DOSSIER - TPCRM e resilienza digitale: proteggere la supply chain oggi

A cura di Federica Livelli

La sicurezza della supply chain è oggi una responsabilità imprescindibile. Le organizzazioni sono chiamate a governare in modo strutturato il rischio cyber ed operativo dei propri fornitori, sia ICT sia non ICT, per garantire la continuità operativa, la resilienza e l'affidabilità dell'intero ecosistema non solo digitale, ma anche operativo e di servizio.

Sommario

Introduzione

In uno scenario in continua evoluzione, la **digitalizzazione**, l'**outsourcing** e **l'interconnessione** stanno ridefinendo profondamente i modelli operativi delle

organizzazioni. Parallelamente, le minacce informatiche hanno assunto una dimensione **sistemica**, propagandosi lungo l'intera **supply chain** non solo **digitale**, ma anche **operativa e di servizio**.

Di conseguenza, la resilienza di un'organizzazione non può più essere considerata un elemento isolato: essa dipende in misura crescente dalla **resilienza dei propri fornitori e partner sia ICT sia non ICT,** che contribuiscono in modo diretto o indiretto all'erogazione di servizi critici e importanti. In tale contesto rientrano, oltre ai fornitori tecnologici, anche operatori logistici, outsourcer di servizi essenziali, fornitori di infrastrutture fisiche, servizi di manutenzione, facility management e altri soggetti esterni con accesso a sistemi, dati o processi aziendali.

Le organizzazioni si trovano, oggi, a operare in un contesto caratterizzato da: una crescente **dipendenza da ecosistemi di terze parti;** una **superficie d'attacco ampliata**; un **quadro normativo** sempre più **stringente** in materia di cybersecurity e resilienza operativa.

Inoltre, il contesto regolatorio europeo – **NIS2, DORA e GDPR** – introduce un cambio di paradigma chiaro: la sicurezza e la resilienza non sono più responsabilità esclusivamente interne, ma un obiettivo di **resilienza condivisa**, da governare attraverso un approccio **risk-based e resilience-based** continuo e orientato all'impatto operativo lungo l'intera supply chain, **digitale e non digitale**.

Scenario attacchi supply chain

Gli incidenti informatici più rilevanti registrati nel corso del 2025 hanno evidenziato una criticità ricorrente: **le vulnerabilità presenti all'interno delle catene di fornitura, sia digitali sia operative**. In numerosi casi, il punto di ingresso degli attacchi non è stato l'obiettivo finale, bensì uno o più fornitori, utilizzati come vettori per amplificare l'impatto operativo e reputazionale.

Oltre ai tradizionali **fornitori ICT**, sono sempre più frequenti eventi che coinvolgono **fornitori non ICT** – quali operatori logistici, servizi di manutenzione, outsourcing di processi di business o fornitori di infrastrutture fisiche – la cui compromissione può generare **effetti a cascata** su sistemi informativi, processi core e continuità dei servizi.

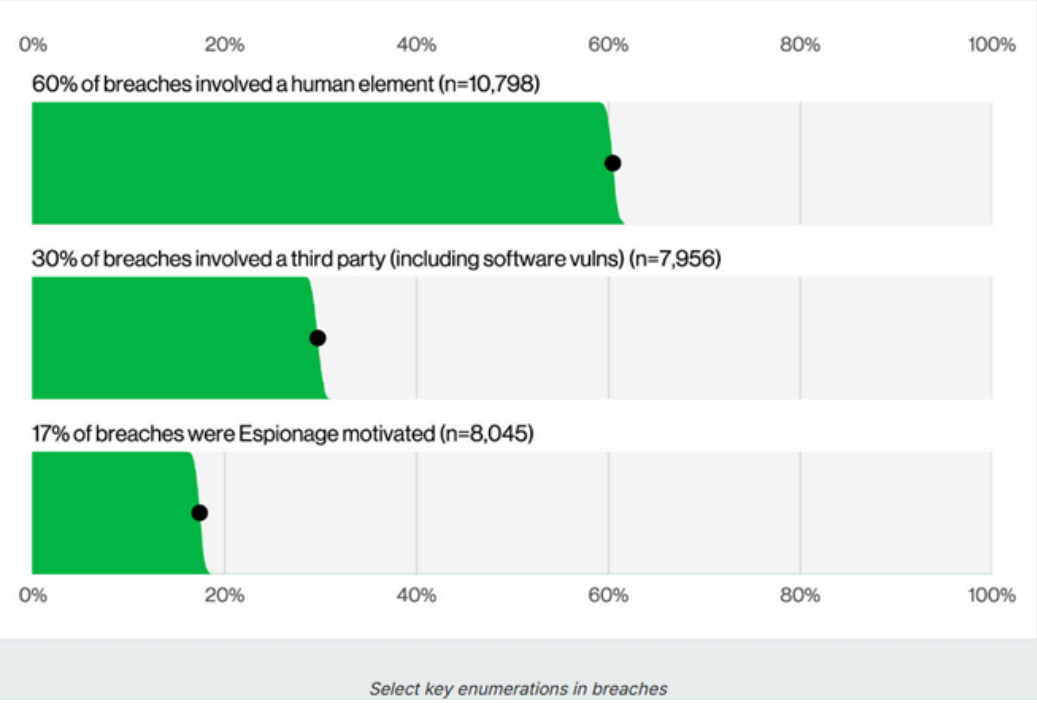
Inoltre, la **visibilità limitata sulla postura di sicurezza dei fornitori**, unita a modelli di protezione, ancora focalizzati prevalentemente sull'ambito ICT, incrementa significativamente l'esposizione complessiva al rischio lungo l'intera supply chain.

I threat actor sfruttano deliberatamente tali interdipendenze, colpendo la supply chain digitale per compromettere servizi critici e generare effetti a cascata su processi operativi e infrastrutture essenziali.

Evidenze dai report di settore

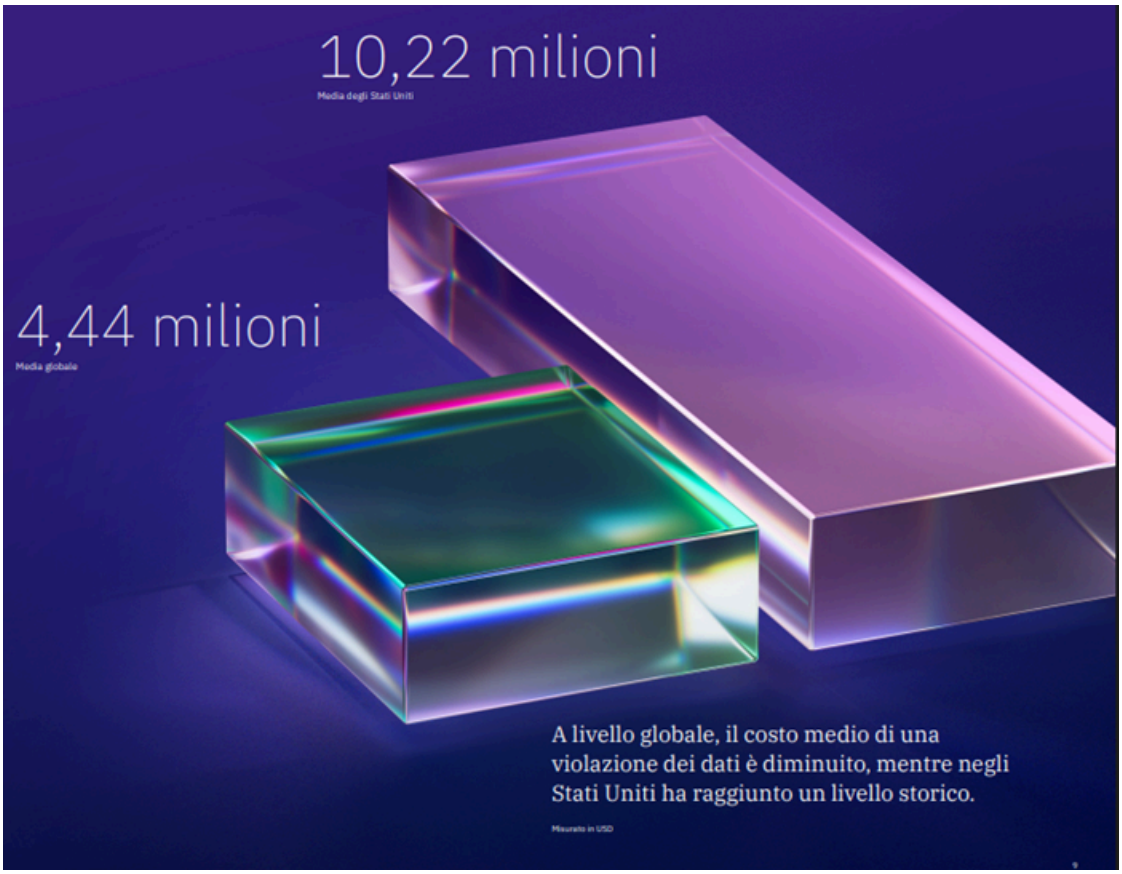
Le analisi più recenti confermano questa evoluzione del rischio:

· **Le violazioni che coinvolgono terze parti sono raddoppiate** in un solo anno, passando dal 15% al 30% del totale degli incidenti analizzati, a dimostrazione del ruolo sempre più centrale della supply chain come vettore di attacco. (*Fonte: Verizon Data Breach Investigations Report – DBIR - 2025*)



Fonte immagine Verizon DBIR 2025

· **Il costo medio globale di una violazione dei dati ha raggiunto i 4,44 milioni di dollari**, con valori che superano i 10 milioni di dollari negli USA, evidenziando l'impatto economico crescente degli incidenti cyber. Interessante notare che il costo medio in **Italia** è diminuito a **3,44 milioni di dollari**. (*Fonte: IBM Cost of a Data Breach Report 2025)*



Misurato in milioni di USD

#	Paese		2025	2024
1	Stati Uniti	↑	10,22 USD	9,36 USD
2	Medio Oriente	↓	7,29 USD	8,75 USD
3	Benelux	↑	6,24 USD	5,90 USD
4	Canada	↑	4,84 USD	4,66 USD
5	Regno Unito	↓	4,14 USD	4,53 USD
6	Germania	↓	4,03 USD	5,31 USD
7	America Latina	↓	3,81 USD	4,16 USD
8	Francia	↓	3,73 USD	4,17 USD

#	Paese		2025	2024
9	ASEAN	↑	3,67 USD	3,23 USD
10	Giappone	↓	3,65 USD	4,19 USD
11	Italia	↓	3,44 USD	4,73 USD
12	Corea del Sud	↓	2,84 USD	3,62 USD
13	Australia	↓	2,55 USD	2,78 USD
14	India	↑	2,51 USD	2,35 USD
15	Sudafrica	↓	2,37 USD	2,78 USD
16	Brasile	↓	1,22 USD	1,36 USD

Fonte immagini - IBM 2025 Cost of Data breach

· La maggior parte degli incidenti analizzati ha interessato **supply chain digitali**, inclusi software open source, piattaforme SaaS, servizi cloud e strumenti aziendali. Inoltre, in diversi casi, eventi di natura digitale hanno generato **interruzioni fisiche o operative**, confermando la stretta interdipendenza tra sistemi informativi e processi di business. *(Fonte: IBM Cost of a Data Breach Report 2025)*

· **Preoccupazione diffusa a livello organizzativo**: il **70% delle organizzazioni** dichiara un livello di preoccupazione molto o estremamente elevato rispetto

ai rischi di cybersecurity lungo la propria supply chain. *(Fonte: IBM Cost of a Data Breach Report 2025)*

· **Evoluzione delle strategie di attacco**: gli attori delle minacce si stanno spostando sempre più a monte nella catena di fornitura, sfruttando fornitori e partner come vettori per compromettere servizi digitali critici. (*Fonte: ISC2 – 2025 Supply Chain Risk Survey)*

· **Impatto operativo trasversale** degli attacchi alla supply chain sta producendo conseguenze concrete con impatti sulla continuità operativa di servizi essenziali ed importanti in molteplici settori industriali. (*Fonte: ISC2 – 2025 Supply Chain Risk Survey)*

Fonte immagine – 2025 ISC2 Supply Chain Survey

L'aumento della complessità tecnologica e dell'interdipendenza tra organizzazioni e fornitori rende sempre meno efficaci gli approcci frammentati o basati su valutazioni episodiche del rischio, richiedendo **un passaggio dalla gestione reattiva degli eventi alla costruzione di una resilienza strutturale della supply chain digitale**.

Pertanto, per rispondere a queste sfide, la gestione dei rischi cyber di terze parti non può più essere gestita come un insieme di attività manuali o scollegate, ma richiede **strumenti in grado di garantire visibilità end-to-end, continuità delle valutazioni e capacità di risposta coordinata** lungo l'intero ciclo di vita del fornitore.

Che cos'è la gestione dei rischi cyber di terze parti e cosa comporta

La **gestione dei rischi cyber di terze parti (Third Party Cyber Risk Management – TPCRM)** è un approccio strutturato volto a identificare, valutare e mitigare i rischi associati a **fornitori** e a **prestatori di servizi esterni ICT e non ICT**, che possono avere un impatto sulla cybersecurity, sulla protezione dei dati, sulla resilienza operativa e sulla continuità dei processi aziendali.

Il TPCRM riguarda **tutte le terze parti** che:

- hanno accesso a sistemi, reti o informazioni aziendali;
- supportano processi critici o essenziali;
- possono, in caso di incidente cyber o operativo, generare impatti significativi sull'organizzazione.

Da buona pratica volontaria, il TPCRM è oggi riconosciuto come **componente centrale dei principali framework di sicurezza e resilienza**, tra cui **ISO/IEC 27001, NIST Cybersecurity Framework, NIS2, DORA, PCI DSS v4.0, SOC 2 e GDPR**, che pongono crescente enfasi sulla gestione del rischio lungo l'intera supply chain.

In particolare, NIS2 e DORA richiedono che le misure di sicurezza siano estese anche a **fornitori e subappaltatori non ICT**, quando svolgono un ruolo essenziale nella continuità operativa, nella sicurezza dei servizi o nel supporto ai processi critici dell'organizzazione.

Inoltre, in presenza di carenze significative, le organizzazioni devono adottare misure correttive, fino alla possibile sostituzione del fornitore al fine di preservare la propria resilienza operativa.

ENISA – Linee guida per la sicurezza della supply chain

La **Direttiva NIS2** e il **Regolamento DORA** introducono una sfida critica per la sicurezza della supply chain, poiché la protezione di un'organizzazione risulta strettamente legata alla sicurezza dei suoi fornitori e prestatori di servizi. Di fatto, come è ben noto, una catena è forte quanto il suo anello più debole e la compromissione di un fornitore può compromettere l'intero ecosistema, con impatti che si estendono oltre il dominio digitale fino ai processi operativi e fisici.

L'**ENISA**, nelle proprie linee guida per la supply chain (ENISA - Good Practices for Supply Chain) evidenzia la necessità per le organizzazioni di **sviluppare e applicare politiche strutturate di sicurezza della supply chain**, estese all'intero ecosistema di fornitori e partner. Ciò richiede di identificare e di comunicare chiaramente il proprio ruolo all'interno della catena del valore e di governare in modo consapevole

le relazioni con **fornitori diretti e partner di servizi sia ITC sia non ICT**, al fine di mitigare i rischi non solo per i sistemi di rete e informativi, ma anche per i **processi operativi, logistici e fisici** che contribuiscono alla continuità dei servizi.

Il quadro di riferimento vigente, in tale prospettiva, spinge le organizzazioni a **coinvolgere attivamente i fornitori, incluse le PMI,** in un percorso strutturato di **rafforzamento della sicurezza informatica e della resilienza**. Tra le principali criticità della supply chain emergono accessi non sicuri, diffusione di malware, nonché **vulnerabilità nei processi operativi e logistici** che, non solo aumentano il rischio di compromissione, ma possono anche generare **interruzioni operative**, **ritardi nei servizi** e tempi di inattività con impatti economici, organizzativi e reputazionali rilevanti.

Migliori pratiche per i requisiti chiave di gestione del rischio da parte di terzi di NIS2 e DORA

La Direttiva NIS2 ed il Regolamento DORA includono raccomandazioni specifiche e migliori pratiche per le organizzazioni affinché possano gestire efficacemente i rischi di terze parti, qui di seguito riportate.

Stabilire politiche di sicurezza della catena di approvvigionamento

Le organizzazioni sono chiamate a definire **politiche strutturate e coerenti di sicurezza della supply chain**, capaci di governare in modo sistematico le relazioni con fornitori diretti e prestatori di servizi. Ciò implica la valutazione della **postura di sicurezza delle terze parti** e la verifica del loro allineamento agli **standard di cybersecurity** e ai requisiti normativi applicabili.

Pertanto, per rispondere a questa esigenza, è necessario adottare un **quadro organico di gestione del rischio di terze parti**, fondato su un approccio **risk-based** e **resilience-based** che includa:

- **Identificazione e prioritizzazione dei rischi** in funzione della criticità dei fornitori e dell'impatto operativo.
- **Valutazioni periodiche e audit di sicurezza**, proporzionati al livello di rischio;
- **Politiche e controlli** volti a garantire l'allineamento continuo delle terze parti agli standard di cybersecurity dell'organizzazione.

È doveroso evidenziare che, in tale contesto, assume un ruolo centrale anche il **coinvolgimento attivo dei fornitori** attraverso la messa a disposizione di

formazione, linee guida e risorse dedicate. Tale approccio consente alle terze parti di comprendere e rispettare i requisiti di sicurezza introdotti da **NIS2** e **DORA**, favorendo al contempo la **collaborazione**, la **condivisione delle informazioni sulle minacce emergenti** e l'adozione di **migliori pratiche comuni** lungo l'intera catena di fornitura.

Condurre analisi e valutazione del rischio

Le organizzazioni che rientrano nel perimetro di NIS2 e DORA sono tenute a svolgere una **due diligence strutturata e continua** e un'accurata **analisi del rischio** per identificare le potenziali vulnerabilità introdotte dalle terze parti. Ciò richiede la valutazione della **criticità dei servizi forniti** e del loro **impatto potenziale sulle operazioni**, sulla continuità operativa e sulla resilienza complessiva dell'organizzazione.

Pertanto, l'analisi deve includere la valutazione di:

- **postura di cybersecurity delle terze parti.**
- livello di **conformità agli standard di settore.**
- **capacità di prevenzione, risposta e recupero dagli incidenti**.

I fornitori, sulla base di tali elementi, devono essere **classificati e prioritizzati** in funzione della loro rilevanza operativa e del contributo al profilo di rischio complessivo.

Inoltre, le organizzazioni, per rendere questo processo sostenibile ed efficace nel tempo, dovrebbero adottare **soluzioni di TPCRM** in grado di **automatizzare e standardizzare le valutazioni**, nonché di mettere a disposizione un **repository centralizzato dei fornitori**. Tale approccio consente di mantenere una visione aggiornata e storicizzata del rischio, includendo valutazioni di sicurezza, stato di conformità e trend evolutivi, a supporto di decisioni informate e di un governo continuo del rischio di terze parti.

Garantire procedure adeguate di gestione e segnalazione degli incidenti

Le organizzazioni devono dotarsi di **procedure chiare e strutturate** per la gestione degli incidenti di cybersecurity che coinvolgono le terze parti. Ciò comprende il **rilevamento**, la **risposta** e la **segnalazione tempestiva** degli incidenti alle autorità competenti, assicurando che gli eventi di sicurezza originati dai fornitori siano trattati con lo **stesso livello di rigore** di quelli interni, rispettando le tempistiche stabilite dal quadro normativo.

Inoltre, per rispondere a tale esigenza, è necessario definire un **piano unificato di incident response** che includa il coordinamento delle terze parti lungo l'intero ciclo di gestione dell'incidente. In particolare, il piano dovrebbe prevedere:

- **Canali di comunicazione formalizzati** per la segnalazione e l'escalation degli incidenti.
- **Processi congiunti di analisi, indagine e risoluzione**, con ruoli e responsabilità chiaramente definiti.
- **Attività di revisione post-incidente**, finalizzate al miglioramento continuo delle pratiche di gestione del rischio e al rafforzamento delle misure di prevenzione.

Ancora, le organizzazioni dovrebbero considerare la **copertura assicurativa cyber** come strumento di gestione del rischio residuo, valutando se le polizze dell'organizzazione e quelle dei fornitori siano adeguate a coprire gli impatti derivanti da incidenti che coinvolgono la **supply chain**.

Monitorare e valutare continuamente terze parti

Il **monitoraggio continuo** delle pratiche di sicurezza delle terze parti rappresenta un elemento essenziale per garantire l'efficacia nel tempo delle misure di gestione del rischio.

Le organizzazioni devono valutare regolarmente l'adeguatezza dei controlli adottati dai fornitori e adattare il proprio modello di governance in funzione dell'evoluzione delle minacce e del contesto operativo.

Inoltre, un processo strutturato di monitoraggio continuo dovrebbe includere valutazioni periodiche di cybersecurity, attività di audit e, ove appropriato, test di sicurezza, nonché l'aggiornamento dinamico delle valutazioni del rischio in presenza di nuovi eventi o cambiamenti rilevanti.

Tale approccio consente di mantenere una visione costantemente aggiornata del profilo di rischio dei fornitori e di supportare decisioni tempestive a tutela della resilienza complessiva della supply chain.

Far rispettare gli obblighi contrattuali

Le organizzazioni devono includere **requisiti di cybersecurity chiari, applicabili e verificabili nei contratti con le terze parti**, al fine di garantire un allineamento effettivo ai requisiti normativi e ridurre i rischi lungo la catena di fornitura. In linea con **NIS2** e **DORA**, la contrattualizzazione rappresenta uno strumento fondamentale

per rendere **vincolanti** le misure di sicurezza richieste e assicurare un governo efficace e continuativo del rischio di terze parti.

Tra gli elementi chiave da includere nei contratti con i fornitori rientrano:

- **Clausole di conformità**, che impongano il rispetto dei requisiti di sicurezza applicabili, inclusi quelli previsti dalla **Direttiva NIS2** e dal **Regolamento DORA**.
- **Obblighi di segnalazione degli incidenti**, con tempistiche e modalità chiaramente definite per la notifica tempestiva degli eventi di cybersecurity, in coerenza con i requisiti di incident reporting.
- **Diritti di audit**, che consentano la verifica periodica delle pratiche di sicurezza adottate dalle terze parti.
- **Clausole di risoluzione**, che prevedano la possibilità di interrompere il rapporto contrattuale in caso di mancata conformità o di livelli di sicurezza non adeguati.
- **Requisiti di certificazione**, in particolare per i fornitori critici, quali **ISO/IEC 27001**, **ISO 22301** o l'adesione ai **CIS Controls**. In specifici settori regolamentati possono inoltre essere richiesti schemi di certificazione dedicati, quali: gli **European Cybersecurity Certification Schemes**. In ambito software, programmi quali **SAFECode** o le certificazioni **BSI per Secure SDLC** possono attestare l'adozione di processi di sviluppo sicuri.

Piattaforme TPCRM – ruolo su maturità fornitori, costi, tempi e frizioni

Le piattaforme di **TPCRM** svolgono un ruolo strategico che va oltre la mera compliance normativa. Esse consentono alle organizzazioni di **governare in modo strutturato, continuo e misurabile il rischio di terze parti** e, al contempo, di promuovere un **percorso di maturazione della cybersecurity dei fornitori sia ICT sia non ICT**, favorendo l'adozione di **standard condivisi**, una maggiore **trasparenza informativa** e una collaborazione più efficace lungo l'intera supply chain.

Attraverso l'automazione delle valutazioni, il monitoraggio continuo del profilo di rischio e la standardizzazione dei processi di gestione, una piattaforma di TPCRM contribuisce a **ridurre costi**, **tempi e complessità operative**, superando approcci manuali o frammentati. Al contempo, essa migliora la **qualità** e **l'affidabilità delle informazioni disponibili** e rafforza il **dialogo strutturato con i fornitori**, rendendo sostenibile nel tempo la gestione del rischio di terze parti.

Pertanto, il TPCRM si configura come un **abilitatore di resilienza dell'ecosistema**, in grado di supportare la capacità complessiva di **prevenire, assorbire e rispondere** agli incidenti cyber e operativi che possono originarsi lungo la supply chain.

Le piattaforme TPCRM integrano un insieme di funzionalità che rendono possibile una **gestione efficace, continua e proporzionata del rischio di terze party** lungo l'intero ciclo di vita del fornitore, quali:

- mappatura e classificazione risk-based dei fornitori ICT e non ITC;
- valutazioni strutturate di cybersecurity e di resilienza;
- automazione dei processi di assessment e re-assessment;
- monitoraggio continuo del profilo di rischio;
- tracciamento dei requisiti contrattuali e degli obblighi di sicurezza;
- produzione di report e indicatori di governo a supporto delle decisioni del management.

Conclusione

Il quadro normativo europeo ha ridefinito l'approccio alla gestione del rischio cyber, spostando l'attenzione da controlli isolati a un **modello strutturato, continuo e basato sul rischio**, orientato alla resilienza dell'intero ecosistema digitale.

Nel 2026, approcci frammentati o fondati su valutazioni episodiche non risultano più sostenibili, né sul piano operativo né su quello regolatorio. Inoltre, la **gestione strutturata del rischio cyber ed operativo di terze parti** si afferma come **elemento centrale della resilienza organizzativa**, estesa ai fornitori, ICT e non ICT, che contribuiscono al funzionamento dell'organizzazione.

Le **piattaforme di TPCRM** rappresentano, quindi, lo **strumento operativo** per tradurre tale approccio in capacità concrete e misurabili, favorendo una **visione integrata del rischio lungo l'intera supply chain**.

Federica Maria Rita Livelli, Consulente in Risk Management & Business Continuity, svolge un'attività di diffusione e sviluppo della cultura della resilienza presso varie istituzioni e università italiane e straniere.

È membro de: CLUSIT – Direttivo; BCI - Cyber Resilience Group; FERMA Digital Committee.

Svolge attività di docente di moduli di resilienza presso l'Università Genova – Master Infrastrutture Critiche, l'Università di Udine -Master di Intelligence & ICT e l'Università di Verona – RiskMaster.

Relatrice e moderatrice in diversi seminari, conferenze nazionali ed internazionali, autrice di numerosi articoli e white paper su diverse riviste italiane e straniere.

Co-autrice de: Rapporto Clusit - Cyber Security (ed. dal 2020 ad oggi); Libri tematici CLUSIT rif. Intelligenza Artificiale (2020) e Rischio Cyber (2021), Supply Chain Risk (2023); "Lo Stato in Crisi" ed. Angeli (2022); "The ACP book of best practices 3rd edition - Important topics within resilience (2025).