RAF assicurazioni: gestione dei rischi Non-Pillar I tra DORA, ORSA e AI Act

Il **Risk Appetite Framework (RAF)** delle compagnie assicurative è stato storicamente costruito attorno ai rischi quantificati dal **Pillar I di Solvency II**, come rischio di mercato, credito, sottoscrizione e rischio operativo.

Oggi, però, il contesto normativo europeo sta cambiando rapidamente. Framework regolamentari come **DORA**, **AI Act**, **Solvency II Review**, **IDD**, **POG** ed evoluzioni EIOPA stanno imponendo alle compagnie assicurative un presidio sempre più strutturato anche dei cosiddetti **rischi Non-Pillar I**.

Si tratta di rischi che spesso non generano direttamente un requisito patrimoniale SCR, ma che possono produrre impatti significativi su:

- continuità operativa,
- liquidità,
- compliance normativa,
- reputazione,
- sostenibilità,
- resilienza aziendale.

Tra i principali rischi Non-Pillar I rientrano:

- rischio cyber,
- rischio ESG,
- rischio di liquidità,
- rischio di condotta,
- rischio reputazionale,
- rischio AI,

- rischio ICT.

Nel nuovo scenario regolamentare assicurativo, il tema non è più stabilire se questi rischi debbano entrare nel RAF, ma dimostrare con criteri metodologici documentati perché alcuni rischi possano eventualmente restarne esclusi.

Questo articolo analizza:

- il ruolo dei rischi Non-Pillar I nel RAF assicurativo;
- gli impatti della Solvency II Review;
- il raccordo con ORSA e governance;
- le aspettative IVASS ed EIOPA;
- le migliori pratiche di classificazione, monitoraggio e gestione dei KPI di rischio.

DORA, Solvency II Review e AI Act: le nuove normative sui rischi Non-Pillar I

L’evoluzione della normativa europea sta modificando in profondità il modo in cui le compagnie assicurative devono presidiare i rischi Non-Pillar I all’interno del RAF e del sistema di governance aziendale. Framework come DORA, Solvency II Review, AI Act, IDD e POG ampliano infatti il perimetro dei rischi considerati rilevanti ai fini della resilienza operativa, della continuità aziendale e della stabilità prudenziale.

DORA e il rafforzamento del rischio cyber

Con l’entrata in vigore del **Regolamento DORA (UE 2022/2554)** da gennaio 2025, il rischio ICT e cyber assume un ruolo sempre più centrale nel sistema di controllo interno delle compagnie assicurative. Il framework introduce obblighi strutturati in

materia di resilienza operativa digitale, richiedendo un presidio più evoluto dei fornitori tecnologici critici, test periodici di resilienza (TLPT), processi di incident reporting e monitoraggio continuo del rischio cyber.

In questo contesto, considerare il rischio cyber come "non significativo" ai fini RAF risulta sempre più difficile da sostenere sotto il profilo regolamentare e di vigilanza.

Solvency II Review, rischio ESG e rischio di liquidità

La Solvency II Review – Direttiva 2025/2/UE rafforza ulteriormente il ruolo dei rischi Non-Pillar I all'interno del sistema di governo societario. Le nuove disposizioni richiedono infatti una maggiore integrazione dei rischi ESG e del rischio di liquidità nei processi ORSA, nei piani di gestione della liquidità e nelle valutazioni prospettiche della solvibilità.

Le aspettative di EIOPA e delle Autorità di Vigilanza si stanno orientando verso un approccio sempre più forward-looking, basato su stress test, analisi di scenario e capacità delle compagnie di dimostrare una gestione strutturata dei rischi emergenti.

In questo scenario, il rischio ESG smette di essere esclusivamente un tema reputazionale o strategico e diventa un elemento centrale del framework di risk management.

IDD, POG e rischio di condotta

Anche il rischio di condotta assume oggi una rilevanza crescente. Le disposizioni IDD, POG e il Regolamento IVASS n. 45/2020 rafforzano infatti il monitoraggio dei processi distributivi e della tutela del cliente.

Indicatori come reclami fondati, riscatti anomali o criticità

rilevate nei processi commerciali rappresentano segnali sempre più osservati dalle Autorità di Vigilanza nella valutazione del profilo di rischio delle compagnie assicurative.

AI Act e rischio Intelligenza Artificiale

Un ulteriore fronte emergente riguarda l'Intelligenza Artificiale. L'**AI Act (Reg. UE 2024/1689)** introduce nuovi obblighi per gli algoritmi utilizzati nei processi assicurativi, dalla tariffazione alla profilazione dei clienti, fino alla liquidazione automatizzata dei sinistri.

Il rischio AI assume quindi una dimensione trasversale che coinvolge aspetti operativi, regolamentari, reputazionali e di condotta. Per questo motivo, l'Intelligenza Artificiale non può più essere trattata esclusivamente come tema tecnologico, ma richiede un presidio strutturato anche all'interno del RAF e dell'ORSA.

La classificazione di un rischio come "non significativo" ai fini del RAF, in assenza di una motivazione analitica documentata, risulta oggi sempre meno sostenibile rispetto alle aspettative normative e di vigilanza di IVASS, EIOPA e del nuovo quadro regolamentare europeo.

Come mappare i rischi Non-Pillar I nel RAF assicurativo

La nostra esperienza sul campo ha portato a identificare numerose tipologie di rischi Non-Pillar I rilevanti per una compagnia assicurativa vita e/o danni.

Non tutti i rischi sono significativi ai fini del RAF: la classificazione della significatività è il primo step metodologico fondamentale, che richiede un processo strutturato che coinvolge gli owner naturali di ciascun rischio, prima però tutti i rischi devono prima essere mappati

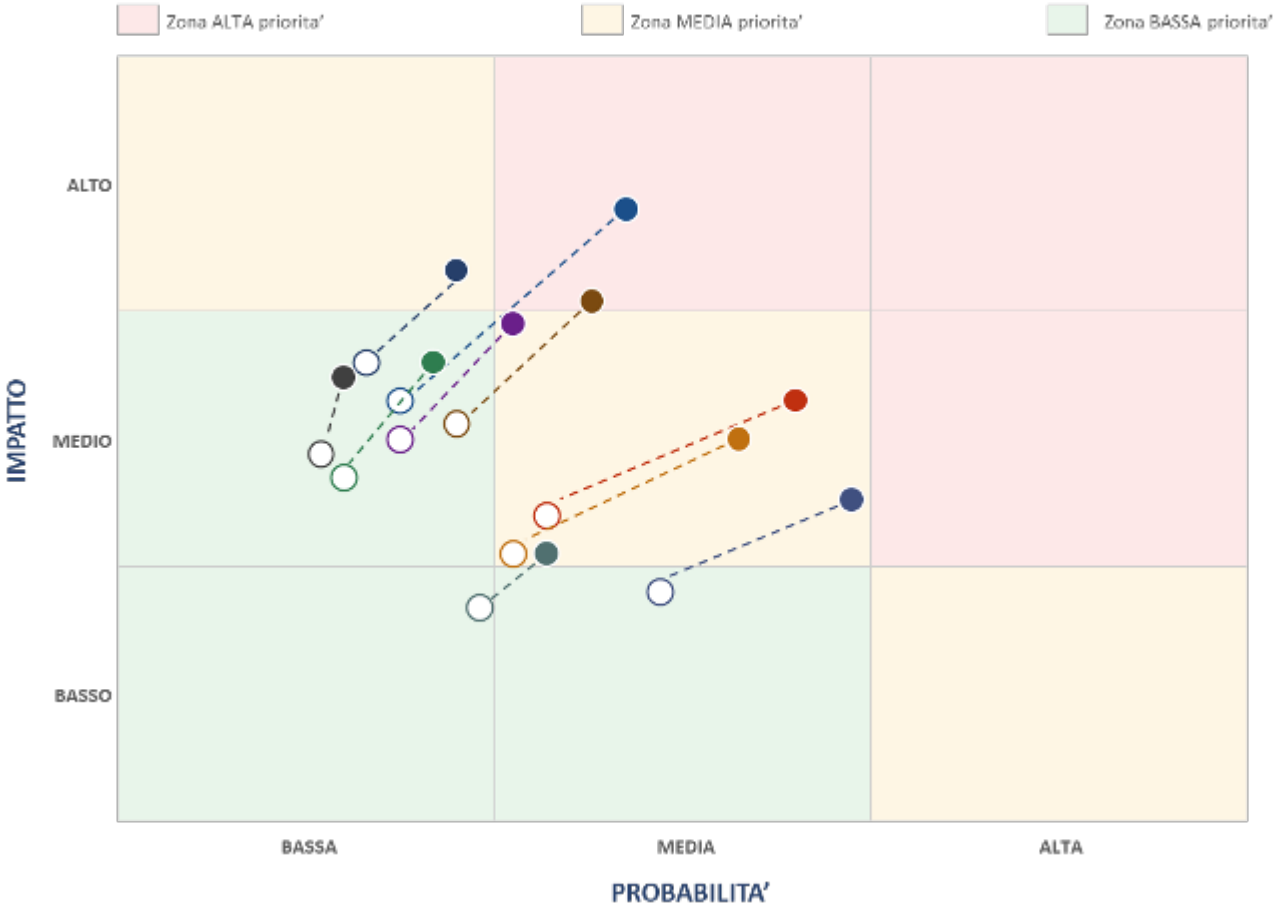
ed organizzati in cluster omogenei per natura, owner e tipologia di metriche di monitoraggio. Di seguito un esempio illustrativo:

#	Cluster di rischio	Owner	Rischi mappati
1	Operativo e di Processo	Risk / COO	Cyber/ICT, Interruzione processi core, Outsourcing critico, Frode interna/esterna, Business Continuity, Errore operativo sistematico, ...
2	Condotta e Conformità	Compliance / Legal	Condotta/mis-selling, Conformità normativa, Value for Money, Conflitti di interesse, Rischio legale/contenzioso, Rischio fiscale, Sanzione amministrativa, ...
3	Strategico e di Business	CEO / CFO / CRO	Rischio Strategico, Redditività, IA, Perdita quota di mercato, Obsolescenza modello distributivo, Trasformazione digitale, Rischio Emergente, ...
4	Reputazionale e di Gruppo	DG / Comunicazione	Rischio Reputazionale, Contagio, Crisi mediatica/social, Perdita fiducia distributori, ...
5	ESG e Sostenibilità	CRO / Investimenti	Rischio climatico fisico, Rischio climatico di transizione, ESG portafoglio investimenti, Rischio sociale supply chain, Greenwashing/qualità dato ESG, ...
6	Rischi Finanziari Specifici	Risk / ALM / Attuariato	Spread Titoli Governativi (BTP), Liquidità, ...

Come classificare la significatività dei rischi Non-Pillar I nel RAF

Identificati i rischi per cluster, il passaggio critico è la classificazione della significatività ai fini RAF. Non si tratta di una scelta a tavolino: richiede un processo strutturato di interviste agli owner naturali di ciascun rischio, finalizzato a raccogliere evidenze sulla probabilità di manifestazione e sull’impatto potenziale sulla Compagnia.

La heatmap che ne risulta ha una doppia valenza: fotografa il posizionamento attuale percepito e visualizza il posizionamento target verso cui il piano di mitigazione deve tendere. È lo strumento che rende la conversazione sul rischio concreta, condivisibile tra funzioni diverse e documentabile verso il regolatore.



[redacted]

KPI e KRI nel RAF assicurativo: esempi e metodologia

Il contributo metodologico più rilevante di un RAF ben costruito è la definizione di una architettura gerarchica degli indicatori che distingue in vari livelli, ciascuno con una funzione precisa nel sistema di governo del rischio. Di seguito un’architettura tipo:

Livello	Natura	Esempi KPI	Soglie	Escalation	ORSA
I Livello (Business)	Metriche attraverso cui il CdA esplicita la propensione al rischio approvata.	• Solvency Ratio • Liquidità • Redditività •	• Appetite • Tolerance • Limit	Formale	Sempre
II Livello (Gestionali)	Metriche che il RM usa per integrare e anticipare l'evoluzione del profilo di rischio.	• SCR Spread • Cyber • ESG • Condotta •	• Target	Informativa	Sempre + focus se fuori Target
III Livello (Operativi)	Rischi non significativi presidiati con indicatori tecnici e trigger operativi.	• KPI Tecnici	• Trigger	Operativa	Non inclusi

I rischi Non-Pillar I significativi possono essere rappresentati nel RAF sia come indicatori di I livello sia di II livello, in funzione della loro rilevanza strategica e regolamentare.

Rischi come, ad esempio, liquidità e redditività richiedono infatti un presidio diretto a livello di CdA, mentre altri (Cyber, Condotta, ESG) possono essere monitorati tramite KPI gestionali e soglie Target dedicate. Non sono indicatori "minori": presidiano rischi che il Pillar I non cattura integralmente.

Metodologia di calibrazione delle soglie Target nel RAF assicurativo

La soglia Target non genera escalation automatica. È il livello di riferimento che consente al Risk Manager di rispondere a una domanda semplice: il rischio è nella norma, o sta evolvendo in modo che richiede attenzione? La sua calibrazione segue una gerarchia di fonti documentate:

1. Dati storici interni – Distribuzione storica del KRI negli

ultimi 3-5 anni. Soglia = percentile 75° (rischi di frequenza) o media + 1 deviazione standard (rischi continui). Fonte primaria dove disponibile.

2. Benchmark di settore – Relazione annuale IVASS, Risk Dashboard EIOPA, loss database ORX (cyber), dati ANIA per indicatori tecnici vita e danni. Usato quando i dati interni sono insufficienti.

3. Piano Industriale – Per rischi di business (redditività, strategico): la soglia Target è il valore coerente con gli obiettivi approvati dal CdA, più una tolleranza operativa definita.

4. Requisiti normativi – Floor assoluto: nessuna soglia Target può essere più permissiva del requisito normativo (es. DORA per cyber, limiti IVASS su reclami fondati).

Dove nessuna fonte quantitativa è disponibile, la posizione nella heatmap costituisce il riferimento qualitativo, con impegno a sviluppare una metrica nel ciclo di revisione successivo.

Integrazione tra RAF, ORSA e rischi Non-Pillar I

Un errore frequente nella progettazione del RAF è pensare che i rischi Non-Pillar I non entrino nell'ORSA o solo quando superano una determinata soglia. È il contrario.

Tutti i rischi Non-Pillar I classificati come significativi devono essere oggetto di valutazione prospettica nell'ORSA, questo perché' l'ORSA, ai sensi dell'art. 45 della Direttiva Solvency II e del Reg. IVASS n. 43/2018, deve coprire tutti i rischi a cui la compagnia è materialmente esposta, indipendentemente dalla loro natura.

Il superamento della soglia Target non apre la porta all'ORSA:

quella porta è già aperta, può cambiare però il livello di approfondimento:

- KPI in Target: Valutazione ORSA standard, conferma del profilo di rischio, scenario avverso con impatto stimato.

- KPI fuori Target per n. rilevazioni consecutive: Valutazione ORSA approfondita, analisi delle cause, stress test dedicato (scenario analysis forward + reverse stress test), stima impatto su Own Funds, valutazione adeguatezza capitale e misure di mitigazione.

Il rischio di liquidità nel RAF assicurativo e nella Solvency II Review

Il rischio di liquidità merita un trattamento a parte. La formula standard Solvency II non prevede un requisito di capitale (SCR) specifico per il rischio di liquidità: tecnicamente è quindi un rischio Non-Pillar I. Eppure, nella pratica di mercato e nelle aspettative regolamentari viene trattato come rischio di primo livello nel RAF, con soglie e processo di escalation formali.

La Solvency II Review (Direttiva 2025/2/UE) rafforza esplicitamente questo orientamento: introduce disposizioni più stringenti in materia di piano di gestione della liquidità (Liquidity Risk Management Plan), richiedendo alle imprese di valutare sistematicamente il proprio profilo di liquidità anche in situazioni di stress, identificare le fonti di rischio e predisporre misure di contingenza documentate. EIOPA ha già fornito orientamenti specifici in materia (Guidelines on liquidity risk management, EIOPA-BoS-14/238).

Le dimensioni del rischio di liquidità rilevanti per una compagnia assicurativa vita e danni sono almeno due:

• Liquidità di funding: incapacità di far fronte agli impegni verso gli assicurati (rimborsi, liquidazioni sinistri, riscatti) nei tempi contrattualmente previsti, senza dover liquidare attivi a prezzi sfavorevoli. Particolarmente rilevante per i rami vita con garanzie di rendimento e per i prodotti con opzioni di riscatto.

• Liquidità di mercato: incapacità di liquidare posizioni nel portafoglio investimenti a prezzi di mercato in tempi ragionevoli, con impatto sul valore degli attivi a copertura delle riserve tecniche. Amplificata in scenari di stress correlati: es. shock sui titoli governativi contestuale a un aumento dei riscatti.

Il rischio di liquidità è il caso più chiaro in cui la distinzione Pillar I / Non-Pillar I non coincide con la distinzione significativo / non significativo. Va trattato come rischio di I livello nel RAF, con KPI dedicati (Liquidity coverage ratio base e stressato) e raccordo esplicito con l'ORSA e il piano di gestione della liquidità richiesto dalla Solvency II Review.

AI Act e rischio Intelligenza Artificiale nelle compagnie assicurative

Tra i rischi emergenti del Cluster Strategico, quello legato all'Intelligenza Artificiale merita un cenno specifico. L'AI Act – Reg. UE 2024/1689, in applicazione progressiva dal 2025 al 2027, introduce una classificazione dei sistemi di IA per livello di rischio. Per le compagnie assicurative, l'utilizzo di algoritmi nella tariffazione, nella selezione del rischio, nella liquidazione automatica dei sinistri o nella profilazione dei clienti può rientrare nelle categorie ad alto rischio.

L’AI rischia di entrare nelle compagnie come tema IT, ma di trasformarsi rapidamente in rischio reputazionale, regolamentare e di condotta.

Il rischio IA è al tempo stesso:

• Rischio operativo: errori algoritmici, bias nei modelli di tariffazione e scoring, opacità delle decisioni automatizzate.

• Rischio di conformità: AI Act (sistemi ad alto rischio), GDPR, IDD su spiegabilità delle decisioni al cliente.

• Rischio reputazionale: decisioni automatizzate non spiegabili verso il cliente, potenziale discriminazione algoritmica, esposizione mediatica.

Governance documentale RAF: cosa chiedono IVASS ed EIOPA

Avere un RAF Non-Pillar I tecnicamente corretto non basta. La vera opportunità di differenziazione è la robustezza documentale del framework:

• Per ogni rischio classificato come non significativo: deve esistere una motivazione analitica documentata, non è sufficiente l’assenza di eventi storici.

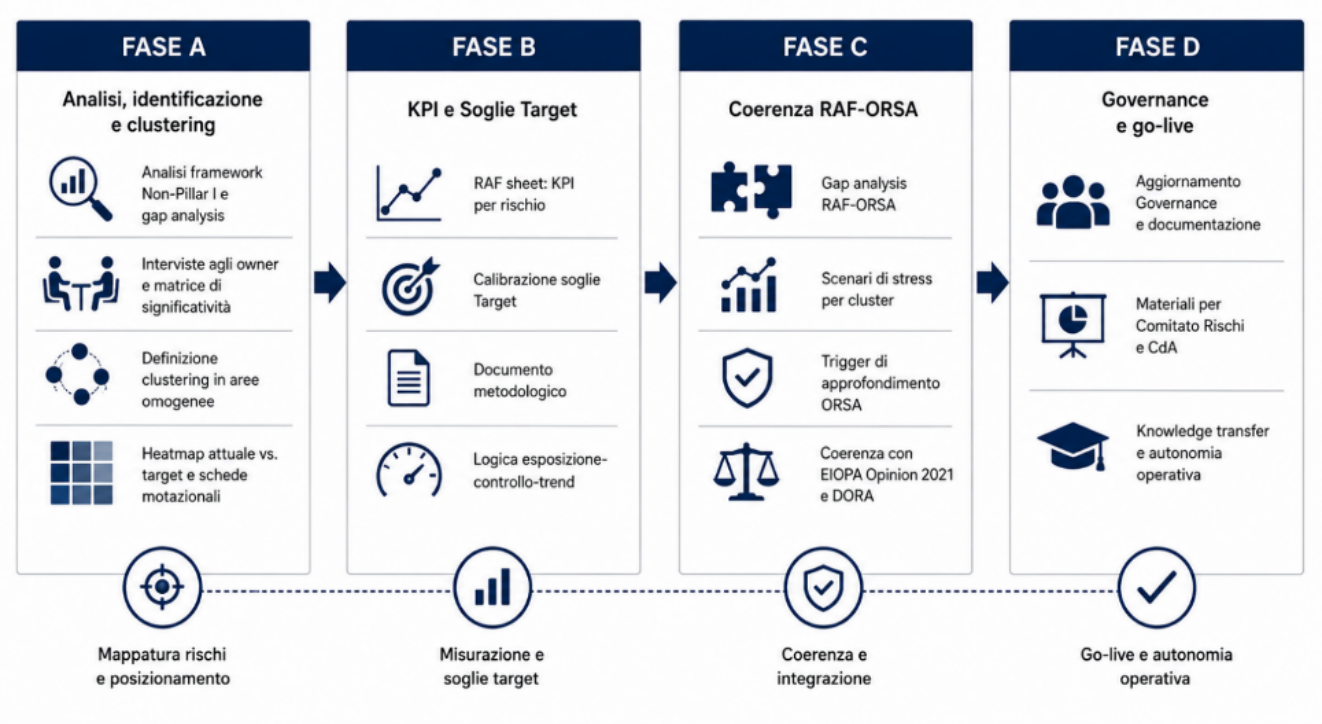
• Per ogni soglia Target: deve essere tracciata la fonte di calibrazione e la logica di determinazione.

• Per ogni KPI: formalizzare formula di calcolo, fonte del dato, periodicità di rilevazione e azioni gestionali previste.

Il sistema di gestione dei rischi è adeguato non quando esiste, ma quando funziona e quando se ne può dimostrare il funzionamento. (EIOPA-BoS-14/253, Reg. IVASS n. 38/2011, Reg. IVASS n. 43/2018)

Come implementare un framework RAF Non-Pillar I

La nostra esperienza su questi temi ci ha portato a strutturare un percorso progettuale articolato in quattro fasi, applicabile con il principio di proporzionalità a compagnie di diversa dimensione e complessità:



Le aspettative regolamentari sui rischi Non-Pillar I stanno cambiando rapidamente e richiedono oggi un approccio più strutturato, documentato e integrato nei processi decisionali aziendali. Cyber risk, intelligenza artificiale, liquidità, ESG e rischio di condotta non rappresentano più temi "collaterali", ma aree di presidio strategico sempre più osservate dalle Autorità di Vigilanza.

In questo contesto, il valore di un RAF efficace non risiede solo nella presenza di KPI o soglie Target, ma nella capacità di dimostrare coerenza metodologica, tracciabilità documentale e integrazione concreta con ORSA, governance e processi di business.

La robustezza del framework documentale diventa quindi il vero

elemento distintivo: motivazioni analitiche, criteri di calibrazione, ownership e azioni gestionali devono essere chiari, formalizzati e sostenibili nel tempo.

Un framework Non-Pillar I maturo consente non solo di rafforzare la compliance normativa, ma anche di anticipare i rischi emergenti e supportare decisioni più consapevoli, forward-looking e data-driven.

FAQ – RAF assicurazioni e rischi Non-Pillar I

Cosa sono i rischi Non-Pillar I nelle assicurazioni?

I rischi Non-Pillar I sono rischi che normalmente non generano direttamente un requisito patrimoniale SCR nella Formula Standard Solvency II, ma che possono avere impatti significativi sulla stabilità della compagnia assicurativa. Tra questi rientrano rischio cyber, ESG, liquidità, condotta, reputazionale e rischio Intelligenza Artificiale.

Il rischio di liquidità è un rischio Pillar I o Non-Pillar I?

Dal punto di vista tecnico, il rischio di liquidità è classificato come rischio Non-Pillar I perché non esiste uno specifico requisito SCR nella Formula Standard Solvency II. Tuttavia, nella pratica regolamentare viene considerato un rischio strategico di primo livello nel RAF e nell'ORSA, soprattutto dopo la Solvency II Review.

Quali normative impattano i rischi Non-Pillar I nelle compagnie assicurative?

Le principali normative europee che rafforzano il presidio dei

rischi Non-Pillar I sono:

- DORA (Digital Operational Resilience Act);
- Solvency II Review;
- AI Act;
- IDD;
- POG;
- linee guida EIOPA e regolamenti IVASS.

Perché i rischi ESG devono entrare nel RAF assicurativo?

Le nuove disposizioni europee richiedono alle compagnie assicurative di integrare i rischi ESG nei processi ORSA, nella governance e nelle valutazioni prospettiche della solvibilità. I rischi climatici e di sostenibilità non sono più considerati soltanto reputazionali, ma elementi strutturali del framework di risk management.

Come vengono classificati i rischi Non-Pillar I nel RAF?

La classificazione avviene tramite un processo strutturato di:

- mappatura dei rischi;
- definizione dei cluster;
- assessment di probabilità e impatto;
- interviste agli owner;
- costruzione di heatmap;
- definizione di KPI, KRI e soglie Target.

L’obiettivo è dimostrare metodologicamente la significatività o non significatività del rischio.

Qual è il collegamento tra RAF e ORSA?

Tutti i rischi Non-Pillar I considerati significativi devono essere valutati prospetticamente nell'ORSA. Il RAF rappresenta infatti uno dei principali input del processo ORSA, soprattutto per stress test, scenario analysis e valutazioni forward-looking della solvibilità.

Alessio Buonfrate, *Partner di CA Insurance*