POSITION PAPER

N° 48

Governance e Risk Culture

AIFIRM
Associazione Italiana Financial Industry Risk Managers

Giugno 2025

AIFIRM RINGRAZIA

Il Coordinatore Scientifico della Commissione

- **Rosa Cocozza** | Università di Napoli Federico II

Il Coordinatore AIFIRM

- **Fernando Metelli** | Presidente Onorario AIFIRM

Il comitato guida

- **Rosaria Cerrone** | Università di Salerno
- **Rosa Cocozza** | Università di Napoli Federico II
- **Elisa Corsi** | Volksbank
- **Adele Grassi** | Vice Presidente APB, Associazione Italiana Pianificazione e Controllo di Gestione nelle banche, società finanziarie ed assicurazioni
- **Corrado Meglio** | Vice Presidente AIFIRM
- **Evandro Menna** | ICCREA Banca
- **Fernando Metelli** | Presidente Onorario AIFIRM
- **Enrica Rimoldi** | Senior Advisor e Amministratore indipendente
- **Paola Schwizer** | Università di Parma

Il gruppo di lavoro

- **Nicola Andreis** | illimity Bank
- **Sabrina Bonomi** | CredemBanca
- **Fabio Bressan** | MedioBanca
- **Elena Bruno** | Università di Pisa
- **Giovanni Camerota** | Revise Regulatory Advisors
- **Rosanna Cappiello** | Bip
- **Luigi de Luca** | AIFIRM
- **Emanuele Diquattro** | Banca Agricola Popolare di Ragusa
- **Greta Benedetta Ferilli** | Università del Salento
- **Paola Ferretti** | Università di Pisa
- **Marisa Friaglia** | Banca Sella
- **Serena Gallo** | Università di Napoli Federico II
- **Francesca Geusa** | Università del Salento
- **Saverio Giorgio** | Università degli Studi "G. d'Annunzio" Chieti – Pescara | Luigi Luzzatti S.C.p.A.
- **Elisa Grillo** | AMCO
- **Valentina Lagasio** | Università di Roma “La Sapienza”
- **Giovanna Marino** | Banca Sella
- **Marianna Medici** | Banca Generali
- **Pina Murè** | Università di Roma “La Sapienza”
- **Miriam Ota** | illycaffè

- **Egidio Palmieri** | Università di Udine
- **Marco Pavoni** | Cassa Depositi e Prestiti
- **Federico Peretti** | Allianz Bank Financial Advisors
- **Antonio Picone** | Bip
- **Gerardo Rescigno** | Mediocredito Centrale
- **Annalisa Richetto** | Intesa SanPaolo
- **Claudio Ruffini** | Augeos
- **Floricel Rugiero** | Enel
- **Francescopaolo Russo** | Protiviti
- **Manuela Sabbatini** | Cassa Depositi e Prestiti
- **Valeria Stefanelli** | Università del Salento
- **Luca Teodonno** | Mediocredito Centrale
- **Gustavo Troisi** | Consulenze Integrate AFC, Risk, Sustainability @Development
- **Enkela Verjoni** | Banco BPM

SUPERVISIONE A CURA DI:

- **Corrado Meglio** | Vice Presidente AIFIRM

IL COORDINAMENTO EY

- **Andrea Lapomarda** | Partner
- **Antonio Altieri Pignalosa** | Partner
- **Simone Smeraldi** | Senior Manager
- **Bence Baranyai** | Manager

ISBN 979-12-80245-31-1

DOI 10.47473/2016ppa00048

INDICE

EXECUTIVE SUMMARY (ENGLISH)

The Position Paper *Governance and Risk Culture* offers a holistic view of "risk culture & culture risk", blending regulatory, organizational and operational perspectives. It begins by distinguishing risk culture – the shared values, norms and behaviors that drive conscious risk-taking – from culture risk, i.e. the risk that arises when declared principles diverge from actual practices. Without a robust risk culture, culture risk becomes a potentially lethal threat to an institution's sustainability.

Regulatory landscape. The paper traces the European evolution from BCBS/FSB standards to the ECB Draft Guide on Governance & Risk Culture (July 2024). Supervisors now expect risk culture to be measurable, verifiable and proportionate to size, complexity and business model. Four ECB pillars are emphasized – tone from the top, effective communication & challenge, accountability and incentives – and the paper adds "red-flag" indicators for early detection of weaknesses.

Governance. The Board, supported by its committees and the control functions, must spearhead risk-culture dissemination, ensuring independent judgement, adequate collective composition and expertise on ESG/ICT topics. The Risk Management function plays a transversal role: defining the Risk Appetite Statement (RAS) and managing the KPI/KRI framework. Compliance and Internal Audit complete the three-lines-of-defense model, providing, respectively, ex-ante conformity and ex-post independent assurance.

Operational framework. Detailed processes are provided for risk identification, measurement, monitoring and reporting, underlining the need for:

- integrated and reliable data-governance systems;
- broad, modular training programs to raise risk awareness;
- clear escalation mechanisms backed by effective whistleblowing channels.

The paper proposes a proportionality matrix aligning governance structures, control intensity and cultural coverage with four banking profiles (LSI, complex domestic, international group, fintech-driven).

Strategic implications. Ultimately, the document presents risk culture not as a mere compliance requirement but as a competitive advantage: by embedding sound risk culture into performance management, institutions can balance growth, innovation and long-term resilience, safeguarding the trust of clients, investors and supervisors.

EXECUTIVE SUMMARY (ITALIANO)

Il Position Paper *Governance e Risk Culture* di AIFIRM affronta in modo organico il tema "*risk culture & culture risk*", delineando una visione olistica che integra prospettive regolamentari, organizzative e operative. Il documento esordisce chiarendo la differenza fra *risk culture* – l'insieme di valori, norme e comportamenti che orientano l'assunzione consapevole dei rischi – e *culture risk*, ossia il rischio generato da un divario fra i principi dichiarati e le pratiche effettive dell'organizzazione. Senza una solida cultura del rischio, il *culture risk* diventa un fattore potenzialmente letale per la sostenibilità dell'intermediario.

Sul piano normativo-regolamentare viene ricostruita l'evoluzione europea: dalle Linee guida BCBS/FSB fino *alla ECB Draft Guide on Governance & Risk Culture* (luglio 2024). La supervisione si attende oggi che la cultura del rischio sia misurabile, verificabile e proporzionata a dimensione, complessità e modello di *business*. Particolare enfasi è posta sui quattro "*pillar*" individuati dalla ECB – *tone from the top*, comunicazione & *challenge*, *accountability* e incentivi – cui l'intervento del Regolatore affianca la declinazione di indicatori di "*red flag*" utili al monitoraggio.

Ampio spazio è dedicato alla *governance*. Il *Board*, supportato dai Comitati e dalle Funzioni di Controllo, deve guidare la diffusione della cultura del rischio, garantendo indipendenza di giudizio, adeguata composizione collettiva e presidio di competenze ESG/ICT. La funzione *Risk Management* assume un ruolo trasversale: dalla definizione del *Risk Appetite Statement* al presidio dei framework di KPI/KRI. *Compliance* e *Internal Audit* completano le "tre linee di difesa", assicurando rispettivamente conformità *ex-ante* e *assurance* indipendente *ex-post*.

Sul versante operativo il *paper* dettaglia processi di identificazione, misurazione, monitoraggio e reporting, evidenziando la necessità di:

- sistemi dati integrati e affidabili (*data-governance*);
- formazione estesa e modulare mirata a elevare la *risk awareness*;
- meccanismi di *escalation* chiari, supportati da canali di *whistleblowing*.

Viene inoltre proposta una matrice di proporzionalità che calibra struttura di governance, intensità dei controlli e copertura culturale rispetto a quattro profili di banca (LSI, domestica complessa, gruppo internazionale, *fintech-driven*).

In sintesi, il documento individua nella cultura del rischio non un mero obbligo regolamentare bensì un vantaggio competitivo: solo integrando *risk culture* e *performance management* un intermediario può coniugare crescita, innovazione e resilienza di lungo periodo, preservando fiducia di clienti, investitori e vigilanza.

1 OBIETTIVI DEL DOCUMENTO

Rosa Cocozza, Fernando Metelli

1.1 Culture Risk e Risk Culture

Le istituzioni finanziarie sono da tempo chiamate a gestire i rischi quale attività intrinseca al loro ruolo nei mercati finanziari. La gestione del rischio, pertanto, costituisce una componente essenziale dell'intermediazione finanziaria (Allen e Santomero, 1997). Con l'aumentare della complessità dei mercati finanziari, le richieste poste alla funzione di gestione del rischio continuano a crescere, rendendo necessarie metodologie e tecniche sempre più sofisticate. Di conseguenza, il *risk management* si caratterizza per un'elevata intensità tecnica, richiedendo al *Chief Risk Officer* (CRO) una profonda padronanza di metodi quantitativi, analisi dei dati e altri ambiti tecnici, spesso radicati nelle scienze esatte. Il ruolo del CRO è divenuto cruciale non solo nel monitoraggio dei rischi esistenti, ma anche nell'anticipazione e nella mitigazione di minacce emergenti. Tale posizione strategica impone una combinazione di competenze tecniche, capacità di *leadership* lungimirante e attitudine a collaborare a tutti i livelli organizzativi, al fine di garantire la resilienza dell'istituzione e il rispetto di *standard* normativi in continua evoluzione.

Una delle principali implicazioni di questa evoluzione risiede nella necessità di integrare la cultura del controllo con una solida cultura del rischio. Sebbene sia ampiamente riconosciuto che rischi e controlli rappresentino due facce della stessa medaglia (Cocozza, 2024a), porre l'accento sulla *"cultura del controllo"* implica interventi di tipo correttivo (affrontando i rischi dopo che si siano manifestati), mentre enfatizzare la *"cultura del rischio"* sottolinea l'importanza e la centralità delle attività preventive (mitigando i rischi prima che insorgano). È superfluo ribadire che entrambe sono indispensabili; tuttavia, la seconda può rivelarsi più efficace ed economicamente vantaggiosa.

Di conseguenza, nelle moderne istituzioni finanziarie, la sola competenza tecnica non è più sufficiente per i responsabili del rischio. La loro frequente partecipazione ai consessi decisionali strategici richiede lo sviluppo di ulteriori capacità, quali solide abilità comunicative, l'abilità di interagire con gli *stakeholder* e una comprensione approfondita delle dinamiche organizzative. Tali competenze consentono ai *risk manager* di contribuire efficacemente ai dibattiti strategici più ampi, assicurando al contempo che le considerazioni relative al rischio siano integrate nei processi decisionali, con l'obiettivo ultimo di garantire una buona *governance*, fondamentale per la stabilità e la sicurezza delle istituzioni finanziarie, in linea con le finalità dei supervisori.

La Guida sulla *Governance* e la Cultura del Rischio, pubblicata nel luglio 2024 dalla *European Central Bank* (ECB, 2024a), sottolinea come eventuali carenze nella cultura del rischio possano costituire segnali precoci di instabilità finanziaria di una istituzione, rendendo una solida *governance* imprescindibile elemento per la resilienza strategica e l'operatività sostenibile. Guardando al futuro, il ruolo del *risk management* sembra destinato ad assumere sempre più una posizione di rilievo nella dinamica aziendale. Non più inteso come un mero centro di costo, si configura invece quale elemento cruciale della catena di creazione del valore. La cultura, nella sua accezione più ampia, comprende l'insieme di valori, credenze, norme e pratiche condivise da un gruppo di individui. Essa funge da cornice di riferimento che orienta il comportamento, il processo decisionale e le interazioni all'interno di un sistema sociale. La cultura si trasmette di generazione in generazione attraverso la socializzazione e pratiche istituzionalizzate, evolvendo nel tempo in risposta alle trasformazioni dell'ambiente, della storia e della società. Da un punto di vista antropologico, la cultura ha sia una dimensione materiale sia una dimensione simbolica, influenzando tanto le espressioni tangibili (manufatti, sistemi) quanto gli aspetti intangibili (ideologie, significati condivisi). In tal modo, essa conferisce un'identità coesa ai gruppi, orientandone il comportamento e garantendo continuità nell'ambito della diversità.

Parallelamente, la cultura aziendale designa il particolare insieme di valori, norme e pratiche condivise che caratterizza un'organizzazione. Essa rappresenta al contempo un prodotto dell'identità organizzativa e un fattore che la alimenta, determinando le modalità di interazione sia tra i membri interni sia con gli attori esterni. La cultura aziendale influisce sui processi decisionali, sulla comunicazione e sulle priorità da perseguire, allineando i comportamenti individuali agli obiettivi dell'organizzazione. Tale cultura emerge dalle filosofie di *leadership*, dalle strategie operative e dal contesto storico-sociale in cui l'organizzazione si inserisce. Le dimensioni fondamentali della cultura aziendale includono valori e regole, aspettative comportamentali, stili di *leadership* e di gestione, nonché simboli e rituali.

La cultura aziendale esercita un'influenza determinante sulle prestazioni organizzative, incidendo sulla capacità di innovare, sul coinvolgimento dei dipendenti, sull'adattabilità ai cambiamenti e sui comportamenti etici. Le culture aziendali solide favoriscono l'allineamento tra gli obiettivi dell'organizzazione e la motivazione individuale; al contrario, culture frammentate possono generare conflitti e inefficienze. In sintesi, come suggerisce la celebre massima, attribuita (sebbene in maniera non confermata) al consulente manageriale Peter Drucker, *"la cultura divora la strategia a colazione"*, a sottolineare che una cultura forte e capace di responsabilizzare i suoi membri costituisce un presupposto imprescindibile per il successo.

La cultura del rischio può essere considerata un sottoinsieme della cultura aziendale. Essa riguarda in modo specifico le norme, gli atteggiamenti e i comportamenti inerenti

la consapevolezza, la valutazione e la gestione del rischio all'interno di un'organizzazione. Include il modo in cui i rischi vengono percepiti, comunicati e affrontati a tutti i livelli, influenzando così la capacità dell'organizzazione di individuare, mitigare e rispondere alle incertezze. Le caratteristiche della cultura del rischio comprendono la consapevolezza del rischio, le norme comportamentali, le modalità di comunicazione, nonché la responsabilità e i meccanismi incentivanti.

Considerato che l'attività bancaria e, più in generale, l'intermediazione finanziaria ruotano intrinsecamente attorno al rischio – *il quale, unitamente alle risorse finanziarie raccolte, costituisce l'input fondamentale di tali operazioni* – la presenza di una solida cultura del rischio non è soltanto auspicabile, ma rappresenta un elemento imprescindibile, attivamente ricercato dalle Autorità di Vigilanza (AdV), nel perseguimento della sicurezza e della stabilità degli istituti di credito. Tale esigenza si fa ancor più pressante nell'attuale contesto, in cui gli intermediari si trovano a fronteggiare sfide di natura economica, competitiva e geopolitica, parallelamente alla gestione di rischi connessi ai cambiamenti climatici, alla sostenibilità ambientale e all'innovazione tecnologica. In effetti, secondo il *Basel Committee on Banking Supervision* (BCBS, 2015), richiamando il *Financial Stability Board* (FSB, 2014), la cultura del rischio è definita come insieme che raccoglie «le norme, gli atteggiamenti e i comportamenti di una banca in relazione alla consapevolezza, all'assunzione e alla gestione del rischio, e i controlli che orientano le decisioni in materia di rischio. La cultura del rischio incide sulle decisioni del management e dei dipendenti nelle attività quotidiane e influisce sui rischi che essi si assumono».

Una solida cultura del rischio allinea i comportamenti relativi all'assunzione del rischio con gli obiettivi dell'organizzazione e con le aspettative di vigilanza, favorendo processi decisionali prudenti e rafforzando la resilienza. Viceversa, una cultura del rischio debole può determinare incentivi non allineati, carenza di controlli e una maggiore probabilità di *defaillance*, sia a livello operativo sia strategico. L'impegno del vertice aziendale, la trasparenza e la formazione continua risultano pertanto fondamentali per integrare efficacemente la cultura del rischio all'interno della più ampia cultura organizzativa. La cultura del rischio comprende la mentalità collettiva, le norme e i comportamenti che influenzano il modo in cui il rischio viene percepito, valutato e gestito nell'ambito di un'organizzazione. Una cultura del rischio solida allinea i comportamenti di assunzione del rischio agli obiettivi organizzativi e alle aspettative di vigilanza, promuovendo decisioni etiche e una maggiore capacità di adattamento.

Il rischio di cultura si manifesta quando si registra una discrepanza tra i valori dichiarati di un'organizzazione e le pratiche e i comportamenti effettivi dei suoi membri. Tale divario può sfociare in carenze etiche, inefficienze operative e danni reputazionali, mettendo in pericolo la stabilità dell'istituto. Coerentemente, per rischio di cultura si possono intendere le possibili conseguenze negative derivanti da disallineamenti tra i

valori, le norme e i principi formalmente enunciati dall'organizzazione e gli atteggiamenti, i comportamenti e le prassi effettivamente messi in atto. In questo ambito rientrano i rischi connessi a lacune nella promozione di una cultura coesa ed etica, capace di sostenere gli obiettivi strategici, la conformità normativa e la sostenibilità di lungo periodo.

Nelle istituzioni finanziarie, il rischio di cultura può declinarsi in diverse forme, tra cui comportamenti non etici, inefficienze operative, resistenza al cambiamento o insufficiente consapevolezza del rischio, ossia un'integrazione carente dei principi di gestione del rischio nella cultura organizzativa, con conseguenti decisioni inadeguate o eccessiva propensione al rischio.

Le AdV conferiscono sempre maggiore rilievo alla gestione del rischio di cultura quale componente essenziale della *governance* degli intermediari finanziari, riconoscendone il ruolo cruciale nel mitigare rischi operativi, finanziari e reputazionali di ampia portata. Affrontare il rischio di cultura richiede un impegno costante della *leadership*, una chiara comunicazione dei valori e l'adozione di meccanismi atti a monitorare e rafforzare i comportamenti desiderati a tutti i livelli dell'organizzazione. In questo contesto, emergono tre pilastri fondamentali per la gestione del rischio di cultura, posti alla base del meccanismo illustrato:

1. il ruolo della *leadership*, che deve manifestare una profonda consapevolezza del rischio e un impegno solido, comunicando le aspettative in modo chiaro e coerente, al fine di promuovere una cultura improntata alla consapevolezza del rischio;
2. l'efficacia della comunicazione a tutti i livelli dell'organizzazione, sia in senso discendente (*top-down*) sia ascendente (*bottom-up*);
3. il ruolo determinante della funzione di organizzazione, oltre alle tradizionali Funzioni Aziendali di Controllo *(Risk Management, Compliance e Internal Audit;* di seguito FAC).

Relativamente al primo pilastro, i principali attori coinvolti sono il Consiglio di Amministrazione (CdA), i comitati a livello consiliare e, ove previsto, gli amministratori o i consiglieri delegati. Con riguardo al secondo pilastro, occorre dare rilievo non soltanto al *"parlare proattivo"*, ma anche all'*"ascolto proattivo"* (Cocozza, 2024b). Infine, il terzo pilastro richiede la *"piena maturità"* della funzione di organizzazione, che opera quale principale presidio di *accountability*, in sinergia con la funzione Risorse Umane (HR) per gli aspetti legati agli incentivi e ai programmi di *induction* e formazione.

Pertanto, il palindromo *"risk culture & culture risk"* non costituisce un mero gioco di parole. La cultura del rischio si riferisce ai valori, agli atteggiamenti e alle pratiche condivise in merito alla consapevolezza e alla gestione del rischio all'interno di un'istituzione. Il rischio di cultura, invece, scaturisce da disallineamenti tra i valori

dichiarati dall'organizzazione e i comportamenti effettivi dei suoi membri. L'assenza di una solida cultura del rischio genera il rischio di cultura, che può risultare dannoso, se non addirittura letale, per la stabilità e la sostenibilità di una banca.

La menzionata assenza di una solida cultura del rischio diviene un fattore di rischio che incide sulla *performance* aziendale in maniera complessa e multiforme, con effetti spesso di difficile misurazione. Promuovere una solida cultura del rischio rappresenta quindi una misura preventiva di ampio respiro nei confronti del rischio di cultura e costituisce, in quanto tale, una componente essenziale del processo di gestione di quest'ultimo. Al centro di tale impostazione preventiva si colloca il concetto di "*tone from the top*", che comprende il clima etico, i valori culturali e gli *standard* comportamentali stabiliti dal vertice dell'organizzazione. Quest'ultimo include il CdA, il *top management* e le altre figure apicali. Il "*tone from the top*" rispecchia gli atteggiamenti, le decisioni e le azioni delle alte cariche, evidenziandone l'incrollabile impegno a favore dei valori aziendali, di una *governance* efficace e di adeguate pratiche di gestione del rischio.

In coerenza con gli elementi fondamentali riportati, si possono individuare immediatamente tre segnali di allarme: la carenza di indipendenza, che segnala un impegno insufficiente da parte della *leadership*; l'assenza di adeguati meccanismi di *whistleblowing*, indicativa di una comunicazione inefficace; e la debole *accountability*, che riflette carenze nelle linee organizzative. In effetti, tali principali campanelli d'allarme consentono di identificare prontamente carenze nella cultura del rischio. Affrontando tali problematiche, le istituzioni possono creare strutture resilienti, in grado di adattarsi ai rischi in evoluzione.

Secondo la ECB (2024a) gli elementi costitutivi della cultura del rischio comprendono, oltre al citato "*tone from the top*", la comunicazione efficace, il confronto e la diversità, nonché meccanismi incentivanti e *accountability* in ambito di rischi. Le cause profonde del rischio di cultura sono individuate nei cosiddetti *"cultural drivers"*. L'approccio della ECB individua due principali fattori di rischio (*risk driver*) per il rischio di cultura: "*governance*" e *"cultura e comportamento"*. Coerentemente, la ECB (2024a) elenca i "*governance red flag*" e i "*behavioural and cultural red flag*". Se ne deduce che il verificarsi di tali segnali di allarme, classificati come *"non esaustivi"*, costituisce riprova della inadeguata cultura del rischio e accresce il rischio di cultura. In sintesi, la presenza di campanelli d'allarme relativi alla *governance* e di quelli relativi agli aspetti comportamentali e culturali segnala la presenza di una inadeguata cultura del rischio, causa primigenia dell'insorgenza del rischio di cultura.

La distinzione tra fattori di rischio riconducibili alla *governance* e fattori di rischio di natura comportamentale e culturale consente di riflettere in modo più approfondito sui profili culturali specifici di ogni istituto finanziario.

Le realtà di minori dimensioni potrebbero risultare più vulnerabili al rischio di cultura a causa delle peculiarità delle proprie strutture di *governance* e dell'impatto di stratificazioni di postura mentale e comportamentali. Di conseguenza, si potrebbe verificare un'inversione del principio di proporzionalità, che suggerisce un'attenzione e una cautela maggiori, in particolare per le *Less Significant Institution* (LSI). Analogamente, l'adozione di un determinato modello di *business* o la focalizzazione su specifiche aree operative possono rappresentare ulteriori elementi di profilazione individuale, sia dal punto di vista dei presidi di controllo, sia in termini di assetti organizzativi. Allo stesso modo, la localizzazione puntuale delle attività, la rilevanza di operazioni transfrontaliere e la prevalenza di operazioni creditizie caratterizzate da connotati peculiari possono costituire fattori significativi per la personalizzazione dei profili di rischio di cultura.

Inoltre, la capacità di comprendere pienamente le carenze nella cultura del rischio può essere condizionata dall'importanza che l'organizzazione e il CdA attribuiscono agli aspetti di *"rischio e controllo"* rispetto alle finalità commerciali.

Sebbene in ambito accademico si insista sull'uguale rilevanza di entrambi, nella prassi aziendale il riconoscimento di tale equivalenza incontra talvolta ostacoli. Tali resistenze possono derivare, tra l'altro, dalle diverse caratteristiche – *per profondità e natura* – dell'esperienza maturata nella gestione degli istituti finanziari, nonché dall'eterogeneità dei contesti culturali e generazionali delle risorse umane coinvolte.

1.2 L'importanza della governance

Una volta definito il rischio di cultura, risulta opportuno – *seguendo il processo logico tipicamente adottato per le altre categorie di rischio* – identificare la funzione o le funzioni aziendali responsabili della sua mitigazione e per la sensibilizzazione dell'organizzazione.

Per quanto riguarda la mitigazione, la responsabilità ricade senz'altro – *seppur non in via esclusiva* – nell'ambito del Sistema dei Controlli Interni. Il Sistema dei Controlli Interni rappresenta un pilastro fondamentale della *governance* negli istituti bancari, poiché assicura la conformità, gestisce i rischi e tutela l'integrità organizzativa. Oltre a tali compiti operativi, il Sistema dei Controlli Interni svolge un ruolo cruciale nel favorire una solida cultura del rischio e nell'affrontare il rischio di cultura. Di fronte alle crescenti sfide – *tra cui vigilanza regolamentare, innovazioni tecnologiche e questioni di sostenibilità* – il Sistema dei Controlli Interni deve evolvere per rispondere a esigenze sempre più complesse, comprese le dimensioni di carattere comportamentale. In tale prospettiva, il Sistema dei Controlli Interni valuta i rischi di cultura mediante *audit*, analisi dei comportamenti e meccanismi di *whistleblowing*. Protocolli chiari di

escalation, efficaci politiche sui conflitti di interesse e strumenti di segnalazione attiva consentono di individuare e correggere in modo proattivo eventuali disallineamenti culturali. L'allineamento del rischio di cultura alla *governance* impone che esso sia integrato nei quadri di governo societario, ivi incluso il *Risk Appetite Framework* (RAF), in modo da garantirne una gestione sistematica. Valutazioni periodiche delle pratiche culturali e la revisione delle "*lesson learned*" dagli incidenti rafforzano la capacità dell'istituzione di mitigare efficacemente il rischio di cultura.

La gestione di tali aspetti richiede un approccio omnicomprensivo, in cui le FAC assolvono ruoli distinti ma interconnessi.

La Funzione di *Compliance* garantisce l'osservanza dei requisiti normativi, degli *standard* etici e delle politiche interne. Attraverso la valutazione dei codici di condotta, la formazione del personale e il monitoraggio dei comportamenti, essa orienta i fondamenti etici dell'organizzazione, segnalando e correggendo tempestivamente eventuali disallineamenti che generano rischio di cultura, così da favorire un contesto in cui i dipendenti riconoscano l'importanza delle pratiche orientate al rischio.

La Funzione di *Risk Management*, invece, individua, valuta, monitora e mitiga i rischi che possono influire sugli obiettivi strategici. Oltre alle tradizionali categorie di rischio, essa integra il rischio di cultura nel RAF e nelle strutture di *governance* più ampie, promuovendo una consapevolezza del rischio di natura proattiva e consolidando l'*accountability*.

La Funzione di *Internal Audit*, dal canto suo, offre un *assurance* indipendente sull'efficacia della *governance*, della gestione del rischio e dei sistemi di controllo dell'organizzazione. Esamina il grado di effettivo radicamento della cultura del rischio all'interno dell'istituzione, evidenziando lacune nel suo allineamento. Inoltre, valuta l'efficacia delle misure adottate per mitigare il rischio di cultura, favorendo così il miglioramento continuo e la dovuta responsabilizzazione.

La tempistica con cui operano le FAC è strategicamente coordinata con le diverse fasi di rischio e controllo in ambito organizzativo. Tali fasi, distinte in *ex-ante* (preventiva), *real-time* (in tempo reale) ed *ex-post* (a posteriori), delineano ruoli e livelli di coinvolgimento specifici per ciascuna funzione.

Nella fase preventiva, l'obiettivo è anticipare e ridurre la probabilità di eventi avversi. La Funzione di *Compliance* assicura l'adesione a requisiti normativi, politiche interne e *standard* etici predisposti per un'azione preventiva. La Funzione di *Risk Management*, parallelamente, individua i rischi emergenti, ne valuta gli impatti potenziali e definisce i limiti di rischio in linea con il RAF dell'istituzione. La Funzione di *Internal Audit*, per sua natura, interviene in misura minima in tale stadio, essendo il suo mandato essenzialmente *ex-post*.

Per quanto attiene alla fase in tempo reale, si pone l'accento sul monitoraggio e sulla gestione attiva dei rischi a mano a mano che si presentano. La Funzione di *Risk Management* assume un ruolo di primo piano, monitorando le esposizioni e intervenendo con eventuali aggiustamenti in tempo reale. La Funzione di *Compliance* supporta queste attività, verificando la costante osservanza dei requisiti normativi e organizzativi in un contesto operativo dinamico. La Funzione di *Internal Audit* fornisce un contributo moderato, offrendo *feedback* immediati sull'efficacia dei controlli e intervenendo quando necessario.

Nella fase *ex-post*, l'attenzione si concentra sull'indagine e il miglioramento dei processi e dei controlli a valle del verificarsi di un evento di rischio o di una falla nei controlli. La Funzione di *Internal Audit* assume il ruolo principale, conducendo analisi approfondite per individuare le cause profonde, raccomandando misure correttive e promuovendo iniziative a favore della resilienza organizzativa. La Funzione di *Risk Management* valuta le implicazioni dell'accaduto sull'assetto complessivo di gestione del rischio, adeguandone le strategie. Nel frattempo, la Funzione di *Compliance* assicura che qualunque violazione normativa sia correttamente identificata, segnalata se del caso a chi di competenza e affrontata tramite azioni correttive.

Questa distribuzione temporale delle responsabilità evidenzia l'interdipendenza delle FAC, i cui contributi complementari mirano a un approccio coeso nella promozione della cultura del rischio e nella mitigazione del rischio di cultura. Operare in sinergia consente di armonizzare analisi, strategie e interventi, dando vita a un sistema unitario che rafforza la resilienza complessiva. La scansione temporale delle iniziative adottate dalle FAC sottolinea la necessità di una pianificazione strategica nell'individuazione e gestione dei rischi, fornendo al contempo una base solida per ulteriori approfondimenti accademici e innovazioni operative in materia di *governance* e *risk management*. Questo quadro unitario mette in luce la rilevanza di un approccio integrato e coerente, volto a consolidare la cultura del rischio e ad anticipare le vulnerabilità di natura culturale. In definitiva, l'ampiezza e l'intensità degli interventi attribuibili alle FAC dipendono dal livello di diffusione della cultura del rischio in seno all'organizzazione e, dunque, dalla consapevolezza maturata in materia di rischio di cultura.

Nel corso della fase di sviluppo, diviene prioritario promuovere la cultura del rischio. Il Sistema dei Controlli Interni rafforza il ruolo della *leadership* nel definire un'impronta etica, stimolando comportamenti orientati alla consapevolezza del rischio e al rispetto delle normative. Nella fase di fondazione, le Funzioni di *Compliance* e di *Risk Management* progettano programmi formativi completi, volti a fornire ai dipendenti una solida base sui principi di gestione del rischio e sulle aspettative culturali, contribuendo così alla formazione e al rafforzamento delle competenze. Nella fase di maturità, le FAC monitorano sistematicamente i comportamenti e gli atteggiamenti dei

dipendenti, fornendo valutazioni e suggerimenti per assicurare l'allineamento con i valori dell'organizzazione. Infine, una volta raggiunto un livello pervasivo di cultura del rischio, il Sistema dei Controlli Interni incorpora pienamente tale cultura nei modelli di *governance* e nei processi operativi, garantendo coerenza e *accountability* a tutti i livelli.

In questo contesto, l'area operativa di una banca – *che riunisce funzioni di natura operativa, tecnologia e servizi di back-office* – riveste un ruolo focale nell'implementare e sostenere una cultura del rischio solida. In quanto fulcro dell'operatività quotidiana, essa traduce gli obiettivi strategici dell'istituto in prassi concrete, riducendo al contempo il rischio di cultura. Le responsabilità dell'area operativa si estendono oltre l'operatività tradizionale e comprendono la promozione di *accountability*, la diffusione della trasparenza e l'allineamento delle prassi operative alla cultura del rischio dell'ente.

Il rafforzamento dell'*accountability* inizia con l'assegnazione chiara di ruoli e responsabilità al personale operativo, affinché ciascuno sia consapevole del proprio contributo alla gestione del rischio e all'allineamento culturale. Parallelamente, meccanismi strutturati di *escalation* consentono di individuare e risolvere prontamente eventuali incidenti di rischio, riducendone così l'impatto potenziale. Integrare la cultura del rischio nei processi operativi significa declinare le politiche organizzative e le linee strategiche in procedure concrete, promuovendo uniformità decisionale, rispetto degli *standard* etici e normativi, nonché un'intrinseca considerazione del rischio in ogni scelta operativa.

Sul fronte della comunicazione, l'area operativa si impegna a sviluppare canali trasparenti ed efficienti per lo scambio di informazioni, favorendo la circolazione di segnalazioni e dati critici relativi al rischio tra i vari livelli aziendali. Un simile contesto comunicativo facilita, da un lato, la collaborazione fra personale operativo e FAC e, dall'altro, incentiva il dialogo costruttivo e la condivisione di preoccupazioni e proposte di miglioramento. A questo scopo, la disponibilità di meccanismi di *whistleblowing* promuove un ambiente in cui i dipendenti si sentano liberi di segnalare in modo riservato eventuali comportamenti non etici o disallineamenti culturali.

Nell'ottica di promuovere prassi etiche, l'area operativa assicura che l'impegno della *leadership* verso una cultura del rischio solida trovi una traduzione pratica, agendo in termini di coerenza tra i valori dichiarati e le procedure aziendali. I processi operativi vengono dunque progettati per riflettere i principi fondamentali dell'istituto, allineando le finalità operative a *standard* etici e obiettivi strategici. In aggiunta, vengono predisposti strumenti e percorsi formativi per supportare i dipendenti nel prendere decisioni etiche, specie in situazioni complesse in cui occorre bilanciare rischi e opportunità.

Infine, l'area operativa risulta determinante nel garantire che gli incentivi siano coerenti con la cultura del rischio dell'organizzazione. Integrare il rispetto della cultura del rischio e la disciplina operativa negli elementi di valutazione delle prestazioni significa premiare chi agisce in linea con gli *standard* etici e di gestione del rischio condivisi. I meccanismi retributivi e i criteri di avanzamento professionale includono pertanto parametri di *risk awareness*, scoraggiando così la ricerca di vantaggi di breve termine a scapito della sostenibilità e della reputazione di lungo periodo. Ricompensare i comportamenti che esemplificano l'adesione alla cultura del rischio e ai valori etici dell'istituto rafforza ulteriormente il ruolo cardine di tali valori.

In virtù di queste responsabilità, l'area operativa non solo contribuisce all'implementazione della cultura del rischio, ma agisce anche come canale privilegiato per la diffusione di prassi etiche e orientate al rischio a tutti i livelli organizzativi. Così facendo, essa favorisce la costruzione di un ambiente coeso e resiliente, nel quale gli obiettivi di gestione del rischio e la cultura aziendale siano integrati con efficacia nella quotidianità operativa.

Pertanto, la cultura del rischio costituisce un *asset* strategico per garantire solidità e resilienza alle imprese bancarie. In un contesto di crescente complessità e competitività la cultura del rischio funge da collante tra gli obiettivi di *business* e i presìdi di salvaguardia della stabilità aziendale e del sistema finanziario.

Dalle prime sezioni del *paper*, dedicate alle definizioni di *governance* e cultura del rischio, emerge con chiarezza il ruolo cruciale delle strutture di governo societario nell'orientare i comportamenti organizzativi. Il concetto di *"tone from the top"* assume un valore particolarmente significativo, in quanto sintetizza l'importanza della *leadership* e della sua capacità di influenzare positivamente – *con coerenza, trasparenza e responsabilità* – i valori e le prassi operative di tutta la banca. La diffusione della cultura del rischio, infatti, non può prescindere da una guida dirigenziale in grado di promuoverla e rafforzarla a livello strategico, coinvolgendo gli organi di supervisione (CdA e Collegio Sindacale) e le diverse funzioni aziendali.

La evoluzione normativa e regolamentare evidenzia come le AdV, sia nazionali sia europee, stiano puntando in modo crescente sulla cultura del rischio come elemento chiave per assicurare la sicurezza e la stabilità del sistema bancario. I riferimenti alle principali normative e linee guida (CRD, CRR, EBA Guidelines, e via discorrendo) testimoniano la volontà di rendere misurabile e concretamente verificabile la presenza di una cultura del rischio matura all'interno delle banche. Ciò implica che i modelli di *governance* e il Sistema dei Controlli Interni si adattino a tali esigenze, prevedendo ruoli e responsabilità ben definiti e processi operativi di monitoraggio continuo.

Un approfondimento significativo viene proposto rispetto ai pilastri della cultura del rischio, che in questo *paper* sono declinati nelle quattro dimensioni – *tone from the top* e *leadership; effective communication*, *challenge*, *diversity; accountability; incentives* –

mettendo in luce come questi fattori, interagendo tra loro, possano dare vita a un ambiente culturale favorevole o ostacolare la costruzione di una piena consapevolezza del rischio. Se, da una parte, il Sistema dei Controlli Interni e l'organizzazione del governo dei rischi costituiscono la spina dorsale dei meccanismi di prevenzione e mitigazione, dall'altra, i comportamenti umani e le dinamiche relazionali ricoprono un ruolo altrettanto determinante: l'assenza di un'etica condivisa e di comunicazioni trasparenti rischia, infatti, di vanificare anche i più sofisticati meccanismi di controllo.

La sezione sui fattori di rischio rilevanti e le aree impattate fornisce una mappatura utile per individuare le potenziali criticità culturali, sia a livello di strutture organizzative sia nel rapporto con i flussi informativi e la gestione dei dati. Viene inoltre evidenziata la necessità di adeguare le pratiche di cultura del rischio ai principi di proporzionalità, tenendo conto della dimensione, della complessità e della vocazione internazionale delle singole banche. Questo approccio modulare e contestualizzato permette alle istituzioni di calibrare la strategia di *governance* e di *risk management* in modo coerente con la propria realtà operativa, evitando eccessivi oneri burocratici e, al contempo, garantendo *standard* minimi di qualità.

Nella parte dedicata ai ruoli e alle responsabilità organizzative, il *paper* sottolinea l'importanza di ogni attore del sistema di *governance* (CdA, Collegio Sindacale, FAC) nel promuovere la cultura del rischio. Ciò implica non solo la definizione di un quadro regolamentare e procedurale solido, ma anche la capacità di esercitare una "*leadership culturale"* che traduca la *vision* di lungo periodo in prassi operative e relazioni quotidiane. Viene così rimarcata la necessità di una costante interazione fra i diversi livelli dell'organizzazione, in cui le buone prassi e i campanelli d'allarme rappresentano due estremità dello stesso *continuum*: da un lato, esempi di comportamenti virtuosi; dall'altro, segnali di rischio culturale potenzialmente in grado di compromettere l'integrità e la reputazione dell'istituto.

Infine, la sezione operativa chiarisce come le diverse fasi del *risk management* – *dall'identificazione e misurazione, al monitoraggio, fino alla gestione e all'escalation* – non possano prescindere da una piena integrazione con la cultura del rischio. È in questo passaggio che la figura del CRO e le FAC, insieme all'area operativa, assumono un rilievo strategico. Formazione, comunicazione interna e sistemi di incentivazione rappresentano i tre cardini per stimolare i comportamenti desiderati, creare consapevolezza diffusa e favorire la nascita di una contezza del rischio che sappia coniugare prudenza e innovazione. Particolarmente rilevante risulta anche il tema della cultura del *data management*, a testimonianza di quanto la qualità e la fruibilità delle informazioni – *oltre alla loro sicurezza* – siano elementi irrinunciabili per un controllo consapevole dei rischi.

Nel complesso, quindi, il *position paper* fornisce un quadro strutturato su *governance* e cultura del rischio, mettendo in luce come la costruzione di una solida cultura

aziendale non sia soltanto una questione di aderenza formale ai requisiti normativi, ma un percorso di crescita organizzativa e relazionale che deve essere condiviso a tutti i livelli. La coerenza tra *vision* strategica, comportamenti quotidiani, metriche di valutazione e responsabilità individuale è la chiave di volta per garantire la sostenibilità dell'impresa bancaria nel medio-lungo termine. Solo in questo modo, infatti, la banca è in grado di affrontare con sicurezza le sfide di un mercato in rapida evoluzione, preservando la fiducia dei clienti, degli investitori e, più in generale, della collettività.

Per offrire un'applicazione concreta del quadro logico qui analizzato, appare utile proporre alcuni esempi pratici. Si presenta nella parte finale, senza pretese di esaustività, una selezione di processi attivabili per il governo del rischio di cultura. A seconda del contesto, tali processi mirano a creare un adeguato clima culturale, valutare la situazione attuale all'interno di ciascuna organizzazione, attivare meccanismi preventivi per ridurre l'esposizione al rischio di cultura e implementare i tradizionali processi di individuazione dei *Key Risk Indicator* (KRI) e del loro monitoraggio.