protiviti
Global Business Consulting

# Insights

Face the Future with Confidence ®

Gennaio

RISK MANAGEMENT

2022

a cura di / **Emma Marcandalli**
Managing Director

a cura di / **Guido Zanetti**
Managing Director

## THIRD PARTY RISK

### Una visione olistica e digitale per gestirlo con efficacia

Con la pressione sulle supply chain seguita allo shock pandemico e alla successiva ripresa del ciclo economico, il rischio Terze Parti ha assunto un'importanza centrale e imposto una revisione del metodo con il quale è gestito. In questo ***Insights*** analizziamo le nuove sfide del Third Party Risk Management (TPRM), illustriamo il Framework Metodologico e Operativo proposto da Protiviti, le tecnologie digitali che lo abilitano e il percorso suggerito alle imprese.

Le risposte a quattro domande chiave sintetizzano la nostra visione.

**1) L'azienda dispone oggi di tutte le informazioni necessarie per determinare il profilo di rischio, individuale e complessivo, delle controparti aziendale?**

Probabilmente, no. Nella maggioranza delle organizzazioni la gestione delle Terze Parti e dei rischi connessi è oggi affidata a processi frammentati e non ancora completamente digitalizzati. Non sempre le diverse funzioni aziendali interessate agiscono in modo coordinato.

Ne deriva una conoscenza parziale dei fattori di rischio (della singola Terza Parte e complessiva) che penalizza l'efficacia delle decisioni manageriali.

2) **È possibile costruire un sistema che monitori l'evoluzione dei rischi generando alert automatici e tempestivi non appena si manifestino situazioni critiche?**

   Sì, a patto di modificare l'approccio adottando un Framework Metodologico e Operativo strutturato, fondato su una visione complessiva delle Terze Parti e abilitato da tecnologie digitali.

3) **Una piattaforma tecnologica integrata può gestire tutte le Terze Parti?**

   Un processo olistico di TPRM permette di gestire tutte le controparti e i rischi di diversa natura che possono originare (operativi, strategici, finanziari, di reputazione, legali/contrattuali, sicurezza, compliance, ecc). Con le soluzioni avanzate di *Natural Language Processing & Understanding* si possono oggi acquisire e analizzare informazioni, automaticamente e in *near real-time,* da molteplici fonti esterne (per esempio documenti, notizie, articoli, report, mail e comunicazioni), *tradurle* in informazioni strutturate e inserirle nel processo valutativo.

4) **Quali sono i benefici di questo approccio?**

   Oltre a ridurre gli errori e le inefficienze inevitabili in un sistema manuale, la gestione olistica e digitale del rischio Terze Parti può anticipare le situazioni critiche riducendo i costi operativi causati da livelli di servizio non ottimali e mitigando il rischio di contestazioni e sanzioni all'azienda o danni alla sua reputazione.

## LE NUOVE SFIDE DEL THIRD PARTY RISK MANAGEMENT

Il forte stress al quale, fin dall'inizio della pandemia, sono state sottoposte le supply chain ha riaffermato l'importanza strategica di gestire le Terze Parti e i rischi connessi, inducendo molte aziende a rivalutare l'efficacia dei programmi di Third Party Risk Management (TPRM).

Oggi la mitigazione dei rischi derivanti da relazioni configurabili come partnership strategiche oppure dipendenze più o meno marcate verso terzi richiede una conoscenza articolata e olistica dei fattori che possano mettere in crisi il soggetto terzo e quindi l'azienda.

Affidabilità e solidità economica non sono gli unici aspetti della controparte da monitorare. Molti altri possono creare danni economici all'azienda e alla sua reputazione: per esempio, gli aspetti legali e contrattuali rilevanti per la sostenibilità etica, sociale e ambientale della controparte; la compliance; la cyber security (di cui abbiamo parlato nel nostro **Insights** ***Supply Chain Security***).

Le interconnessioni del sistema economico globale e la necessità di accrescere la resilienza delle filiere hanno portato lo stesso legislatore nazionale ed europeo a imporre alle aziende strumenti idonei per la selezione e il monitoraggio delle Terze Parti (e.g. CCPA, FIPA, PIPEDA, le leggi SHIELD e LGPD) inclusi, a titolo di esempio, strumenti di due diligence in materia ambientale e di diritti umani delle catene di fornitura e relativi standard di riferimento (ISO 37001).

Oggi le aziende sviluppano partnership, accordi e collaborazioni per rinforzare il proprio network, sviluppare nuovi prodotti o migliorarne la qualità, così come garantire una maggiore flessibilità nella gestione della domanda di clienti e consumatori. Non sempre, invece, adottano un approccio integrato alla gestione delle Terze Parti e dei rischi connessi.

I processi, abitualmente, sono frammentati e gestiti verticalmente; le diverse funzioni aziendali non sono sempre coordinate e ciascuna ha una vista solo sulla propria sfera di competenza con una conseguente percezione incompleta degli elementi di rischio connessi alla Terza Parte.

Le principali criticità, diffuse in Italia, si possono schematicamente riassumere così:

- valutazioni focalizzate solo su contenimento dei costi e/o qualità della fornitura;
- scarso coordinamento delle funzioni aziendali coinvolte (Procurement, funzioni di business richiedenti, Qualità, Risk Management, Finance, Compliance / DPO, ESG / Sostenibilità, IT / Security, Legale);
- frammentazione delle metodologie e degli strumenti di valutazione e monitoraggio;
- elevata manualità delle attività dovuta alla frammentazione dei sistemi applicativi aziendali con conseguente scarsa fruibilità delle informazioni;
- scarsa fruizione d'informazioni esterne e di business intelligence che, al contrario, arricchirebbero il paniere d'informazioni riducendo il rischio di valutazioni autoreferenziali o basate su autodichiarazioni.

La buona notizia è che, dal nostro osservatorio, la sensibilità sul tema delle aziende è in chiara crescita.

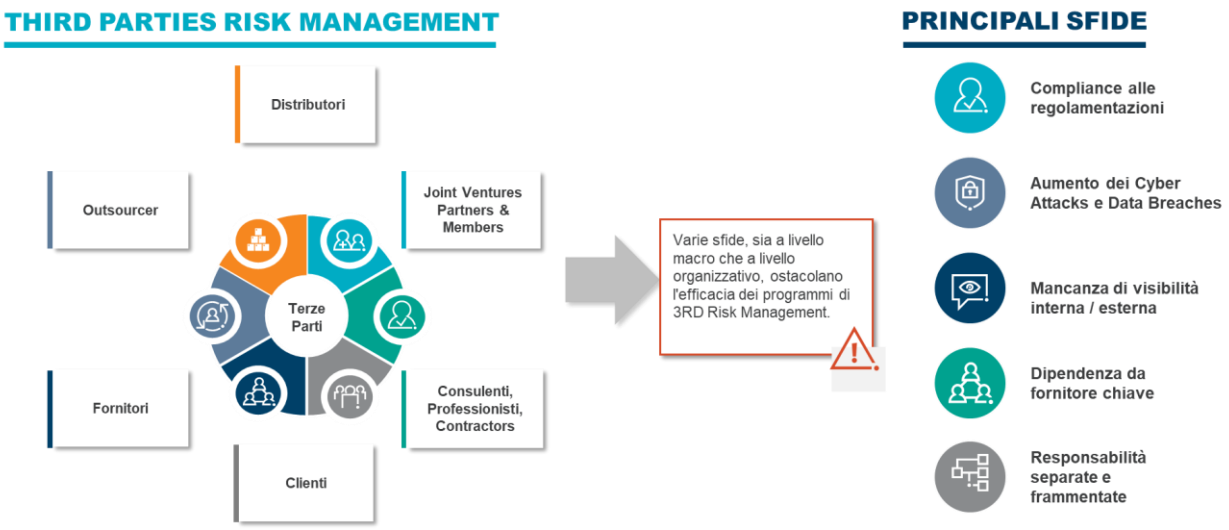
Tra le priorità generali delle Funzioni Finance, l'Italia conferma, in linea con le tendenze globali, l'esigenza di una gestione e analisi dei dati più avanzata e più efficiente, oltre alla gestione della sicurezza e privacy dei dati.

Altre tematiche su cui si riconferma l'attenzione includono l'esigenza di:

- adottare applicazioni cloud-base a supporto delle attività Finance,
- definire nuovi standard di contabilità e bilancio,
- migliorare i sistemi IT di gestione della contabilità e finanza.

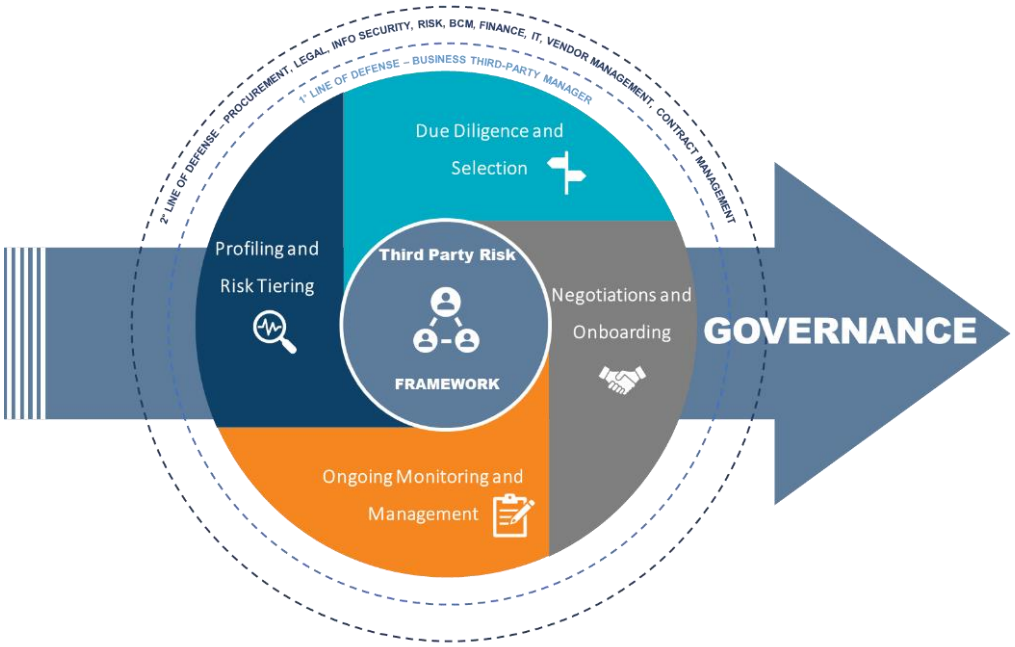
Relativamente alle **priorità** nel contesto nazionale su cui investire nei prossimi 12 mesi, i risultati emersi si discostano parzialmente dalle tendenze globali, posizionando al primo posto la necessità espressa dalle Funzioni Finance di focalizzarsi su Robotic Process Automation.

Un altro elemento che emerge è relativo alla crescente complessità nella predisposizione e pubblicazione dei report relativi a ESG e Human Capital, confermando quanto tali processi siano ben visti dagli *stakeholder* delle organizzazioni e producano valore aggiunto a lungo termine.



## VERSO UN TPRM INTEGRATO: IL FRAMEWORK DI PROTIVITI

Le criticità tipiche di un processo TPRM possono essere superate adottando un Framework Metodologico e Operativo strutturato, fondato su una visione complessiva delle Terze Parti e abilitato da tecnologie digitali. Il Framework proposto da Protiviti (*schematizzato nella figura qui sotto),* si compone di quattro fasi.




### Fase 1) Profiling & Risk Tiering

È necessario: (i) definire i driver di scoring (e.g. dimensioni e fattori di rischio), diversificati per tipologia di controparte e/o di contratto, e i relativi livelli di rischiosità; (ii) identificare i dati e le informazioni necessari per il *Risk Tiering*; (iii) comprendere dove tali dati e informazioni risiedono; (iv) creare un inventario unico delle Terze Parti.

Per questo occorre:

- definire le modalità di raccolta delle informazioni rilevanti rispetto a tutte le categorie di rischio applicabili alla controparte e/o all'incarico (e.g. questionari da compilare internamente o far compilare alla Terza Parte, acquisizione automatizzata di dati dai sistemi IT interni o da fonti esterne, etc.);
- stabilire come i dati devono essere elaborati e rappresentati (dashboard/reporting);
- decidere la frequenza con cui condurre le analisi e le valutazioni;
- stabilire le escalation decisionali in relazione ai livelli di rischio e alla loro evoluzione nel tempo.

È complesso e inefficiente gestire manualmente questa fase per tutte le Terze Parti.

Servono, per questo, supporti tecnologici, tipicamente rappresentati da strumenti GRC / di Risk Management, che permettono di definire un solido processo end-to-end di governance e coordinare la raccolta dei dati e la generazione di un reporting integrato.

### Fase 2) Due Diligence & Selection

È importante acquisire e analizzare informazioni di diversa natura, rilevanti per una corretta e completa valutazione della Terza Parte (e.g. aspetti di Compliance, Legali, Etico/Reputazionali, di Business, di Sicurezza Tecnologica). Questo processo va condotto non solo in fase di prima selezione, ma anche successivamente, secondo regole di frequenza e profondità adeguate al livello di rischio della controparte e delle relazioni sottostanti affinché il *Risk Tiering* risulti sempre aggiornato rispetto all'evoluzione degli scenari.

In questa fase le tecnologie digitali sono indispensabili per identificare e analizzare in modo intelligente una quantità importante di dati, spesso non strutturati, derivanti da fonti interne e/o esterne, gratuite e/o a pagamento. Diversi strumenti utilizzano oggi funzionalità avanzate di *Natural Language Processing and Understanding* che restituiscono all'utente insight pronti da utilizzare nei processi decisionali.

### Fase 3) Negotiations & Onboarding

Si focalizza sulla definizione degli aspetti contrattuali. La funzione responsabile dovrebbe tenere in considerazione sia i risultati della Due Diligence sulla Terza Parte sia i requisiti di business e il profilo di rischio del singolo incarico, ed essere in grado di evidenziare clausole di mitigazione del rischio, processi di escalation per vizi o violazioni, requisiti sulla sicurezza dei dati, requisiti sulla conformità a leggi e regolamenti, ecc.

### Fase 4) Ongoing Monitoring & Management

Sono monitorate le relazioni durante tutto il loro ciclo di vita di contratti, così come i rischi legati alle stesse Terze Parti. In particolare, sottolineiamo l'importanza che:

- le strutture aziendali interessate supervisionino attivamente le relazioni con le Terze Parti attraverso il monitoraggio di adeguati KPI;
- le valutazioni dei rischi siano eseguite con periodicità coerenti con i profili di rischio;
- le iniziative di mitigazione dei rischi siano identificate, tracciate e gestite;
- le funzioni Legal, Procurement e le altre funzioni coinvolte nella gestione della Terza Parte si coordinino per le attività di competenza e le azioni di mitigazione.

Anche queste attività si avvantaggiano di soluzioni di Data Analytics e reporting, al fine di gestire molteplici informazioni provenienti da diverse fonti e integrarle negli strumenti di GRC/Risk Management per l'aggiornamento del profilo di rischio e il monitoraggio delle azioni correttive in caso di superamento di soglie di accettabilità.

In tale ottica, anche il disegno di adeguati KPI/KRI diventa indispensabile sia per l'aggiornamento dinamico del *Risk Tiering*, sia per l'intervento tempestivo a fronte di criticità emergenti. Per operare efficacemente, le aziende possono dotarsi di portali per coordinare le attività lungo l'intero ciclo di vita dei contratti (dall'archiviazione della documentazione fino al monitoraggio dei Service Level Agreement).

In termini di governance, il coordinamento del Framework andrebbe attribuito alla funzione Risk & Compliance che, meglio di altre, potrebbe agevolare un approccio olistico e comune rispetto alle diverse metodologie di valutazione dei rischi e assicurare l'allineamento costante degli attori coinvolti. In alternativa, potrebbe essere costituito un Comitato manageriale inter-funzionale con un ruolo di supervisione e coordinamento. In un percorso di evoluzione digitale, è naturalmente essenziale il coinvolgimento proattivo delle strutture di Technology e Digital Transformation.

## Su quali tecnologie conviene puntare

La gestione manuale delle Terze Parti è ancora prevalente, ma gli applicativi disponibili sul mercato sono molti.

Nelle aziende in cui sono stati fatti i primi passi verso il digitale, si è agito settorialmente, con applicazioni standalone sviluppate per rispondere alle esigenze della funzione richiedente (Approvvigionamenti *versus* Risk *versus* Legal e Compliance, ecc.). Sono stati creati *ambienti chiusi*, incapaci di sfruttare in modo intelligente il patrimonio di dati generati dai sistemi aziendali e senza possibilità di successiva scalabilità o di futuri sviluppi basati, per esempio, sulle potenzialità dell'intelligenza artificiale.

La figura qui sotto rappresenta una mappa degli applicativi utilizzati per gestire le Terze Parti e i relativi rischi. Il quadro è articolato e non sempre allineato che penalizza efficacia/efficienza e impedisce di fornire al management una visione d'insieme, necessaria per un decision making tempestivo.

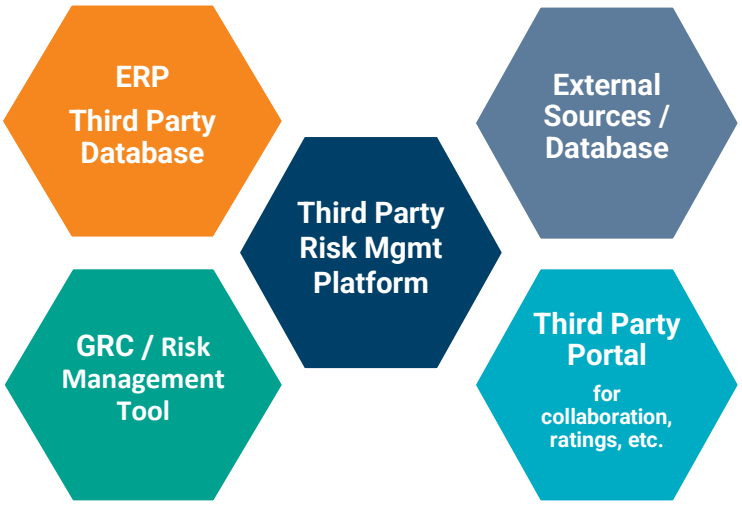

La scelta degli strumenti deve essere guidata dallo scenario ottimale al quale si vuole tendere.

Data la complessità del processo e i numerosi stakeholder coinvolti (interni ed esterni) sono necessari tool avanzati, i soli che consentano un efficace Framework Metodologico e Operativo.

La soluzione è una piattaforma integrata che copra tutte le fasi del processo. Gli strumenti tecnologici devono consentire:

- l'automazione dei processi;
- l'analisi intelligente di dati e informazioni (strutturate e non);
- l'automazione della reportistica (e.g. Risk Tiering & Profiling, dashboard KPI/KRI).

L'esperienza diretta nelle imprese indica che l'utilizzo di moderne piattaforme di TPRM è fondamentale per il coordinamento dei sistemi coinvolti *(rappresentato nella figura qui sotto).*



L'integrazione di queste piattaforme digitali, che possono essere adattate alle specifiche esigenze dell'organizzazione, garantisce le seguenti funzionalità:

- gestione integrata degli assessment di rischio;
- gestione di alert automatici in base alle logiche impostate in fase metodologica;
- capacità di scoring delle Terze Parti (inclusa la possibilità d'interagire con la Terza Parte attraverso un portale ad hoc per la raccolta d'informazioni);
- calcolo di KPI/KRI e proposta di evoluzione del Risk Tiering;
- organizzazione e monitoraggio delle azioni di Risk Mitigation;
- gestione dei workflow autorizzativi;
- reportistica con vari livelli di dettaglio.

La raccolta e l'interpretazione intelligente di dati e informazioni (ottenute anche da fonti esterne non strutturate) arricchiranno la piattaforma, consentendo il monitoraggio e l'aggiornamento continuo del profilo di rischio delle Terze Parti.

Risulterà preziosa l'integrazione con i sistemi della Terza Parte per arricchire il quadro con informazioni sui livelli di servizio erogati.


Grazie all'intelligenza artificiale, le soluzioni evolute di *Natural Language Processing & Understanding* permettono oggi di acquisire e analizzare, automaticamente e in *near real-time,* informazioni esterne non strutturate (documenti, notizie, articoli, report, mail e comunicazioni) sulle diverse Terze Parti (clienti, prospect, business partner, fornitori, ecc.), di **tradurle** in informazioni strutturate e inserirle (anche automaticamente) nel processo valutativo.

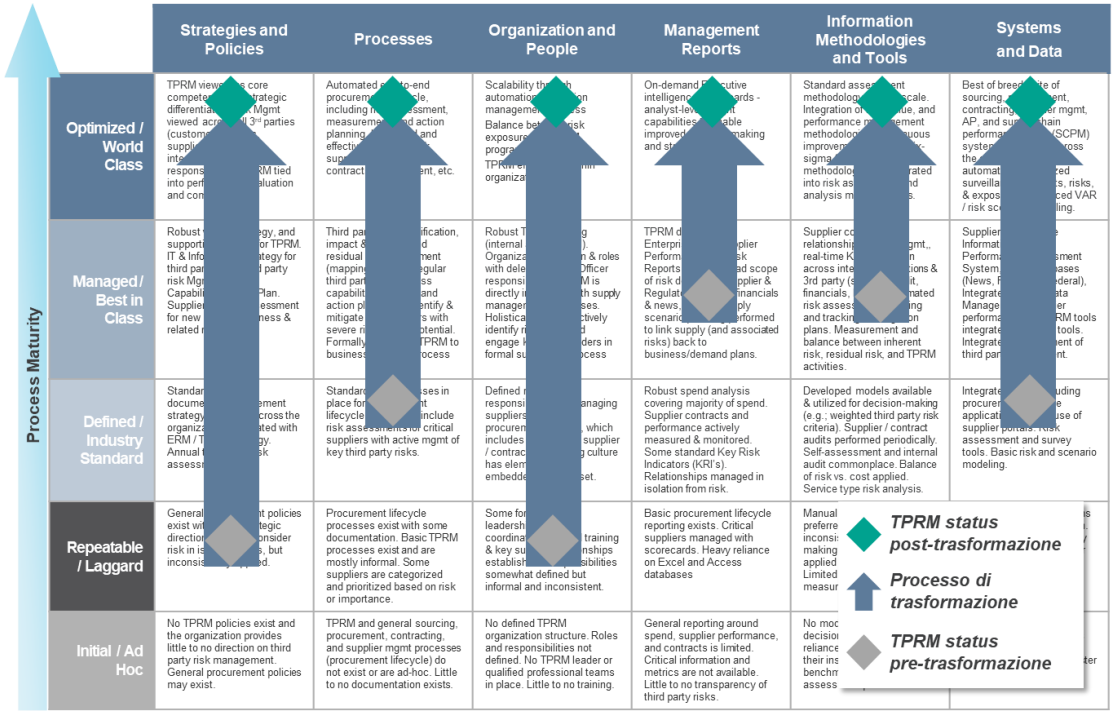
Tali soluzioni consentono schematicamente di:

- reperire informazioni da fonti esterne aperte e chiuse, ad accesso gratuito e/o a pagamento;
- effettuare scouting su fonti non strutturate (per esempio, siti web e social media);
- integrare le informazioni raccolte con quelle già disponibili nei sistemi informativi aziendali e interpretarle attraverso le tecnologie di *Natural Language Understanding*;
- estendere la copertura geografica dell'analisi grazie alla comprensione di più lingue;
- aggiornare le informazioni in modo automatico e in tempo reale.

## IL PERCORSO SUGGERITO

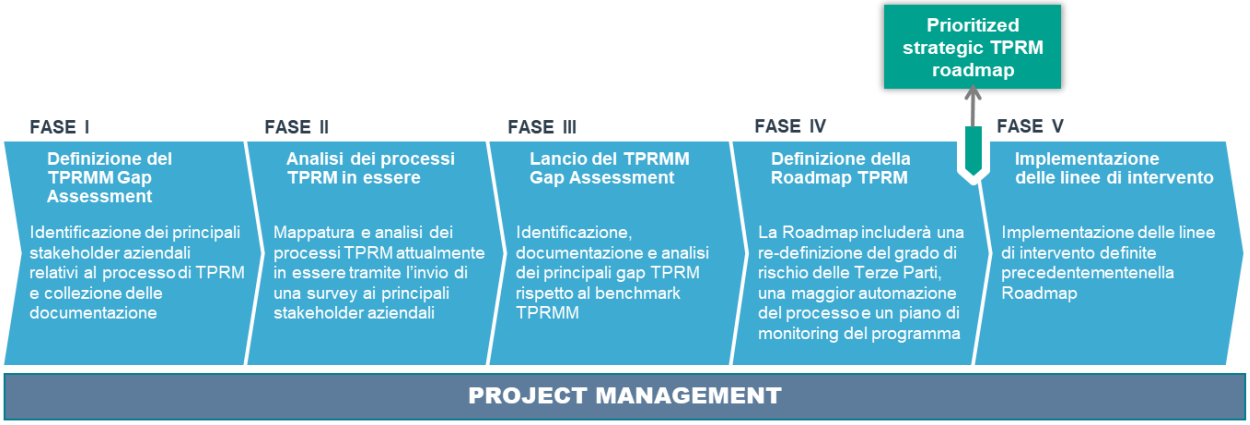
Grazie a un team multidisciplinare di professionisti specializzati nel Risk Management e in collaborazione con i propri partner tecnologici, Protiviti può affiancare le imprese in questo percorso evolutivo con un approccio adattabile alle caratteristiche dell'azienda e al livello di maturità nella gestione del rischio Terze Parti.

L'approccio proposto da Protiviti identifica lo stato di maturità dell'azienda attraverso il **Third Party Risk Maturity Model** (TPRMM), uno strumento di benchmarking (*esemplificato nella figura qui sotto*) costruito partendo dalle best practice internazionali nel TPRM.




L'approccio progettuale proposto, suddiviso in cinque fasi (*sintetizzate nella figura qui sotto*), assegna un livello di maturità ai diversi ambiti TPRM e consente di stabilire le aree prioritarie d'intervento.

L'esito è la costruzione di un percorso evolutivo sostenibile che bilancia maturità metodologica, digitalizzazione e sfruttamento delle tecnologie d'intelligenza artificiale, governance e copertura delle Terze Parti coinvolte.



## CONTATTI

**Emma Marcandalli**
Managing Director
emma.mercandalli@protiviti.it

**Guido Zanetti**
Managing Director
guido.zanetti@protiviti.it

protiviti®
Global Business Consulting