

**Dalla Cultura del rischio al Rischio di cultura.
Strumenti di Governance per Allineare
Comportamenti e Valori.**

di Rosa Coccozza e Fernando Metelli

IPE Working Paper

N. 27

July 15, 2025

ISSN 2284-1229

Dalla Cultura del rischio al Rischio di cultura. Strumenti di *Governance* per Allineare Comportamenti e Valori.

Di Rosa Coccozza¹ e Fernando Metelli²

Abstract

Il saggio esamina la distinzione concettuale e operativa tra “cultura del rischio” (risk culture), intesa come l’insieme di norme condivise e comportamenti che guidano negli intermediari finanziari un’assunzione di rischio responsabile, e “rischio di cultura” (culture risk), definito come la minaccia derivante dalla divergenza tra i valori istituzionali dichiarati e le prassi effettive.

L’analisi inquadra il culture risk quale vulnerabilità trasversale con ricadute di natura sia prudenziale sia reputazionale. Attraverso una prospettiva articolata che integra governance e logiche di controllo interno, il lavoro delinea un quadro organico per la mitigazione del culture risk. Vengono altresì proposti meccanismi operativi – quali indicatori chiave e protocolli di *escalation* – volti a radicare una risk culture resiliente all’interno delle strutture di governance. La Guida della European Central Bank (ECB, 2024) costituisce un passo significativo nell’evoluzione delle aspettative di vigilanza, segnando un chiaro spostamento verso l’istituzionalizzazione della cultura come fattore cruciale per la solidità prudenziale e l’integrità operativa.

In risposta a questo mutato orizzonte regolamentare, il presente lavoro offre una riflessione sistematica sui fondamenti concettuali, sulle strutture di governance e sugli strumenti operativi necessari per promuovere la risk culture e contenere il culture risk. Inquadrando la risk culture come ambito governabile e il culture risk come minaccia trasversale alla stabilità istituzionale, lo studio intende supportare la comunità accademica ed il mondo dei practitioner nella comprensione e nell’implementazione delle aspettative delineate dalla ECB,

¹ Professore Ordinario di Economia degli Intermediari Finanziari nell’Università degli Studi di Napoli Federico II.

² Presidente Onorario di AIFIRM, Associazione Italiana Financial Industry Risk Managers. Chief Risk Officer Alba Leasing S.p.A.

proponendo una prima ricognizione del set di strumenti analitici e operativi, radicati tanto nella teoria quanto nelle best practice, per tradurre gli obiettivi culturali in risultati di governance duraturi. Ne risulta un *framework* olistico che valorizza la cultura come elemento centrale della gestione strategica e del dialogo tra la Vigilanza e gli istituti finanziari.

Keywords: chief risk officer, corporate governance, corporate culture, tone-from-the-top, mentalità di gruppo, comunicazione, remunerazione, accountability, business ethics, banking, intermediari finanziari.

JEL Classification: G21, G23, G28, G41, M14.

Indice

1	Introduzione	5
2	Fondamenti concettuali e prospettive di inquadramento	7
2.1	Cultura del rischio e rischio di cultura: un gioco di specchi concettuali	7
2.2	La governance quale leva di radicamento culturale	9
3.	Governance e assetti infrastrutturali della cultura del rischio	10
3.1	Architetture di governance e flussi culturali nelle istituzioni finanziarie	11
3.2	Le quattro dimensioni della cultura del rischio	12
3.3	Driver del rischio di cultura	15
3.4	Il principio di proporzionalità nel governo del rischio di cultura	18
4	Il rischio di cultura: protagonisti, elementi e dinamiche.	20
4.1	Gli attori del governo del rischio di cultura	21
4.2	Gli strumenti di governo del rischio di cultura	23
4.3	Integrazione della cultura del rischio all'interno dei sistemi di risk management	25
5	Conclusioni	27
	Bibliografia	29

1. Introduzione

L'integrazione della cultura del rischio nel contesto regolamentare e di vigilanza europeo è avvenuta progressivamente nel corso delle ultime due decadi, sollecitata sia dalle crisi finanziarie sia dalla progressiva formalizzazione delle norme prudenziali. La crisi finanziaria globale del 2007–2009 ha rappresentato un punto di svolta, rivelando diffuse carenze nella gestione del rischio e portando al riconoscimento che le carenze nella cultura organizzativa potessero costituire minacce sistemiche alla stabilità finanziaria. In risposta, i Regolatori hanno elevato la cultura del rischio a tema centrale nelle rispettive agende regolamentari.

Il Financial Stability Board (FSB, 2014) ha sottolineato il ruolo delle strutture di *governance*, degli indicatori comportamentali e dell'allineamento culturale nel plasmare le decisioni sensibili al rischio. Il Comitato di Basilea sulla Supervisione Bancaria (BCBS, 2015) ha codificato l'aspettativa che le banche adottino *framework* di *governance* esplicitamente orientati alla valorizzazione di conoscenze e di competenze, inclusa la solidità culturale degli esponenti, della *C-Suite* e – a cascata – del personale. A livello europeo, tali sviluppi sono stati recepiti ed estesi dai Regolatori sovranazionali e nazionali introducendo obblighi vincolanti in tema di *governance* interna, composizione degli organi sociali, articolazione del *risk appetite* e integrazione delle considerazioni di rischio nel processo di pianificazione strategica. Le conseguenti trasposizioni richiamano *driver* culturali, *tone-from-the-top* e rendicontazione delle responsabilità comportamentali.

Partendo da questi snodi regolamentari, lo studio inquadra la cultura del rischio come un *asset* strategico, delineando i quattro pilastri fondamentali individuati dalla ECB (2024): *tone-from-the-top*; comunicazione efficace e *challenge*; *accountability*; incentivi allineati. Il lavoro analizza tali elementi in relazione ai modelli di *governance*, al comportamento organizzativo e alla necessità di un adattamento dedicato e proporzionato.

La cultura del rischio deve essere radicata a tutti i livelli – strategico, operativo e comportamentale – e supportata da strumenti di *governance* quali *Key Performance Indicator* (KPI) culturali, *Key Risk Indicator* (KRI), protocolli di *escalation*, sistemi di *reporting* interni e programmi formativi. Viene inoltre esaminato il ruolo centrale delle funzioni di controllo, in particolare del Chief Risk Officer (CRO), nel sostenere l'integrità culturale lungo i processi di *risk management*.

Riconoscendo la diversità dimensionale e della vocazione operativa delle istituzioni, si propone un approccio proporzionato ma rigoroso: le aspettative culturali devono essere adattate, non diluite. Il *culture risk* deve essere concepito come fenomeno dinamico e misurabile, con una solida *data governance* e strumenti diagnostici che ne consentano il continuo perfezionamento e l'interazione con la Vigilanza.

La classificazione del *culture risk* all'interno dell'architettura più ampia del *governance risk*, così come declinato dalla European Banking Authority (EBA) negli Orientamenti sulla gestione dei rischi ambientali, sociali e di *governance* (EBA, 2025), ne conferma ulteriormente la rilevanza regolamentare. Sebbene non sempre esplicitamente nominato, il *culture risk* si colloca concettualmente all'intersezione fra carenze di *leadership*, deficienze etiche e pratiche manageriali inadeguate. Tali lacune rappresentano minacce dirette alla solidità finanziaria e rientrano, pertanto, a pieno titolo nel perimetro di vigilanza del pilastro "G" della triade *Environmental, Social and Governance* (ESG).

In conclusione, il *culture risk* costituisce una vulnerabilità di fondo nei sistemi finanziari. La sua mitigazione richiede un'azione coordinata da parte degli organi di governo, del *management* e delle Autorità di Vigilanza. Le istituzioni che pongono la maturità culturale quale priorità strategica sono nelle migliori condizioni per conseguire una resilienza duratura e mantenere la fiducia di clienti, investitori e supervisori.

Il saggio articola un *framework* completo per la comprensione, la misurazione e la *governance* della *risk culture* e del *culture risk* nelle istituzioni finanziarie, distinguendo – ed è questa una novità – tra *risk culture*, vale a dire la "cultura del rischio" ossia le norme e i comportamenti condivisi che guidano decisioni consapevoli del rischio, e *culture risk*, cioè il "rischio di cultura" ossia la minaccia derivante da disallineamenti fra valori dichiarati e condotte effettive (Cocozza e Metelli, 2025).

La struttura del saggio è la seguente. La Sezione 2 definisce il fondamento concettuale, differenziando *risk culture* e *culture risk* ed esplicitando come la *corporate governance* operi da ancoraggio culturale. La Sezione 3 esamina il panorama regolamentare europeo in evoluzione, analizza modelli alternativi di *governance* e sviluppa il *framework* dei quattro pilastri della ECB (*tone-from-the-top*; comunicazione e *challenge*; *accountability*; incentivi), prima di individuare i principali *driver* organizzativi e comportamentali del *culture risk* e di discutere la logica della "proporzionalità inversa" per le *Less Significant Institutions* (LSI). La Sezione 4 traduce tali spunti in prassi, dettagliano i ruoli degli attori di *governance*, il *toolkit* dei KPI/KRI

culturali e l'integrazione delle considerazioni culturali nei processi di *risk management*, nei *framework* di *data governance* e nei protocolli di *escalation*. La Sezione 5 conclude con raccomandazioni di *policy* e un'agenda per un dialogo di sorveglianza continuo.

2. Fondamenti concettuali e prospettive di inquadramento

Il quadro teorico entro il quale si collocano i concetti di *risk culture* e *culture risk* ricomprende le radici dottrinali e il loro significato operativo per gli intermediari finanziari. È quindi opportuno indagare la dialettica tra “cultura del rischio e “rischio di cultura”. In tale ambito spicca il ruolo della *corporate governance* quale leva primaria di radicamento culturale, per poter offrire un apparato concettuale utile a comprendere le dinamiche di governo e mitigazione del *culture risk* (Cocozza e Metelli, 2025; AIFIRM 2025).

2.1 Cultura del rischio e rischio di cultura: un gioco di specchi concettuali

Le istituzioni finanziarie operano in un contesto caratterizzato da un'intrinseca esposizione all'incertezza e di conseguenza ai rischi, una situazione in cui l'attività di *risk management* non è soltanto un obbligo regolamentare, ma rappresenta una dimensione integrante del *core business* e, di conseguenza, della *leadership* strategica (Allen e Santomero, 1997). All'interno di questo ambito, *risk culture* e *culture risk* costituiscono due costrutti concettualmente distinti, ma strettamente interdipendenti.

La *risk culture* denota l'insieme di valori condivisi, atteggiamenti, competenze e norme comportamentali che plasmano il modo in cui il rischio viene percepito, comunicato e gestito all'interno di un'organizzazione. Essa si manifesta nelle azioni quotidiane di dipendenti e vertici aziendali, permeando le decisioni strategiche, l'allocazione del capitale e le scelte operative. Una *risk culture* solida funge da bussola interna, allineando i comportamenti con la sostenibilità a lungo termine dell'istituto e con le aspettative di vigilanza. Come sottolineato

dai principali Organismi Regolatori, la *risk culture* rappresenta il fondamento di una *governance* efficace e resiliente.

Al contrario, il *culture risk* si manifesta quando si registra un disallineamento tra i valori, aprioristicamente giusti³, enunciati dall'istituto e i comportamenti effettivamente praticati in tutta l'organizzazione. Tale disallineamento può dar luogo a scorrettezze etiche⁴, inefficienze operative e danni reputazionali, che minacciano al contempo la solidità prudenziale e la legittimità sociale dell'ente. Il *culture risk*, pertanto, va inteso come il rischio derivante da carenze nella costruzione di una cultura istituzionale coerente e "morale". I suoi sintomi includono l'erosione dei meccanismi di *accountability*, la rottura dei flussi comunicativi interni e la presenza di incentivi non allineati a comportamenti prudenti o, peggio, l'impunità di condotte critiche. Di fondamentale rilievo è il fatto che l'assenza di una *risk culture* matura costituisce essa stessa un vettore di *culture risk* (AIFIRM, 2025). Questa relazione ricorsiva spiega perché le Autorità di Vigilanza considerino oggi il *culture risk* non più un concetto astratto, ma un rischio materiale che richiede una *governance* strutturata, un monitoraggio sistematico ed azioni di mitigazione mirate. In questa prospettiva, la European Central Bank (ECB, 2024) sottolinea la necessità che le banche articolino, istituzionalizzino e valutino la *risk culture* come un *asset* strategico, anziché concepirla come un mero *ethos* intangibile.

La distinzione tra questi due concetti supera il mero gioco semantico: essa traccia il confine tra una *governance* proattiva e una reattiva. Mentre la *risk culture* mira a infondere valori prima che insorgano comportamenti devianti, il *culture risk* richiede meccanismi in grado di rilevare e correggere tali deviazioni. Di conseguenza, qualsiasi istituto che non investa preventivamente nella prima si troverà inevitabilmente a confrontarsi con il secondo, spesso a costi molto elevati.

Affrontare il *culture risk* richiede più di un impegno retorico: è indispensabile un quadro coerente, fondato su un'architettura di governo e rafforzato da sistemi di *performance management*. In particolare, esso esige una valutazione sistematica del *tone-from-the-top*, della coerenza dei canali di comunicazione interna, della credibilità degli incentivi e dell'efficacia

³ Il riferimento è al concetto di morale di Kant, ossia al complesso di norme e principi che regolano il comportamento di un individuo o di una collettività. Essa rappresenta l'insieme delle regole, dei valori e delle convinzioni concrete condivise da una comunità in un dato contesto storico-culturale. La moralità kantiana esalta il rispetto incondizionato per la dignità umana e l'impersonalità delle norme morali, contrastando derive utilitaristiche che subordinano l'individuo al benessere collettivo o al risultato contingente.

⁴ La morale è descrittiva: descrive "ciò che si fa" e "ciò che è considerato giusto o sbagliato" in un determinato gruppo sociale. L'etica invece è normativa: si occupa di stabilire "come bisognerebbe comportarsi", sviluppando criteri e teorie (deontologiche, utilitariste, comunitariste, ecc.) per valutare la moralità delle azioni.

dei meccanismi di *accountability*. È in questo contesto che la *corporate governance* può fungere da ancoraggio per un simile *framework*, mitigando il *culture risk* alle sue origini.

2.2. La governance quale leva di radicamento culturale

La *corporate governance*, nella sua formulazione più rigorosa, rappresenta l'infrastruttura istituzionale mediante la quale vengono distribuiti all'interno dell'impresa autorità, responsabilità e processi decisionali. Nel settore finanziario, tale infrastruttura non è mero strumento di adeguamento regolamentare, ma costituisce il fondamento del *risk management* e dell'orientamento strategico. L'attività di intermediazione creditizia e finanziaria si configura come un'attività caratterizzata da quelle che potrebbero essere definite, in maniera provocatoria, due principali "*business unit*": una commerciale ed una preposta ai controlli. Nell'ambito delle gestioni in esame nessuna delle due unità dovrebbe prevalere perché, se l'unità commerciale fosse preminente, ne potrebbero scaturire rischi incontrollabili e potenzialmente esiziali, mentre, se fosse predominante l'unità dei controlli, le attività commerciali potrebbero risultare fortemente compromesse da una parimenti esiziale "prudenza" o se si preferisce "eccessiva avversione al rischio". L'equilibrio tra le due anime dell'attività di intermediazione è forse la sfida maggiore per una *governance* consapevole e competente (Cocozza, 2024a e 2024b). In questa prospettiva, la *governance* delle istituzioni finanziarie deve non soltanto garantire la solidità procedurale, ma anche favorire l'interiorizzazione di comportamenti consapevoli del rischio a tutti i livelli organizzativi, fungendo da meccanismo di ancoraggio culturale. Come sottolineato sia dalla ECB sia dal BCBS, una *governance* solida è prerequisito imprescindibile per lo sviluppo di una *risk culture* efficace. Il *framework* di *governance*, infatti, costituisce l'architettura entro cui i valori culturali vengono formalizzati, comunicati e fatti rispettare. Il Consiglio di amministrazione, in quanto massima autorità decisionale, detiene la responsabilità primaria di istituire e mantenere una cultura etica e prudentiale. Ciò si traduce operativamente nell'allineamento strategico, nella supervisione tramite comitati dedicati e nell'adozione di salvaguardie strutturali quali l'indipendenza delle funzioni di controllo interno (AIFIRM, 2024).

La Vigilanza attribuisce al *board* non solo il compito di definire il *risk appetite* dell'istituto, ma anche di garantirne l'effettiva applicazione nei domini operativo, tecnologico e

comportamentale. Tali competenze includono la progettazione dei sistemi di incentivazione, il monitoraggio degli indicatori culturali e la valutazione della credibilità della *leadership*. Analogamente, il *top management*, sotto la direzione del consiglio, deve fungere da portatore di cultura, veicolando un *tone-from-the-top* coerente e assicurando l'allineamento tra valori dichiarati e azioni concrete. Inoltre, il modello delle tre linee di difesa riveste un ruolo cruciale nell'ancoraggio delle aspettative culturali all'interno dei processi istituzionali. *Risk management*, *compliance* e *internal audit* devono operare in modo indipendente, competente e con un mandato esplicito volto a monitorare la coerenza culturale. In particolare, il *Chief Risk Officer* (CRO) assume il ruolo di fulcro, collegando la *governance* strategica all'implementazione operativa; alla sua autorità deve corrispondere un adeguato *empowerment* strutturale e un canale di accesso diretto al *board*.

È fondamentale, quindi, che il sistema di *governance* recepisca il principio di proporzionalità. Le istituzioni di minori dimensioni possono necessitare di soluzioni su misura, senza tuttavia derogare agli *standard* di rigore culturale. Anzi, i rischi connessi a pratiche di *governance* informali e alla concentrazione decisionale nelle LSI richiedono una sensibilità culturale ancor più accentuata. In conclusione, la *governance* costituisce il substrato operativo della *risk culture*: essa definisce i canali attraverso cui la cultura si traduce in azione e stabilisce i meccanismi di controllo volti a individuare e correggere le deviazioni. Pertanto, qualsiasi istituto che intenda mitigare il *culture risk* deve partire da un'onesta valutazione dell'efficacia della propria struttura di *governance*.

3. Governance e assetti infrastrutturali della cultura del rischio

I concetti teorici devono essere tradotti in un'analisi sistematica delle architetture e degli strumenti di *governance* che sorreggono una cultura del rischio efficace. In questo ambito assumono rilievo le principali configurazioni di governo societario nel settore bancario ed il loro impatto sui flussi culturali interni. Le quattro dimensioni fondamentali – *tone-from-the-top* e credibilità della *leadership*; comunicazione efficace, *challenge* e diversità; *accountability*; incentivi allineati – identificate dalla Guida BCE (2024) come pilastri di un'infrastruttura

culturale resiliente costituiscono il fondamento della cultura del rischio. Essi però assumono contenuto concreto se collegati con i *driver* organizzativi del *culture risk* e il principio di proporzionalità, evidenziando come il dimensionamento e l'articolazione dei meccanismi di controllo debbano adattarsi alla complessità e alle caratteristiche delle istituzioni.

3.1. Architetture di governance e flussi culturali nelle istituzioni finanziarie

Nel sistema bancario europeo, l'evoluzione storica e regolamentare ha definito l'attuale sensibilità in materia di cultura e *governance* nella vigilanza finanziaria. Le strutture di governo istituzionale non fungono soltanto da meccanismi formali di controllo societario, ma anche da vettori di trasmissione culturale e di allineamento etico. La configurazione e il funzionamento dei modelli di *governance*, siano essi tradizionali, monistici o dualistici, incidono direttamente sulla capacità dell'istituto di ancorare una cultura del rischio coerente e di attenuare l'insorgenza del rischio di cultura.

Il modello di *governance* tradizionale, prevalente in Italia, si caratterizza per la netta separazione tra il Consiglio di amministrazione, incaricato della supervisione strategica e delle decisioni di *business*, e il Collegio Sindacale, cui è affidato il controllo sull'operato del Consiglio di amministrazione. Tale distinzione assicura un perimetro chiaro tra funzioni esecutive e di controllo, rafforzando l'efficacia del sistema dei controlli e degli equilibri interni. Nel modello monistico, il *framework* di *governance* è unificato in un unico organo, integrato da un comitato endoconsiliare di controllo interno composto da consiglieri indipendenti con adeguate competenze professionali. Questo assetto privilegia flessibilità ed efficienza, ma richiede salvaguardie più robuste per prevenire conflitti di interesse e garantire una vigilanza effettiva. Il modello dualistico, al contrario, prevede una separazione strutturale tra un Consiglio di Gestione (*Management Board*) e un Consiglio di Sorveglianza (*Supervisory Board*). Quest'ultimo, oltre alle funzioni tradizionali di controllo, può assumere responsabilità specifiche. Sebbene meno diffuso, questo schema può accrescere *accountability* e focalizzazione strategica, risultando particolarmente adatto a istituzioni complesse o appartenenti a gruppi bancari.

A prescindere dalle differenze strutturali, tutti i modelli di *governance* devono affrontare la dimensione culturale dell'intermediazione finanziaria: promuovere una comprensione condivisa del rischio, favorire *standard* comportamentali orientati alla creazione di valore di lungo periodo e radicare un approccio sensibile al rischio in tutti i livelli decisionali. La *governance* culturale, dunque, non si esaurisce negli statuti o nelle composizioni degli organi, ma richiede un costante rafforzamento attraverso prassi, valutazioni periodiche ed esempi di *leadership*.

Le più recenti iniziative regolamentari della Vigilanza hanno inoltre posto crescente attenzione sulla composizione del *board*, sulla diversità di prospettive e sull'idoneità collettiva dei consiglieri. È ormai acclarato che un consiglio eterogeneo per genere, competenze ed età riduce il rischio di “pensiero unico” – o dello sviluppo di una mentalità di gruppo – e favorisce decisioni più solide e radicate in presupposti etici. La presenza di membri con esperienza specifica in ambito ESG e *Information and Communication Technology* (ICT) è sempre più considerata non soltanto un requisito di conformità, ma una vera e propria garanzia di integrità reputazionale e strategica. In definitiva, i modelli di *governance* non sono meri schemi istituzionali, bensì quadri di legittimazione culturale e di allineamento comportamentale. Nella misura in cui la *governance* promuove trasparenza, inclusività e resilienza strategica, essa si configura come la prima linea di difesa contro l'insidiosa insorgenza del *culture risk*.

3.2. Le quattro dimensioni della cultura del rischio

L'EBA ha approfondito il proprio impegno sui temi culturali, emanando gli orientamenti in materia di *governance* interna (EBA, 2021a) e di politiche retributive solide (EBA, 2021b), entrambe inquadranti la *risk culture* come presupposto imprescindibile per una *performance* sostenibile e per la conformità regolamentare. Tali linee guida mettono in evidenza l'interdipendenza fra consapevolezza culturale, responsabilità individuale e resilienza istituzionale.

La pubblicazione della Guida su Governance e Cultura del Rischio (ECB, 2024) rappresenta il portato concettuale e operativo di questi filoni di intervento. Essa delinea un insieme di aspettative di vigilanza per la valutazione della qualità della *governance* e della

solidità culturale, articolate in quattro dimensioni fondamentali: *tone-from-the-top* e credibilità della *leadership*; Comunicazione efficace, *challenge* e diversità; *Accountability* nella condotta di rischio e Incentivi allineati a comportamenti prudenti. Particolarmente significativi sono i campanelli di allarme (*red flags*) specificati dalla Guida, ossia segnali diagnostici di disfunzioni di *governance* e culturali, utili per orientare l'*engagement* del sistema dei controlli interni sia delle Autorità di Vigilanza. Questo passaggio segna un mutamento paradigmatico: si passa da una mera conformità procedurale a una vera e propria "*cultural assurance*" (Cocoza, 2024a). Oggi i regolatori considerano l'integrità culturale non più un complemento desiderabile della *risk governance*, bensì il suo nucleo operativo.

Figura 1: Dimensioni della risk culture



Le istituzioni sono quindi chiamate a istituzionalizzare meccanismi di diagnostica culturale e al contempo ad integrare obiettivi culturali nelle valutazioni di performance, dando evidenza e dimostrando, a tutti i livelli, comportamenti proattivi in materia di contenimento del rischio.

La traiettoria regolamentare dell'ultimo decennio riflette un consenso crescente sul fatto che la stabilità finanziaria non dipenda soltanto da adeguati coefficienti patrimoniali e livelli di liquidità, ma anche dall'architettura etica e dall'integrità comportamentale delle istituzioni finanziarie. Tali attese si concretizzano nei quattro pilastri fondanti della *risk culture*, ciascuno

dei quali incarna un dominio critico del comportamento organizzativo e contribuisce non solo a radicare la consapevolezza del rischio, ma anche a edificare un'infrastruttura di *governance* resiliente ai disallineamenti culturali.

I valori e le priorità espressi e incarnati dal vertice definiscono i confini epistemici ed etici del comportamento organizzativo. Consiglio di amministrazione e *management* esecutivo non devono limitarsi a dichiarare l'impegno verso comportamenti sensibili al rischio, ma esemplificarli con coerenza. Il *tone-from-the-top* non è un mero artificio retorico, bensì un fattore strategico che permea ogni livello dell'istituto. Un'efficace *leadership* si esplica attraverso un messaggio chiaro, una visibilità dell'orientamento etico, un comportamento esemplare e la coerenza tra obiettivi strategici e aspettative comportamentali. Studi empirici evidenziano come l'incoerenza o l'opacità della *leadership* alimentino il *culture risk*, favorendo cinismo, ambiguità e razionalizzazioni di comportamenti scorretti. Al contrario, *leader* che mostrano umiltà, apertura al confronto e responsabilità personale creano un punto di riferimento normativo che legittima decisioni prudenti e frena derive etiche (Carretta et al., 2024).

Una comunicazione aperta e multidirezionale è condizione necessaria per garantire l'integrità culturale. La *risk culture* prospera in contesti in cui il personale è incoraggiato a sollevare preoccupazioni, mettere in discussione assunti ed esprimere dissenso senza timore di ritorsioni. Le istituzioni devono istituire canali formali (protocolli di *escalation*, piattaforme di *whistleblowing*) e promuovere norme informali che consolidino la sicurezza psicologica e dialogo costruttivo, ossia un contesto in cui non sussiste timore di esprimere opinioni o dissenso (Cocozza, 2024b). La diversità di pensiero, di *background*, di competenze e di esperienza rafforza questa funzione comunicativa: *team* eterogenei sondano meglio i processi decisionali, contrastano la mentalità di gruppo e individuano i rischi da molteplici prospettive, talché la Vigilanza sottolinea sempre più l'importanza della diversità nella composizione degli organi sociali, nelle strutture manageriali e nella *governance* dei progetti come leva per una profondità culturale maggiore e più efficace.

Una *risk culture* credibile richiede ruoli e responsabilità chiaramente definiti e la tracciabilità delle determinazioni di rischio fino ai nodi decisionali. Le istituzioni devono istituzionalizzare sistemi di *accountability* individuale e collettiva, affinché le scelte in ambito creditizio, di *trading*, sicurezza IT o *design* di prodotto possano essere verificate ex post rispetto alle *policy* e alle aspettative etiche. L'*accountability* implica altresì una chiarezza

sanzionatoria: occorre evitare tanto l'impunità quanto il capro espiatorio, favorendo una cultura in cui gli errori siano affrontati in modo proporzionato e costruttivo, mentre i comportamenti scorretti siano penalizzati con fermezza. Le guide di ECB (2016; 2024) ed EBA (2021a) sottolineano costantemente la centralità della chiarezza dei ruoli, della trasparenza delle conseguenze e dei meccanismi di *feedback* come indicatori di una "cultura della responsabilità" funzionante.

Le strutture incentivanti sono le leve comportamentali attraverso le quali la cultura si traduce in pratica. Quando i parametri di *performance* premiano esclusivamente il profitto a breve termine, ignorando l'esposizione al rischio, si genera *moral hazard* e si compromette l'integrità dei controlli. Per questo motivo, i Regolatori richiedono ora che i *framework* retributivi integrino metriche *risk-adjusted* e indicatori di sostenibilità economico-finanziaria. In fase antecedente, la variabile retributiva dovrebbe dipendere dall'osservanza delle norme etiche, dal rispetto delle *policy* di rischio e dal contributo agli obiettivi strategici di lungo periodo. In fase susseguente, le clausole di *malus* e *clawback* devono essere operative per contrastare comportamenti negligenti o imprudenti. Inoltre, anche gli incentivi non finanziari – riconoscimenti, percorsi di carriera e opportunità di formazione – devono allinearsi alle prestazioni culturali, rafforzando norme etiche e collaborative.

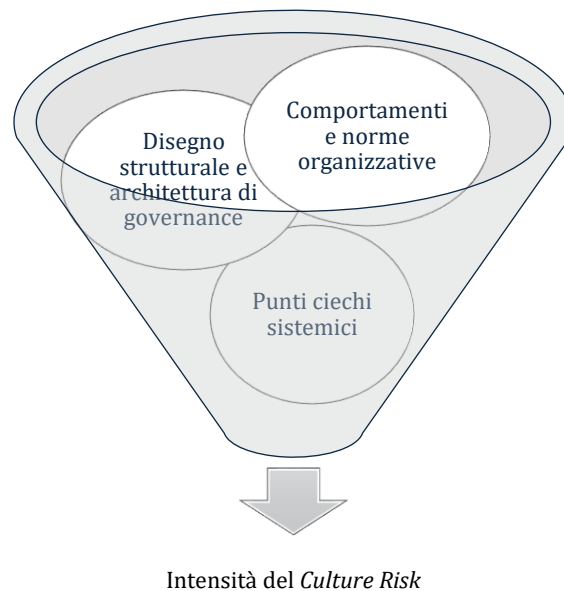
Questi quattro pilastri, considerati nel loro complesso, non operano in modo indipendente: interagiscono come un sistema in cui la debolezza di una dimensione (ad esempio, una comunicazione inefficace o incentivi ambigui) può minare l'integrità dell'insieme. Le istituzioni impegnate a coltivare una *risk culture* resiliente devono dunque valutare, calibrare e integrare tutte e quattro le dimensioni all'interno dei propri *framework* di *governance*.

3.3. Driver del rischio di cultura

I quattro pilastri orientano l'individuazione dei *driver* di *culture risk* all'interno dei diversi sottosistemi organizzativi. La comprensione dei fattori determinanti del *culture risk* richiede una prospettiva analitica in grado di integrare variabili strutturali, comportamentali e contestuali. Il *culture risk* non emerge "spontaneamente": esso si sviluppa in condizioni organizzative che consentono o non correggono i disallineamenti fra valori istituzionali

dichiarati e comportamenti quotidiani. Tali condizioni si manifestano su tre dimensioni principali: comportamenti e norme organizzative, disegno strutturale e architettura di *governance*, e punti ciechi sistemici.

Figura 2: Driver del culture risk



Per quanto attiene ai comportamenti e alle norme organizzative, il *culture risk* trova terreno fertile in contesti caratterizzati da un *drift* comportamentale, in cui le norme informali divergono dalle aspettative formali. Quando l'assunzione incontrollata di rischio viene normalizzata senza adeguati meccanismi di controllo, o quando il superamento dei limiti viene ignorato o peggio tacitamente premiato, si crea ciò che è stato definito un "contesto permissivo" per derive culturali. Questi ambienti si contraddistinguono per culture di *challenge* deboli, ancora etiche indebolite ed erosione dei meccanismi interni di *accountability*. Tali comportamenti tendono a autoalimentarsi: una volta che si radica una cultura del silenzio o dell'indifferenza diventa sempre più difficile ristabilire una disciplina etica. Questo fenomeno si accentua in contesti ad alta pressione, come le postazioni di *trading*, le culture commerciali aggressive o i poli di innovazione tecnologica, nei quali gli incentivi di *performance* possono sovrastare i confini della *governance*.

Anche la forma organizzativa può fungere da fattore di rischio culturale, in quanto il disegno strutturale e l'architettura di governo contribuiscono a definire il portato concreto della cultura del rischio e quindi l'intensità dell'esposizione al rischio di cultura. Gerarchie

centralizzate con flussi informativi inadeguati spesso isolano il processo decisionale e reprimono il dissenso. Al contrario, strutture eccessivamente frammentate possono ostacolare una supervisione coerente e permettere la proliferazione di incoerenze culturali tra linee di *business*, aree geografiche o entità giuridiche. Il rischio è particolarmente accentuato in modelli di *governance* in cui le linee di *accountability* risultano ambigue, la separazione delle funzioni è poco definita o le funzioni di controllo sono strutturalmente subordinate agli obiettivi di *business*. L'assenza di percorsi di *escalation* diretta verso organi di controllo indipendenti – in particolare per *compliance* e *risk management* – può ostacolare la tempestiva individuazione di violazioni culturali. Inoltre, una composizione del *board* inadeguata e una carenza di competenze in aree emergenti quali ESG e *digital risk governance* possono condurre a un'analisi superficiale dei rischi connessi ai comportamenti organizzativi. Un consiglio di amministrazione privo degli strumenti per interpretare indicatori culturali o valutarne le implicazioni strategiche può involontariamente aggravare l'esposizione a criticità reputazionali e operative.

Oltre alle strutture interne, il *culture risk* è alimentato da punti ciechi cognitivi e procedurali e dalle carenze di *feedback*. Le istituzioni che non raccolgono o non valorizzano il *feedback* – proveniente da dipendenti, clienti o funzioni di controllo – creano un'asimmetria tra cultura percepita e cultura reale. Questa dissonanza può celare vulnerabilità critiche fino a quando non si manifestano in scandali o interventi di vigilanza. Tra i campanelli di allarme rientrano l'assenza di segnalazioni *whistleblowing*, la mancanza di canali di *feedback* ascendenti, punteggi di *engagement* bassi nelle *survey* del personale o rilievi ricorrenti degli *audit* relativi ad anomalie comportamentali. Quando tali indicatori vengono ignorati o giustificati, l'istituzione perde l'opportunità di correggere tempestivamente la propria rotta culturale.

È importante osservare che i fattori di *culture risk* difficilmente si manifestano in isolamento: essi costituiscono spesso un ecosistema di disfunzioni in cui debolezze di *governance*, incentivi comportamentali e carenze comunicative si rafforzano reciprocamente. È pertanto imprescindibile che le istituzioni adottino un *framework* diagnostico integrato, capace di individuare la fragilità culturale sia a livello micro sia a livello macro.

3.4. Il principio di proporzionalità nel governo del rischio di cultura

L'implementazione efficace della *governance* culturale nelle istituzioni finanziarie richiede un adattamento al contesto specifico in cui ciascun ente opera. Il principio di proporzionalità, da lungo tempo presente nel dibattito regolamentare europeo, impone che strutture di *governance*, funzioni di controllo e *framework* di *risk culture* siano calibrati in base a dimensioni, complessità, rilevanza sistemica e modello di *business* dell'istituto. Tuttavia, la proporzionalità non può essere fraintesa come un invito alla semplificazione o all'indulgenza. Al contrario, essa implica un'adeguata modulazione delle aspettative di *governance* affinché istituti di profili diversi – che siano *Global Systemically Important Banks* (G-SIBs), LSI o nuovi operatori *fintech* – possano interiorizzare gli imperativi culturali in modo significativo e operativo.

Per gli enti di maggiori dimensioni o complessità, la proporzionalità richiede processi di *governance* formalizzati, diagnosi culturali dettagliate e indicatori di *performance* robusti e collegati alla consapevolezza del rischio e ai comportamenti aziendali. Tali istituti devono istituire organismi di *governance* multilivello, garantire una solida indipendenza dell'*Internal Audit* e documentare le iniziative culturali lungo linee di *business* e aree geografiche.

Per le banche più piccole o meno complesse, la *governance* culturale non può essere meno rigorosa, ma la sua attuazione può avvenire con modalità meno burocratiche. Le LSI, ad esempio, possono adottare metriche culturali semplificate, comitati formali ridotti e un più diretto coinvolgimento della *leadership*. Ciò che non possono permettersi, tuttavia, è un approccio informale alla cultura o una *governance* basata esclusivamente sulla personalità dei vertici, a scapito del dibattito interno e della resilienza istituzionale.

Un errore frequente nell'applicazione del principio di proporzionalità è ritenere che il *culture risk* sia meno rilevante nelle entità di piccole dimensioni o specializzate. Al contrario, la loro vulnerabilità aumenta a causa di strutture decisionali concentrate, pratiche di *governance* informali o carenza di consapevolezza culturale. Pertanto, la proporzionalità non deve diventare un pretesto per la negligenza, bensì un meccanismo di rilevanza operativa, che assicuri l'appropriatezza, l'agilità e l'integrazione strategica dei presidi culturali.

In quest'ottica, la proporzionalità opera in senso "inverso": proprio perché le LSI dispongono di strutture di *governance* più snelle, decisioni concentrate e risorse di controllo interne limitate, esse sono ancor più esposte al *culture risk* e richiedono vigilanza rafforzata piuttosto che alleggerimenti procedurali (Cocozza e Metelli, 2025). La ECB (2024) afferma esplicitamente che buona *governance* e solida cultura del rischio sono ugualmente essenziali per tutte le banche, a prescindere dalle dimensioni, e che la proporzionalità non deve mai compromettere la sostanza delle salvaguardie aziendali in termini di cultura del rischio. Analogamente, gli orientamenti in tema ESG (EBA, 2025) escludono la dimensione aziendale come criterio sufficiente per un trattamento agevolato, lasciando intendere che le banche minori non sono necessariamente meno esposte potendo subire minacce amplificate in ragione della concentrazione dei portafogli.

Dal punto di vista del diritto positivo, la proporzionalità va interpretata come personalizzazione qualitativa anziché come diluizione quantitativa: un numero minore di livelli burocratici non legittima un numero inferiore di difese culturali, ma obbliga l'istituto ad adottare indicatori ad alta granularità e un presidio diretto da parte del consiglio per compensare le fragilità strutturali. In termini operativi, questo implica che le LSI debbano mettere in campo canali di *whistle-blowing* particolarmente efficaci, garantire un *surplus* di *challenge* indipendente nella composizione del *board* e integrare KPI/KRI sensibili alla cultura nei cruscotti delle *business line*: strumenti che, pur riducendo la burocrazia, aumentano l'accuratezza nel monitoraggio dei comportamenti. La "proporzionalità inversa" riconosce così che la compiacenza culturale comporta un costo sistemico proporzionalmente più elevato per le LSI, e che le aspettative di vigilanza verso di loro devono considerarsi acute piuttosto che attenuate.

Infine, la proporzionalità richiede un allineamento con il modello di *business* dell'istituto. Per le banche *retail* con estesi rapporti diretti con la clientela, il *culture risk* può manifestarsi attraverso comportamenti scorretti *in front line* o pratiche di *misselling*. Per le *investment bank*, esso può derivare dal comportamento dei *trader* e dal disallineamento degli incentivi. Per le *fintech*, cicli di innovazione rapidi e strutture orizzontali possono generare *culture risk* a causa di decisioni guidate dalla velocità e responsabilità sfocate. Inoltre, le istituzioni con operatività *cross-border* devono affrontare variazioni giurisdizionali in termini di aspettative culturali, quadri normativi e livelli di scrutinio regolamentare, mantenendo una sostanziale coesione culturale senza imporre uniformità artificiale.

Le funzioni di controllo devono essere dimensionate e dotate in misura corrispondente al grado effettivo di *risk culture* dell'istituto. Ogni ente deve garantire indipendenza dei controlli, integrità delle linee di *reporting* e capacità di *oversight* culturale. La chiave non è la mera replica strutturale, ma la sufficiente efficacia funzionale dei controlli. Indicatori culturali quali *survey* di *engagement*, *report* di incidenti, attività di *whistle-blower* e integrazione di KRI/KPI devono essere implementati in funzione della maturità istituzionale: metriche ad alta frequenza possono rivelarsi cruciali in ambienti particolarmente dinamici, mentre *review* narrative e “*pulse check* periodici” possono bastare in contesti più stabili e basati su relazioni consolidate.

In definitiva, un approccio proporzionato alla *risk culture* richiede una calibrazione dinamica: riconoscere che le istituzioni evolvono, che i rischi mutano e che la *governance* deve adeguarsi di conseguenza. Analogamente, le valutazioni della Vigilanza riflettono tale dinamicità, esaminando non solo la conformità formale, ma anche la coerenza culturale e la resilienza dei sistemi di *governance*.

4. Il rischio di cultura: protagonisti, elementi e dinamiche.

La traduzione della gestione del rischio di cultura in prassi operative richiede la mappatura dei ruoli e delle responsabilità degli attori chiave dal Consiglio di amministrazione al CRO fino alle funzioni di controllo interno e alla funzione organizzativa (Cocozza e Metelli, 2025) chiarendo il contributo fornito da ognuno dei protagonisti al presidio continuo dell'integrità culturale. Questa mappatura deve essere integrata dal *toolkit* degli strumenti di governo, quali indicatori comportamentali, protocolli di *escalation* e piattaforme di *culture-pulse*, fondamentali per rilevare e correggere tempestivamente le derive culturali. L'integrazione della cultura del rischio nei sistemi di *risk management* da atto di come monitoraggio, reportistica e *governance* dei dati si combinino per trasformare la *risk culture* da aspirazione retorica in elemento “*hard-wired*” nella gestione del rischio complessivo.

4.1. Gli attori del governo del rischio di cultura

L'istituzionalizzazione della *risk culture* si fonda innanzitutto sugli attori incaricati della sua *governance*. Consigli di amministrazione, comitati endoconsiliari, vertici esecutivi e funzioni di controllo svolgono ruoli distinti ma interdipendenti nel consolidare una cultura allineata all'assunzione prudente del rischio, all'integrità regolamentare e alla condotta etica. Nella presente sezione vengono mappate le loro responsabilità, con particolare riguardo ai meccanismi mediante i quali la cultura viene plasmata, monitorata e corretta. A titolo esemplificativo, i principali ruoli all'interno della struttura organizzativa di un'istituzione finanziaria possono essere così articolati: Consiglio di amministrazione, Comitati endoconsiliari, *C-Suite*, Funzioni Aziendali di Controllo (FAC), Organizzazione e risorse umane (AIFIR; 2025).

Il Consiglio di amministrazione è di fatto il paladino strategico della cultura del rischio. Il Consiglio detiene la responsabilità ultima nella definizione della *risk culture* dell'istituto. Tra le sue attribuzioni vanno annoverate la definizione del *tone-from-the-top*, l'approvazione – ed implicitamente la definizione – del *Risk Appetite Framework* (RAF), la valutazione della dinamica degli indicatori culturali e la vigilanza sul rispetto, da parte del vertice esecutivo, dei valori dichiarati. I membri del Consiglio di amministrazione devono possedere, collettivamente, non solo competenze bancarie e finanziarie, ma anche conoscenze in materia di comportamento organizzativo, temi ESG e *governance* ICT. Diversità e indipendenza nella composizione del *board* sono essenziali per evitare visioni monoculturali e favorire un'efficace attività di *challenge*. Inoltre, il Consiglio di amministrazione dovrebbe interagire utilmente con i comitati rischi e *audit* per esaminare i risultati delle diagnosi culturali interne e promuovere un miglioramento continuo dell'ambiente etico e dei principi ispiratori, sotto il profilo culturale, del sistema dei controlli interni.

All'interno del *board*, i comitati endoconsiliari specializzati traducono i principi di *governance* in un'effettiva attività di vigilanza strutturata. Il Comitato Rischi è – con riferimento al tema qui in esame – incaricato di monitorare il profilo di rischio dell'istituto includendo i rischi di natura culturale, e di fornire pareri – e, ove di necessità, proporre anche iniziative – sull'allineamento tra strategia e resilienza culturale. Il Comitato Audit si concentra sull'efficacia dei controlli interni, comprendendo anche quelli relativi alla conformità comportamentale, al *tone-from-the-top* e alla gestione delle segnalazioni *whistleblowing*. In

alcuni modelli di *governance* può essere istituito un Comitato Etica o Condotta, con il compito di sovrintendere ai *framework* di integrità, particolarmente in istituzioni esposte a rischi reputazionali elevati.

Il *management* esecutivo, con il *Chief Executive Officer* (CEO) e gli altri *C-level*, agisce da principale vettore di trasmissione culturale e, dunque, di effettiva efficacia. Il loro ruolo va ben oltre l'esecuzione operativa, includendo il rafforzamento dei messaggi strategici, l'esempio di elevati *standard* etici e la responsabilizzazione dei *team* sui risultati comportamentali. In questo contesto, il Chief Risk Officer (CRO) funge da fulcro tra *governance* e operatività: egli dovrebbe godere di accesso diretto al *board*, di indipendenza da pressioni commerciali e di un mandato che comprenda anche l'identificazione, la misurazione e la mitigazione dei rischi culturali. Una stretta collaborazione tra CRO, *Chief Financial Officer* (CFO), *Chief Human Resources Officer* (CHRO) e *Chief Compliance Officer* (CCO) è fondamentale per garantire l'allineamento tra controlli, sostenibilità finanziaria e valori organizzativi.

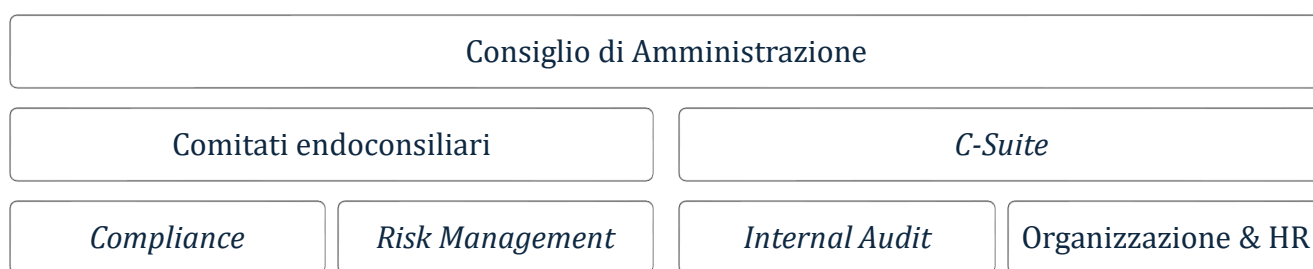
La FAC – *Compliance, Risk Management, Internal Audit* – costituiscono insieme la difesa dell'istituto nei confronti del *culture risk*. Ciascuna opera in dimensioni temporali e procedurali distinte. La compliance, impegnata prevalentemente in una attività di controllo antecedente, verifica, tra l'altro, che le *policy* interne aderiscano a *standard* regolamentari ed etici, monitorando anche che le modifiche organizzative proposte siano coerenti agli obiettivi valoriali dell'istituto. Il *Risk Management* interviene sia *ex ante* sia in tempo reale, identificando e valutando i rischi culturali emergenti, consigliando strategie di mitigazione e integrando metriche culturali nel RAF. L'*Internal Audit* fornisce *assurance ex post*, valutando in modo indipendente se le aspettative culturali siano effettivamente radicate nei processi decisionali, nelle prassi di controllo, nelle norme organizzative e nelle condotte individuali.

È cruciale che queste funzioni dispongano di adeguato *standing*, indipendenza e risorse: la loro subordinazione strutturale alle linee di *business* o linee di *reporting* incoerenti possono comprometterne credibilità ed efficacia e sono contendibili sotto il profilo dell'adeguatezza del sistema dei controlli interni.

Pur non rientrando tecnicamente nelle funzioni di controllo, le Risorse Umane e le strutture che si occupano di sviluppo organizzativo svolgono un ruolo centrale nell'implementazione della *risk culture*. Dalla selezione e *onboarding*, alla valutazione delle *performance* e ai piani di successione, queste funzioni influenzano i valori e gli atteggiamenti introdotti e rinforzati quotidianamente. I programmi formativi, gli incentivi di carriera e le

iniziative di *engagement* devono essere esplicitamente concepiti in funzione degli obiettivi culturali. In presenza di segnali di *culture risk* il CHRO deve agire come *partner* nella fase di *remediation*, proponendo adeguamenti di *policy*, rafforzando le aspettative e fornendo *feedback* di sviluppo.

Figura 3: Protagonisti del culture risk



Nel loro insieme, questi attori costituiscono un ecosistema di *governance* culturale. La loro efficacia non dipende soltanto da chiarezza di mandato e competenza tecnica, ma anche da fiducia reciproca, trasparenza e da un'effettiva volontà istituzionale di intercettare i comportamenti prima che possano evolvere in rischi sistemici.

4.2. Gli strumenti di governo del rischio di cultura

Per radicare e sostenere una cultura sensibile al rischio, le istituzioni devono adottare un insieme integrato di strumenti che traducano le intenzioni culturali in prassi operative e misurabili. Tali strumenti supportano il monitoraggio, il rinforzo e il continuo perfezionamento delle aspettative culturali all'interno delle funzioni di *governance* e di *business*. Essi comprendono metriche di *performance*, sistemi di *reporting* interno, protocolli di *escalation* e diagnostiche culturali.

I KPI e i KRI costituiscono strumenti fondamentali per verificare l'aderenza tra obiettivi culturali e comportamenti effettivi. I KPI non devono riflettere unicamente target finanziari o operativi, ma anche parametri culturali, quali ad esempio livelli di *engagement* dei dipendenti, frequenza delle segnalazioni di incidenti, tassi di completamento della formazione o valutazioni comportamentali derivanti da *review* a 360 gradi. I KRI, invece, forniscono segnali precoci di possibili *culture risk*, quali variazioni nel *turnover* delle funzioni di controllo, picchi

di violazioni di *compliance*, ritardi nelle azioni correttive o anomalie nei comportamenti incentivati. Un *framework* coerente deve collegare KPI e KRI affinché gli obiettivi di performance non compromettano la condotta attenta al rischio. Per massimizzare l'efficacia, tali indicatori devono essere: pertinenti al profilo strategico e di rischio dell'istituto; quantificabili ove possibile, ma comprensivi di valutazioni qualitative (ad esempio *audit* comportamentali); tempestivi, per consentire risposte proattive e presentati tramite *dashboard* accessibili a funzioni di controllo ed esecutive oltre che ai vertici aziendali.

Sistemi di *reporting* trasparenti, affidabili e bidirezionali sono essenziali per una *governance* culturale efficace. Le istituzioni dovrebbero istituire canali formali di comunicazione – quali report sulla cultura del rischio, *dashboard* di condotta e *heat-map* culturali – periodicamente riesaminati da comitati rischi, vertici esecutivi e *internal audit*. I dati culturali vanno incorporati nelle *overview* del *risk management* e inclusi come oggetto ricorrente nei verbali dei comitati secondo le rispettive competenze. Il vertice, a sua volta, deve chiudere il ciclo fornendo riscontri sui problemi segnalati e illustrando le azioni intraprese, rafforzando così la credibilità dei meccanismi di *reporting*.

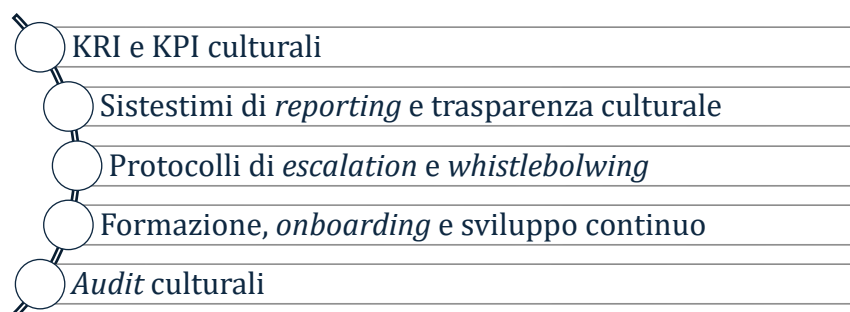
I protocolli di *escalation* e *whistleblowing* sono un altro strumento essenziale di governo del rischio di cultura. La capacità di far emergere tempestivamente preoccupazioni culturali è un indicatore chiave dell'integrità comportamentale dell'istituto. I protocolli di *escalation* devono essere chiari, confidenziali e accessibili, supportati da canali di *whistleblowing* formalizzati, costantemente monitorati, protetti da ritorsioni e sottoposti a verifiche periodiche. Il personale deve essere formato su modalità e momenti in cui sollevare segnalazioni, e i *log* di *escalation* vanno analizzati per identificare tendenze. Un basso numero di segnalazioni, se isolato, non deve essere interpretato automaticamente come indice di buona salute culturale, soprattutto se altri indicatori, ad esempio *survey* sul personale, evidenziano timori o cinismo.

La formazione svolge, in questo ambito, un ruolo fondamentale. I programmi formativi devono non solo trasmettere conoscenze tecniche, ma favorire l'interiorizzazione dei valori della cultura del rischio. I percorsi di inserimento per le nuove risorse, in particolare per ruoli sensibili al rischio, dovrebbero includere l'illustrazione delle aspettative culturali dell'istituto, l'analisi di *case study* di condotta e il *mentoring* da parte di figure che incarnano la cultura desiderata. Opportunità di sviluppo continuo, quali *workshop*, analisi di scenari e simulazioni comportamentali, possono rinforzare la cultura a tutti i livelli di anzianità. L'efficacia della

formazione va misurata non solo in termini di partecipazione, ma anche in base a cambiamenti di atteggiamenti, metriche di condotta o *feedback* dei pari.

Audit culturali periodici, interni o condotti da terzi qualificati, offrono uno strumento strutturato per valutare il grado di allineamento culturale. Tali revisioni dovrebbero esaminare tendenze comportamentali, norme organizzative, analisi di casi di incidente e la percezione dell'integrità dei messaggi di *leadership*. Strumenti di autocertificazione, quali *survey* di “*culture pulse*”, interviste qualitative e diagnostiche di atteggiamento al rischio, possono integrare *audit* più formali. I risultati devono alimentare l'adeguamento del *risk appetite*, la revisione delle *policy* e i *framework* di *performance management*.

Figura 4: Strumenti di gestione del culture risk



Implementati in modo integrato, questi strumenti di *governance* trasformano la cultura del rischio da mera aspirazione retorica in una realtà istituzionale misurabile, gestita e – auspicabilmente – in costante miglioramento.

4.3. Integrazione della cultura del rischio all'interno dei sistemi di Risk Management

Per radicare e sostenere una *risk culture* autenticamente resiliente, è indispensabile che gli impegni astratti enunciati dal Consiglio di amministrazione si traducano senza soluzione di continuità nelle *routine* quotidiane dell'architettura di gestione del rischio, dalla fase iniziale di identificazione fino all'atto finale di *escalation*.

Nella fase di identificazione, le banche devono ampliare l'orizzonte della tradizionale scansione dei rischi per cogliere fragilità comportamentali e culturali. Ciò significa integrare

diagnosi qualitative, quali debolezze nelle funzioni di controllo, segnali di *leadership* contraddittori e disimpegno dei dipendenti, all'interno delle valutazioni di rischio a livello di impresa, delle analisi post-incidente e degli esercizi di scenario, esplicitamente concepiti per tenere conto della fallibilità umana e della normalizzazione di condotte deviate e devianti. Un'identificazione esaustiva non si limita a censire le esposizioni finanziarie o strategiche, ma ingloba le vulnerabilità comportamentali e culturali, attraverso *framework* diagnostici in grado di rilevare l'insorgere di erosioni culturali.

Il *Risk Appetite Statement* (RAS) rappresenta la pietra angolare giuridica della *governance* contemporanea del rischio e, al contempo, un vero e proprio "patto culturale". Redatto e periodicamente aggiornato da Consiglio di Amministrazione, secondo le proposte avanzate dal del CRO e dai vertici esecutivi, il RAS accoppia soglie quantitative a tolleranze comportamentali chiaramente articolate, vincolando le aspettative etiche all'allocazione strategica delle risorse e consentendo la declinazione a cascata in schemi incentivanti, *policy* e piani industriali. Per essere strumento credibile di allineamento culturale, il RAS deve fissare limiti espliciti anche per il rischio culturale ed etico, definire *standard* di integrità e incorporare i valori organizzativi in ogni percorso decisionale legato al rischio. Approvato dal *board*, il RAS va diffuso all'intera organizzazione e collegato in modo esplicito alle architetture retributive e ai cicli di pianificazione strategica.

Gli obiettivi culturali devono essere resi osservabili mediante l'integrazione accurata di KPI e KRI, indicatori "*leading*" come tassi di completamento della formazione e punteggi di *tone-from-the-top*, devono essere affiancati da "*lagging*" quali violazioni di compliance, indifferenza ai *finding* e alle azioni rimediali, procrastinazione nel perfezionamento dei correttivi. Tali metriche, granulari a livello di *business unit*, devono confluire in *dashboard* destinate a *performance review* che mettano in chiaro il nesso tra condotta e creazione di valore. Un solido *framework* connette indicatori anticipatori (es. *survey* etiche, punteggi di clima aziendale) con indicatori a consuntivo (es. sanzioni, reclami), supportando sia interventi tattici sia la ricalibrazione strategico del *risk appetite*.

La sorveglianza permanente di questi indicatori richiede un *toolbox* ibrido che combini test di controllo tradizionali con analisi comportamentali, dati di *whistleblowing* e tracciamento del *sentiment*, governati da *trigger* di *escalation* predeterminati. Quando emergono anomalie culturali, queste devono essere tempestivamente elevate all'esame del *board* o di un eventuale comitato dedicato.

In questo ecosistema, il CRO assume una funzione chiave: dotato di accesso diretto al *board* e di autonomia dalle pressioni commerciali, il CRO promuove metriche culturali, sfida eventuali condotte devianti e verifica che ogni iniziativa strategica venga esaminata anche nelle sue ricadute culturali, incarnando egli stesso una *leadership* etica.

Protocollo cruciale è una *data governance* robusta, basata su integrità e trasparenza, nel rispetto della privacy, che consenta la raccolta, la validazione e l'analisi sistematica degli indicatori culturali: dai *log* formativi all'attività della linea etica, dalle deviazioni di *performance* ai colloqui di uscita strutturati. Tecniche di *advanced analytics*, inclusi modelli di *machine learning* e *network analysis*, possono far emergere pattern significativi e correlare i comportamenti a esiti di rischio, pur rimanendo entro i limiti di un approccio proporzionato.

Quando questi elementi convergono, la *risk culture* non resta una mera aspirazione retorica, ma diviene un vettore *hard-wired* di *risk management*. In tal modo, l'istituto rafforza la propria immunità giuridica, prudenziale ed etica in un contesto di vigilanza sempre più complesso.

Conclusioni

Il presente saggio ha indagato, in una prospettiva dottrinale e manageriale, le basi concettuali, gli assetti di *governance*, le leve operative e le attese di vigilanza che orientano la coltivazione di una solida *risk culture* e l'attenuazione del *culture risk* nelle istituzioni di credito. L'analisi supporta alcune proposizioni di fondo, che possono essere considerate linee guida per la gestione del *rischio di cultura*. All'esito delle riflessioni proposte, si propone un'agenda, certamente non esaustiva, volta al continuo perfezionamento della *governance* culturale in un'era di rapidi cambiamenti regolamentari, sociali e tecnologici.

La *risk culture* come *asset* strategico

La *risk culture* va intesa come elemento centrale e non come un fenomeno periferico e di scarso rilievo. Essa è un *asset* strategico che condiziona le decisioni, modella gli incentivi comportamentali e definisce l'equazione rischio-rendimento dell'istituto. Pertanto, merita un peso probatorio pari a quello dei tradizionali indicatori finanziari, tanto nella pianificazione strategica quanto nella valutazione delle *performance*. Le banche devono trattare la cultura del

rischio non come un semplice strumento di *compliance* o di tutela reputazionale, ma come fattore centrale di sostenibilità istituzionale.

La *stewardship* culturale nella *governance*

La cura della cultura è funzione dell'architettura di *governance* e della qualità dell'esempio. Consigli di amministrazione e vertici esecutivi *C-level* devono concretizzare le parole in comportamenti, preservare l'indipendenza delle funzioni di controllo e inserire la vigilanza culturale quale mandato esplicito e non delegabile del *board*, riconoscendo che la credibilità della *leadership* costituisce la condizione *sine qua non* della resilienza culturale.

La managerialità del *culture risk*

Sebbene la *risk culture* non sia direttamente misurabile, il *culture risk* lo è senza dubbio. Ne consegue che il rischio culturale è sia monitorabile sia mitigabile: non è elusivo né inquantificabile, ma deve essere individuato, misurato e gestito attraverso sistemi integrati di KPI/KRI che catturino segnali comportamentali, tendenze incidentali e *intelligence* da *whistle-blower*, supportati da *trigger* di *escalation* predefiniti e sottoposti a *stress-test* periodici all'interno delle valutazioni di rischio a livello di impresa. Le diagnostiche culturali devono dunque divenire componente ordinaria del *risk assessment*.

Proporzionalità come personalizzazione intelligente

Il principio di proporzionalità richiede modulazione "intelligente", non attenuazione: le istituzioni di dimensioni o complessità minori non possono invocare la scala come giustificazione per un minimalismo culturale. Al contrario, devono adottare meccanismi su misura, pur rigorosi, commisurati alla loro maggiore esposizione a fragilità di *governance*, mentre la vigilanza rimane egualmente esigente su LSI, nuovi operatori fintech e banche tradizionali.

La *data governance* a supporto dell'integrità culturale

Una *governance* dei dati responsabile è prerequisito e banco di prova per l'integrità culturale. Le istituzioni devono investire in infrastrutture sicure e trasparenti capaci di raccogliere e analizzare dati culturali – dalle analisi di *sentiment* ai *pattern* comportamentali – garantendo al contempo il rigoroso rispetto delle norme di *privacy* ed etica.

La governance culturale come processo dinamico

La *governance* culturale è un'attività dinamica, che deve evolvere in sincronia con i cambiamenti di *leadership*, i riallineamenti strategici e gli *shock* esogeni. Gli intermediari finanziari dovrebbero istituzionalizzare un'autovalutazione culturale continua. Del pari è ragionevole attendersi che le Autorità di Vigilanza promuovano progressivamente un dialogo aperto e iterativo, valorizzando pratiche esemplari, fornendo linee guida tematiche e incorporando indicatori culturali nel Supervisory Review and Evaluation Process (SREP). In tale contesto, il *culture risk* si configura come elemento integrante del *governance risk* nell'ambito ESG e merita come tale un'adeguata collocazione nel processo di revisione e valutazione da parte della Vigilanza.

Il *culture risk* non è né astratto né incidentale: è la radice di tutti i rischi, la condizione da cui scaturiscono inadeguatezza della *governance*, violazioni etiche e fallimenti strategici. La sua mitigazione non compete esclusivamente alle funzioni di controllo, bensì all'intera architettura di *governance*. In un'epoca di elevata complessità, scrutinio e cambiamento trasformativo, le istituzioni che investono nella maturità culturale sono quelle meglio posizionate per preservare la fiducia, fronteggiare l'incertezza e conseguire una resilienza duratura.

Bibliografia

AIFIRM. 2024. Comments to ecb guide on governance and risk culture. <https://www.aifirm.it/wp-content/uploads/2024/10/2024-45-Risposta-cons.-BCE-Draft-Guide-on-Governance-and-Risk-Culture.pdf>.

AIFIRM. 2025. Governance and risk culture. <https://www.aifirm.it/wp-content/uploads/2025/06/2025-Position-Paper-48-Governance-e-Risk-Culture.pdf>.

Allen, F. e A. Santomero. 1997. The theory of financial intermediation. *The Journal of Banking and Finance* 21(2): 1461–1485 .

BCBS. 2015. Corporate governance principles for banks. <https://www.bis.org/bcbs/publ/d328.pdf>.

Carretta, A., L. Fattobene, E.A. Graziano, e P. Schwizer. 2024. Errors and misbehaviors in banking and finance: a systematic literature review and an integrative framework. *Journal of Management Governance* .

Cocozza, R. 2024a. Fattori critici di successo del risk management: qualche istruzione per l'uso. *Rivista Bancaria Minerva Bancaria* 2024(3): 57 – 84 .

Cocozza, R. 2024b. Risk management, the board and the C-Suite: The adaptive art of communication in times of change. *Journal of Risk Management in Financial Institutions* 2024(18): 14 – 25 .

Cocozza, R. e F. Metelli. 2025. Risk culture & culture risk: not a play on words. *Risk Management Magazine* 21(2): *forthcoming* .

EBA. 2021a. Final report on guidelines on internal governance under directive 2013/36/eu. eba/gl/2021/05. <https://www.eba.europa.eu/sites/default/files/document library/Publications/Guidelines/2021/1016721/Final%20report%20on%20Guidelines%20on%20internal%20governance%20under%20CRD.pdf>.

EBA. 2021b. Final report on guidelines on sound remuneration policies under directive 2013/36/eu. eba/gl/2021/04. <https://www.eba.europa.eu/sites/default/files/document library/Publications/Guidelines/2021/1016720/Draft%20Final%20report%20on%20GL%20on%20remuneration%20policies%20under%20CRD.pdf>.

EBA. 2025. Guidelines on the management of environmental, social and governance (esg) risks. <https://www.eba.europa.eu/sites/default/files/2025-01/fb22982a-d69d-42cc-9d62-1023497ad58a/Final%20Guidelines%20on%20the%20management%20of%20ESG%20risks.pdf>.

ECB. 2016. SSM supervisory statement on governance and risk appetite. https://www.bankingsupervision.europa.eu/ecb/pub/pdf/ssm_supervisory_statement_on_governance_and_risk_appetite_201606.en.pdf.

ECB. 2024. Draft guide on governance and risk culture. https://www.bankingsupervision.europa.eu/framework/legal-framework/public-consultations/pdf/ssm.pubcon202407_draftguide.en.pdf.

FSB. 2014. Guidance on supervisory interaction with financial institutions on risk culture. <https://www.fsb.org/uploads/140407.pdf>.