non dei singoli quartieri.

10. TPRM che guardi ai 'nuovi mondi': ESG e anti-riciclaggio allargato

- Le recenti evoluzioni normative, prime tra tutte la **CSDDD** e l'estensione del **perimetro dei soggetti obbligati AML/CFT** previsto dal nuovo pacchetto UE, obbligano ad includere nei processi TPRM delle nuove riflessioni in ambito ESG e anti-riciclaggio.
- Per quanto riguarda l'ESG, è opportuna una riflessione operativa che consenta di operativizzare e misurare in maniera concreta, ma allo stesso tempo scientificamente solida, le **dimensioni ambientale, sociale e di *governance***, ed i relativi rischi ed impatti.
- Per quanto riguarda l'anti-riciclaggio, considerato il prossimo allargamento degli obblighi anche a diversi soggetti nel settore del **manifatturiero, del lusso e dell'*entertainment***, è auspicabile un dialogo ancora più stretto tra i controlli AML/CFT e quello delle altre aree di rischio sopra ricordate.

Come 'collante' di tutti questi suggerimenti rimane la raccomandazione su un continuo lavoro per **rafforzare la sensibilità e la cultura aziendale** sui temi di valutazione del rischio delle terze parti, che comprenda tutti i livelli, dai vertici aziendali, alle funzione di business, alle seconde linee.

Bibliografia

ANAC. (2017). Nuove linee guida per l'attuazione della normativa in materia di prevenzione della corruzione e trasparenza da parte delle società e degli enti di diritto privato controllati e partecipati dalle pubbliche amministrazioni e degli enti pubblici economici. https://www.anticorruzione.it/-/determinazione-n.-1134-del-08/11/2017

ANAC. (2023). Piano Nazionale Anticorruzione. https://www.anticorruzione.it/-/ecco-il-piano-nazionale-anticorruzione-approvato-da-anac

Associazione Italiana Internal Auditors. (2019). Top Risk 2020 secondo i CAE Europei. https://www.aiiaweb.it/sondaggio-i-top-risk-del-2020-secondo-i-cae-europei

Borsa Italiana. (2024). Regolamento dei mercati organizzati e gestiti da Borsa Italiana S.p.a. https://www.borsaitaliana.it/borsaitaliana/regolamenti/regolamenti/regolamento-25032024-conevidenza.pdf

Comitato di Sicurezza Finanziaria. (2019). Relazione al Parlamento sullo stato dell'azione di prevenzione del riciclaggio e del finanziamento del terrorismo, elaborata dal comitato di Sicurezza finanziaria. https://www.dt.mef.gov.it/export/sites/sitodt/modules/documenti_it/prevenzione_reati_finanziari/prevenzione_reati_finanziari/relazione_parlamento/Relazione_Al_Parlamento_Anno_2019.pdf

Confindustria. (2021). Linee guida per la costruzione dei modelli di organizzazione, gestione e controllo ai sensi del decreto legislativo 8 giugno 2001, n. 231. https://www.confindustria.it/wcm/connect/68e8ada9-cbfa-4cad-97db-82ba3cc3e963/Position+Paper_linee+guida+modelli+organizzazione_giugno2021_Confindustria.pdf?MOD=AJPERES&CACHEID=ROOTWORKSPACE-68e8ada9-cbfa-4cad-97db-82ba3cc3e963-nFyjPuZ

Consiglio dell'UE. (2024). Antiriciclaggio: Accordo tra Consiglio e Parlamento su norme più rigorose. https://www.consilium.europa.eu/it/press/press-releases/2024/01/18/anti-money-laundering-council-and-parliament-strike-deal-on-stricter-rules/

Council of the European Union. (2024). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937.

Crime&tech e SAS. (2021). Next Generation AML. https://www.transcrime.it/wp-content/uploads/2023/01/Next_Generation_AML.pdf

Deloitte. (2021). Third-Party Risk Management Outlook 2021. https://www2.deloitte.com/it/it/pages/risk/articles/third-party-risk-management-global-survey-2021--deloitte-italy-.html

Deloitte. (2022). Global third-party risk management survey 2022. https://www2.deloitte.com/it/it/pages/risk/articles/global-third-party-risk-management-survey-2022--deloitte-italy--risk-advisory.html

DIA. (2023). Direzione Investigativa Antimafia. https://direzioneinvestigativaantimafia.interno.gov.it/wp-content/uploads/2023/09/DIA_secondo_semestre_2022Rpdf.pdf

EBA. (2022). FINAL REPORT ON GUIDELINES ON CUSTOMER DUE DILIGENCE AND THE FACTORS CREDIT AND FINANCIAL INSTITUTIONS SHOULD CONSIDER WHEN ASSESSING THE ML/TF RISK ASSOCIATED WITH INDIVIDUAL BUSINESS RELATIONSHIPS AND OCCASIONAL TRANSACTIONS. https://www.eba.europa.eu/sites/default/files/document_library/Publications/Guidelines/2021/963637/Final%20Report%20on%20Guidelines%20on%20revised%20ML%20TF%20Risk%20Factors.pdf

Ernst & Young. (2018). Can you transform your third parties' risk into a competitive advantage? https://assets.ey.com/content/dam/ey-sites/ey-com/en_ie/topics/advisory/transforming-your-third-party-risk-into-a-competitive-advantage.pdf

European Commission. (2022). Proposal for a directive of the European Parliment and of the Council on Corporate Sustainability Due Diligence and amending Directive (EU) 2019/1937. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52022PC0071

Europol. (2024). Decoding the Eu's Most Threatening Criminal Networks. https://www.europol.europa.eu/cms/sites/default/files/documents/Europol%20report%20on%20Decoding%20the%20EU-s%20most%20threatening%20criminal%20networks.pdf

Eurosif, IIGCC, & PRI. (2023). The EU Corporate Sustainability Due Diligence Directive: Key Questions Answered. https://www.eurosif.org/news/the-eu-corporate-sustainability-due-diligence-directive-key-questions-answered/

FATF. (2014). GUIDANCE FOR A RISK-BASED APPROACH. https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Risk-Based-Approach-Banking-Sector.pdf

FATF. (2023). INTERNATIONAL STANDARDS ON COMBATING MONEY LAUNDERING AND THE FINANCING OF TERRORISM & PROLIFERATION. https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

KPMG. (2022). Third-Party Risk Management Outlook 2022. https://kpmg.com/xx/en/home/insights/2022/01/third-party-risk-management-outlook-2022.html

McKinsey & Company, & ORIC International. (2017). Improving third-party risk management. https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/Risk/Our%20Insights/Improving%20third%20party%20risk%20management/Improving-third-party-risk-management.ashx

Moody's Analytics. (2023). The rising tide of third-party risk management: Surfacing risks to safeguard reputations. https://www.moodys.com/web/en/us/site-assets/ma-kyc-the-rising-tide-of-third-party-risk-management-report-LOWRES.pdf

Nicolazzo, G., Anastasio, M., & Riccardi, M. (2024). The Economic Interests of Russian Oligarchs in Italy: An Investigation into the Ownership of Italian Companies.

OECD. (2018). OECD Due Diligence Guidance for Responsible Business Conduct. https://mneguidelines.oecd.org/OECD-Due-Diligence-Guidance-for-Responsible-Business-Conduct.pdf

Peta, M. (2024). Adottata la Corporate Sustainability Due Diligence Directive, CSDDD. Fisco e Tasse. https://www.fiscoetasse.com/approfondimenti/15983-adottata-la-corporate-sustainability-due-diligence-directive-csddd.html

Transcrime (www.transcrime.it) è il Centro interuniversitario su criminalità e innovazione dell'Università Cattolica del Sacro Cuore, Alma Mater Studiorum Università di Bologna e Università degli Studi di Perugia. Fondato nel 1994, Transcrime è il principale hub di ricerca in Italia e in Europa per lo studio della criminalità organizzata e finanziaria. Ha condotto oltre 300 progetti a livello nazionale e internazionale, collaborando con enti di rilievo come le Nazioni Unite, la Commissione Europea, Europol, autorità di supervisione e forze di polizia a livello nazionale e internazionale. Sviluppa analisi dei fenomeni criminali complessi e applicazioni per le indagini finanziarie e la valutazione e prevenzione dei rischi associati alle terze parti per utenti pubblici e privati.

Crime&tech (www.crimetech.it) è lo spin-off universitario di Transcrime, che traduce le ricerche accademiche in analisi, soluzioni e strumenti per il settore pubblico e privato, per valutare, prevenire e ridurre i rischi di criminalità e per la sicurezza. È leader nella fornitura di indicatori di rischio per l'identificazione tempestiva di anomalie e imprese ad alto rischio e per la due diligence e il monitoraggio continuo di terze parti, come clienti e fornitori. Tramite l'impiego di approcci innovativi e AI, gli strumenti sviluppati da Crime&tech consentono la ricostruzione di strutture societarie e reti di relazioni complesse, la combinazione di banche dati e fonti non strutturate, e profilazione evoluta del rischio per lo svolgimento di indagini finanziarie e attività di due diligence sui partner commerciali.

Lab4Compliance è la prima associazione in Italia composta esclusivamente da professionisti *in-house* della Compliance. Mission dell'associazione è quella di sostenere e promuovere la cultura dell'etica e della compliance e le relative best practices attraverso la creazione di molteplici occasioni di confronto, discussione e approfondimento nonché di supportare i professionisti del settore creando modelli, metodologie e best practices condivise e sempre più strutturate.

Il DEMS (Dipartimento di Scienze Politiche e Relazioni Internazionali) dell'Università di Palermo è un dipartimento interdisciplinare (cui afferiscono storici, giuristi, economisti, sociologi, psicologi e politologi) incentrato su di un obiettivo comune di ricerca: elaborare i diversi saperi che concorrono a delineare le "cornici cognitive" sottostanti al duplice processo di integrazione europea e di auspicabile creazione di un nuovo assetto internazionale fondato su principi universalistici. In questo orizzonte, assumono rilievo centrale -tra gli obiettivi di ricerca- le prospettive di integrazione/armonizzazione tra gli ordinamenti giuridici, incluse le strategie di contrasto della criminalità e progettazione di direttrici di politica criminale creati a livello sopranazionale. Il DEMS tra le altre cose supporta organizzazioni pubbliche e private nel disegno di politiche organizzative utili a prevenire fenomeni di criminalità organizzata, finanziaria e corruzione, con particolare riferimento al D.Lgs 231/2001 e altra disciplina rilevante in questo ambito