Risk Culture and Culture Risk: Governance Accountability in the Face of Organizational Misalignment

Rosa Cocozza[1*†] and Fernando Metelli[2†]

[1*]Department of Economics, Management, Institutions, Università degli Studi di Napoli Federico II, Complesso Universitario di Monte S. Angelo, Napoli, 80126, Italy.

[2*]AIFIRM, Associazione Italiana Financial Industry Risk Managers, via Sile 18, Milano, 20139, Italy.

*Corresponding author(s). E-mail(s): rosa.cocozza@unina.it;
Contributing authors: fernando.metelli@aifirm.it.

[†]These authors contributed equally to this work.

Abstract

This paper explores the conceptual and operational distinction between *risk culture*, understood as the set of shared norms and behaviours guiding responsible risk-taking, and *culture risk*, defined as the systemic threat emerging from divergences between declared institutional values and actual practices. Building on regulatory sources including the ECB's 2024 Draft Guide on Governance and Risk Culture, the analysis frames culture risk as a transversal vulnerability with both prudential and reputational consequences. Through a multidisciplinary lens integrating governance theory, behavioural risk, and internal control practices, the paper outlines a holistic framework for mitigating culture risk. The paper also introduces practical mechanisms – such as key cultural indicators and escalation protocols – for embedding a resilient risk culture across governance structures. The mentioned ECB guide represents a significant step in the evolution of supervisory expectations, marking a deliberate shift toward the institutionalization of culture as a critical determinant of prudential soundness and operational integrity. In response to this evolving regulatory landscape, the present work offers a structured reflection on the conceptual underpinnings, governance structures, and operational instruments necessary to embed risk culture and mitigate culture risk. It draws on regulatory guidance from the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS), and the European Banking Authority (EBA), while contextualizing these within the European Single Supervisory Mechanism. By framing risk culture as a governable domain, and culture risk as a transversal threat to institutional stability, the paper aims to support banks, supervisors, and scholars in understanding and implementing the ECB's expectations. It proposes a set of analytical and operational tools, rooted in both theory and best practice, to translate cultural objectives

into durable governance outcomes. The result is a holistic framework that repositions culture as a core element of strategic management and supervisory dialogue.

Keywords: chief risk officer, corporate governance, corporate culture, tone-from-the-top, group-thinking, effective communication, incentives, accountability, business ethics, banking, financial institutions

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

1 Introduction

The integration of risk culture into the European regulatory and supervisory landscape has emerged incrementally over the last two decades, driven by both episodic financial crises and the progressive formalization of prudential norms. The 2007–2009 global financial crisis served as a critical inflection point, revealing widespread failures in risk governance and leading to the recognition that deficiencies in organizational culture could pose systemic threats to financial stability. As a response, the FSB and the BCBS elevated risk culture to a central theme within their respective regulatory agendas. In its 2014 *Guidance on Supervisory Interaction with Financial Institutions on Risk Culture*, the FSB emphasized the role of governance structures, behavioural indicators, and cultural alignment in shaping risk-sensitive decision-making. The BCBS's 2015 *Corporate Governance Principles for Banks* codified the expectation that banks adopt governance frameworks explicitly attuned to cultural effectiveness. At the European level, these developments were echoed and expanded through the EBA Guidelines, mainly the Guidelines on internal governance under Directive 2013/36/EU (EBA, 2021a), which establishes binding obligations for internal governance, including requirements on board composition, risk appetite articulation, and the integration of risk considerations in strategic planning. National transpositions are expected to be integrated for cultural drivers, tone from the top, and behavioural accountability.

Drawing on regulatory developments from the FSB, the BCBS, the EBA and the European Central Bank (ECB), the study frames risk culture as a strategic asset, outlining the ECB four foundational pillars: tone from the top, effective communication and challenge, accountability, and aligned incentives. We examined the topic in relation to structural governance models, organizational behaviour, and proportional adaptation.

We emphasize that risk culture must be embedded at every level, strategic, operational, and behavioural, and supported by governance tools such as cultural Key Performance Indicators (KPIs), Key Risk Indicators (KRIs), escalation protocols, internal reporting systems, and training programs. It further explores how control functions, particularly the Chief Risk Officer (CRO), play a central role in sustaining cultural integrity across risk management processes (AIFIRM, 2025). Recognizing that institutions vary in size and complexity, we advocate for a proportional but uncompromising approach: cultural expectations should be adapted, not diluted.

Culture risk is presented as dynamic and measurable, with data governance and diagnostic tools enabling continuous refinement and supervisory engagement.

The classification of culture risk within the broader architecture of governance risk, as articulated by the EBA in its ESG Guidelines (EBA, 2021a), further affirms its regulatory materiality. Although not always explicitly named, culture risk resides conceptually at the intersection of leadership deficiencies, ethical shortfalls, and inadequate managerial practices. These shortcomings pose direct threats to financial soundness and are therefore subject to supervisory scrutiny under the 'G' pillar of ESG as directly applied to financial intermediaries.

In conclusion, we argue that culture risk constitutes a root vulnerability within financial systems. Mitigating it requires coordinated action from governance bodies, management, and regulators alike. Presumptively, institutions that elevate cultural maturity as a strategic priority will be best positioned to achieve long-term resilience and retain the trust of clients, investors, and supervisors.

The paper articulates a comprehensive framework for understanding, measuring, and governing risk culture and culture risk within financial institutions. It distinguishes between risk culture, the shared norms and behaviours guiding risk-aware decisionmaking, and culture risk, the threat arising from misalignments between stated values and actual conduct (Cocozza and Metelli, 2025).

The remainder of this article is organised as follows. Section 2 establishes the conceptual groundwork by distinguishing between risk culture and culture risk, and by explaining how corporate governance functions as a mechanism of cultural anchoring. Section 3 surveys the evolving European regulatory landscape, analyses alternative governance models, and develops the ECB's four-pillar framework(tone from the top, communication and challenge, accountability, and incentives) before identifying the principal organisational and behavioural drivers of culture risk and discussing the doctrine of 'reverse proportionality' for Less Significant Institutions (LSIs). Section 4 translates these insights into practice, detailing the roles of key governance actors, the tool-kit of cultural KPIs/KRIs, and the integration of cultural considerations into risk-management processes, data-governance frameworks and escalation protocols. Section 5 concludes by distilling policy recommendations and outlining an agenda for continuous supervisory dialogue and scholarly inquiry.

2 Conceptual Foundations and Framing Perspectives

2.1 Defining the Dialectic: Risk Culture versus Culture Risk

Financial institutions operate in an environment characterized by intrinsic exposure to uncertainty, where the management of risk is not merely a regulatory necessity but an integral dimension of strategic leadership (Allen and Santomero, 1997). Risk culture and culture risk represent two conceptually distinct, yet interdependent, constructs within this domain.

Risk culture denotes the shared values, attitudes, competencies, and behavioural norms that shape how risk is understood, communicated, and managed within an

organization. It manifests in the day-to-day actions of staff and executives, embedding itself in strategic decision-making, capital allocation, and operational choices. A robust risk culture acts as an internal compass, aligning conduct with long-term institutional sustainability and regulatory expectations. As emphasized by regulators (FSB (2014); BCBS (2015)), risk culture is foundational to effective governance and resilience.

In contrast, culture risk emerges when there is a misalignment between a firm's espoused values and the actual behaviours practised throughout the organization. This misalignment can lead to ethical lapses, operational inefficiencies, or reputational erosion, which in turn threaten both prudential soundness and societal legitimacy. Culture risk, therefore, should be understood as the risk that originates from deficiencies in cultivating a coherent and ethical institutional culture. Its symptoms include the erosion of accountability, breakdowns in communication, and the presence of incentives misaligned with prudent conduct. Crucially, the absence of a mature risk culture is itself a vector for culture risk (AIFIRM, 2025). This recursive relationship highlights why supervisory authorities now view culture risk not as an abstract ideal but as a material risk deserving structured governance, systematic monitoring, and targeted mitigation. In this light, the *Draft Guide on Governance and Risk Culture* (ECB, 2024) underscores the need for banks to articulate, operationalize, and measure risk culture as a strategic asset, rather than an intangible ethos.

The distinction between these two concepts is more than semantic. It delineates the boundary between proactive and reactive governance. Whereas risk culture seeks to instil values before misbehaviour occurs, culture risk requires mechanisms for detecting and correcting deviations once they arise. Thus, any institution that fails to invest in the former will inevitably confront the latter, often at significant cost.

We contend that addressing culture risk requires more than rhetorical commitment; it demands a coherent framework, grounded in governance architecture and reinforced by performance systems. In particular, it necessitates a systematic evaluation of the institutions' tone from the top, the coherence of internal communication channels, the credibility of incentives, and the effectiveness of accountability mechanisms. Corporate governance can anchor such a framework and mitigate culture risk at its source.

2.2 Governance as a Mechanism of Cultural Anchoring

Corporate governance, in its most rigorous formulation, is the institutional infrastructure by which authority, accountability, and decision-making are distributed within a firm. Within the financial sector, this infrastructure is not merely instrumental to regulatory compliance, but foundational to risk management and strategic orientation. The governance of financial institutions must not only ensure procedural robustness but also enable the internalization of risk-aware conduct across all organizational levels, representing a mechanism of cultural anchoring. As the ECB and the BCBS have increasingly emphasized, sound governance is a prerequisite for an effective risk culture. Indeed, the governance framework constitutes the architecture within which cultural values are formalized, communicated, and enforced. The board of directors, as the highest decision-making authority, bears primary responsibility for

establishing and maintaining an ethical and prudent culture. This is operationalized through strategic alignment, committee oversight, and structural safeguards such as the independence of internal control functions (AIFIRM, 2024).

Contemporary supervisory expectations articulate the board's role not only in defining the institution's risk appetite, but also in ensuring its embedding across operational, technological, and behavioural domains. This encompasses the design of incentive systems, the monitoring of cultural indicators, and the assessment of leadership credibility. Equally, the senior management team, under the board's direction, must serve as cultural transmitters, articulating a consistent tone from the top and ensuring congruence between values and actions. Furthermore, the three-lines-of-defence model plays a crucial role in anchoring cultural expectations within institutional processes. Risk management, compliance, and internal audit must each operate with independence, competence, and an explicit mandate to monitor cultural coherence. Notably, the CRO serves as a linchpin, linking strategic governance with operational execution; accordingly, the CRO's authority must be buttressed by structural empowerment and direct access to the board.

Importantly, governance must also accommodate the principle of proportionality. Smaller institutions may require tailored approaches, but this does not diminish the need for cultural rigour. On the contrary, the risks associated with informal governance practices and concentrated decision-making in LSIs necessitate a heightened cultural sensitivity. Therefore, governance is the operational substrate of risk culture. It provides the channels through which culture is translated into action, and it establishes the checks through which deviations are detected and corrected. As such, any institution seeking to mitigate culture risk must begin with an honest appraisal of its governance effectiveness.

3 Governance, Regulation, and Risk Culture Infrastructure

3.1 Governance Models and Cultural Dynamics in Banking Institutions

Within the European banking system, historical and regulatory evolution shaped the current expectations regarding culture and governance in European financial supervision. Institutional governance structures serve not only as formal mechanisms for corporate control but also as vehicles for cultural transmission and ethical alignment. The design and functioning of governance models, whether traditional, monistic, or dualistic, bear directly on an institution's ability to embed a coherent risk culture and mitigate the emergence of culture risk.

The traditional governance model, predominant in Italy and other civil law jurisdictions, is characterized by a separation between the Board of Directors, responsible for strategic supervision and business decisions, and the Board of Statutory Auditors, which oversees compliance and control. This separation ensures a clear

distinction between executive and monitoring functions, enhancing the robustness of checks and balances. In the monistic model, the governance framework is unified within a single board, which includes an internal control committee composed of independent directors with specific professional qualifications. This model emphasizes flexibility and efficiency but may require stronger safeguards to prevent conflicts of interest and ensure effective oversight. The dualistic model, in contrast, establishes a clear structural division between a Management Board and a Supervisory Board. The latter not only performs traditional monitoring functions but also assumes some specific responsibilities, such as appointing members of the board itself. This structure, while less common, may enhance accountability and strategic focus, particularly in complex or group-based banking institutions.

Irrespective of structural variation, all governance models must address the cultural dimension of financial intermediation. This involves fostering a shared understanding of risk, promoting behavioural standards that align with long-term value creation, and embedding risk-sensitive thinking into all levels of decision-making. Cultural governance, therefore, is not confined to formal statutes or board configurations but must be continually reinforced through practice, evaluation, and leadership example. Moreover, evolving supervisory expectations have brought increasing attention to board composition, diversity of perspectives, and the collective suitability of directors. A diverse board, by gender, expertise, and generational background, has been shown to reduce the incidence of group-thinking and promote more robust, ethically grounded decision-making. The presence of directors with substantive experience in Environmental, Social, and Governance (ESG) and Information and Communication Technology (ICT) domains is increasingly considered essential, not only for compliance purposes but as a safeguard for reputational and strategic integrity.

In sum, governance models are more than institutional templates; they are frameworks for cultural legitimacy and behavioural alignment. To the extent that governance fosters transparency, inclusiveness, and strategic resilience, it acts as a primary defence against the insidious emergence of culture risk. The next section turns to the regulatory and supervisory developments that have progressively shaped this paradigm.

3.2 The Four Pillars of Risk Culture: From Tone to Incentives

The EBA has deepened its focus on cultural matters, issuing guidelines on internal governance (EBA, 2021a) and sound remuneration policies (EBA, 2021b), both of which frame risk culture as a prerequisite for sustainable performance and regulatory compliance. These guidelines underscore the interdependence between cultural awareness, individual accountability, and institutional resilience. The publication of the *Draft Guide on Governance and Risk Culture*(ECB, 2024) represents a conceptual and operational consolidation of these strands. As stated, it proposes a set of supervisory expectations for assessing governance quality and cultural soundness, grounded in four principal dimensions: tone from the top and leadership credibility; effective

communication, challenge, and diversity; accountability for risk conduct; incentives aligned with prudent behaviour.

Notably, the guide introduces 'red flags' for governance and cultural dysfunctions, offering a diagnostic apparatus for supervisory engagement. This evolution marks a paradigmatic shift from procedural compliance to cultural assurance (Cocozza, 2024a). Regulators now view cultural integrity not as a desirable supplement to risk governance but as its operational core. Institutions are therefore expected to institutionalize cultural diagnostics, embed cultural objectives in performance evaluations, and demonstrate proactive risk conduct at all levels. As a matter of fact, the regulatory trajectory of the last decade reflects a growing consensus that financial stability hinges not only on capital adequacy and liquidity ratios but equally on the ethical architecture and behavioural integrity of financial institutions. These expectations are internalized through the four foundational pillars of risk culture, each of which reflects a critical domain of organizational behaviour. These dimensions are central not only to embedding risk consciousness but also to creating a governance infrastructure that is resilient to cultural misalignments.

1. *Tone from the Top and Leadership Credibility*. The values and priorities articulated, and embodied, by senior leadership define the epistemic and ethical boundaries of organizational behaviour. The board of directors and executive management must not only declare commitment to risk-sensitive behaviour but exemplify it through consistent actions. Tone from the top is not a rhetorical artefact; it is a strategic determinant of conduct, cascading downward through every layer of the institution. Effective leadership is evidenced by clarity of message, visibility of ethical stance, and congruence between strategic objectives and behavioural expectations. Empirical studies have shown that leadership inconsistency or opacity contributes significantly to culture risk, as it fosters cynicism, ambiguity, and rationalization of misconduct . Conversely, when leaders demonstrate humility, openness to challenge, and personal accountability, they establish a normative reference point that legitimises prudent decision-making and ethical restraint (Carretta et al., 2024).
2. *Communication, Challenge, and Diversity*. Open, multidirectional communication is a precondition for cultural integrity. Risk culture thrives in environments where staff are encouraged to raise concerns, question assumptions, and express dissent without fear of reprisal. Institutions must establish both formal channels, such as escalation mechanisms and whistleblowing platforms, and informal norms that foster psychological safety and constructive dialogue (Cocozza, 2024b). Diversity of thought, background, expertise, and experience enhances this communicative function. Diverse teams are more likely to interrogate consensus, resist groupthink, and anticipate risk from multiple vantage points. Regulatory expectations increasingly underscore the importance of diversity in board composition, managerial structures, and project governance as a mechanism for enhancing cultural vigilance and robustness.
3. *Accountability for Risk Conduct*. A credible risk culture requires that responsibilities are clearly defined and that behavioural outcomes are traceable to decision-making

nodes. Institutions must institutionalize systems of individual and collective accountability, ensuring that risk-related decisions, whether in lending, trading, IT security, or product design, can be evaluated ex post for adherence to policy and ethical expectations. Accountability also entails disciplinary clarity. Institutions must avoid both impunity and scapegoating, cultivating a culture where mistakes are addressed proportionately and constructively, but misconduct
is sanctioned decisively. Regulators (ECB (2016); ECB (2024); EBA (2021a)) guidance consistently emphasize the centrality of role clarity, transparent consequences, and feedback loops as markers of a functioning culture of responsibility.

4. *Incentives Aligned with Prudence and Sustainability*. Incentive structures are the behavioural levers through which culture is translated into practice. When performance metrics prioritize short-term profit without regard for risk exposure, the resulting culture is one of moral hazard and erosion of control integrity. Accordingly, regulators now require that remuneration frameworks integrate risk-adjusted metrics and sustainability indicators. *Ex ante*, variable compensation should be contingent on ethical compliance, adherence to risk policies, and contribution to long-term strategic objectives. *Ex post*, *malus* and clawback provisions should be operationalized to address adverse outcomes that stem from negligent or reckless behaviour. Moreover, non-financial incentives, such as recognition, career progression, and learning opportunities, should also be aligned with cultural performance, reinforcing ethical and collaborative norms.

These four pillars, when considered collectively, do not operate independently of one another. They interact as a system, where weaknesses in one domain, such as poor communication or ambiguous incentives, can undermine the integrity of the whole. Institutions committed to fostering a resilient risk culture must therefore assess, calibrate, and integrate all four dimensions within their governance frameworks. The next section explores how these pillars inform the identification of culture risk drivers across organizational subsystems.

3.3 Culture Risk Drivers: Organizational Behaviour and Structural Gaps

Understanding the drivers of culture risk requires an analytical lens that integrates structural, behavioural, and contextual variables. Culture risk does not arise spontaneously; it is incubated by organizational conditions that either permit or fail to correct misalignments between declared institutional values and everyday conduct. These conditions manifest across three principal dimensions: organizational behaviours, structural design, and systemic blind spots.

1. *Organizational Behaviours and Norms*. Culture risk often finds fertile ground in environments marked by behavioural drift, wherein informal norms diverge from formal expectations. When risk-taking is normalized without commensurate oversight, or when boundary-pushing is tacitly rewarded, institutions create what has been termed a 'permissive context' for cultural deviance. These environments are

characterized by weak challenge cultures, diluted ethical anchors, and the erosion of internal accountability. Such behaviours are often self-reinforcing. Once a culture of silence, indifference, or rationalization takes root, it becomes increasingly difficult to re-establish ethical discipline. This dynamic is compounded in high-pressure environments, such as front-office trading, aggressive sales cultures, or tech-driven innovation hubs, where performance incentives can eclipse governance boundaries.

2. *Structural Design and Governance Architecture*. Organizational form can also act as a driver of culture risk. Centralized hierarchies with poor information flows often suppress dissent and isolate decision-making. Conversely, overly fragmented structures may impede coherent oversight and allow cultural inconsistencies to proliferate across business lines, geographies, or legal entities. Risk is particularly pronounced in governance models where lines of accountability are ambiguous, where the separation of duties is ill-defined, or where control functions are structurally subordinated to business objectives. The lack of direct escalation paths to independent control bodies, especially for compliance and risk management, can obstruct the timely detection of cultural breaches. Moreover, inadequate board composition and insufficient expertise in emerging areas such as ESG and digital risk governance can result in superficial scrutiny of conduct-related risks. A board ill-equipped to interpret cultural indicators or assess their strategic implications may inadvertently exacerbate exposure to reputational and operational failures.
3. *Systemic Blind Spots and Feedback Deficiencies*. Beyond internal structures, culture risk is also driven by cognitive and procedural blind spots. Institutions that fail to gather and act upon feedback—whether from employees, customers, or control functions—create an asymmetry between perceived and actual culture. This dissonance can mask critical vulnerabilities until they materialize as scandals or supervisory interventions. Red flags include the absence of whistleblowing reports, lack of upward feedback channels, low engagement scores in staff surveys, or recurring audit findings related to behavioural anomalies. When such indicators are ignored or rationalized, the institution forfeits its opportunity for cultural course correction.

As previously noted regarding the four pillars of risk culture (§ 3.2), culture risk drivers are rarely isolated. They often form an ecosystem of dysfunctions, where weaknesses in governance, behavioural incentives, and communication reinforce each other. It is therefore imperative that institutions adopt an integrated diagnostic framework capable of capturing cultural fragility at both the micro and macro levels.

3.4 Proportionality and Contextualization of Cultural Governance

The effective implementation of cultural governance within financial institutions requires tailoring to the specific context in which each entity operates. The principle of proportionality, long embedded in European regulatory discourse, mandates that governance structures, control functions, and risk culture frameworks be calibrated to an institution's size, complexity, systemic relevance, and business model. However,

proportionality must not be misconstrued as an argument for leniency. Rather, it entails the intelligent adaptation of governance expectations so that institutions of varying profiles – whether Global Systemically Important Banks (G-SIBs), LSIs, or fintech oriented entrants – can internalize cultural imperatives in a manner that is meaningful and operationally feasible.

For larger or more complex entities, proportionality implies more formalized governance processes, detailed cultural diagnostics, and robust performance-linked indicators of risk awareness and behavioural conduct. These institutions are expected to establish multi-tiered governance bodies, maintain strong internal audit independence, and document cultural initiatives across business lines and geographies. Conversely, for smaller or less complex banks, cultural governance must be no less rigorous, but its implementation may be less bureaucratic. LSIs, for example, may adopt simplified cultural metrics, fewer formal committees, and more direct leadership engagement. What they cannot afford, however, is cultural informality or reliance on personality-driven leadership at the expense of institutional resilience. A frequent misapplication of proportionality is the assumption that cultural risk is less material in small or specialized entities. As a matter of fact, the supervisory principle of proportionality is frequently misconstrued as a licence for simplification in LSIs. In fact, such institutions may be more vulnerable due to concentrated power structures, informal governance practices, or lack of cultural awareness. Proportionality must not become a pretext for neglect. Instead, it should serve as an enabler of relevance, ensuring that cultural governance mechanisms are appropriate, agile, and strategically embedded. Accordingly, within the cultural sphere, proportionality operates in reverse. Precisely because LSIs operate with leaner governance structures, concentrated decision-making and limited internal-control resources, they are more prone to culture risk and therefore require greater vigilance rather than procedural relaxation. In fact, such institutions may be more vulnerable due to concentrated power structures, informal governance practices, or lack of cultural awareness. Proportionality must not become a pretext for neglect. Instead, it should serve as an enabler of relevance, ensuring that cultural governance mechanisms are appropriate, agile, and strategically embedded. The ECB (2024, 4) explicitly states that *good governance and sound risk culture are equally important for all banks, whatever their size*, and that proportionality must never compromise the substance of cultural safeguards. The very traits that typify smaller institutions (tight hierarchies, dominant personalities, geographic or sectoral concentration) magnify the impact of behavioural failings, prompting what we identify as reverse proportionality referring to an 'inversion of the principle of proportionality' whereby heightened supervisory attention is warranted for LSIs. Consistently, on the one hand the ESG-risk guidelines (EBA, 2021a) reject size as a sufficient basis for lighter treatment, warning that smaller banks 'are not necessarily less exposed' and may, by virtue of portfolio concentration, face amplified governance threats that demand robust, albeit not unnecessarily complex, controls. On the other hand, from the standpoint of positive law alone ought to be construed as a matter of qualitative customisation rather than quantitative dilution: fewer layers of bureaucracy do not entitle an institution to fewer cultural defences, but oblige it to adopt bespoke, high-granularity indicators and

more direct board oversight to compensate for structural fragilities. In practical terms, this means LSIs must deploy sharper whistle-blowing channels, maintain a surplus of independent challenge in board composition, and hard-wire culture-sensitive KPIs/KRIs into business-line dashboards tools that, while less bureaucratic, are more exacting in their scrutiny of conduct. Thus, reverse proportionality recognises that cultural complacency carries a proportionally higher systemic cost for LSIs, and supervisory expectations are expected to rise rather than recede accordingly.

Proportionality also requires alignment with the institution's business model. For retail banks with extensive customer interfaces, culture risk may manifest through frontline misconduct or misselling practices. For investment banks, it may stem from trader behaviour and incentive misalignment. For fintechs, rapid innovation cycles and horizontal hierarchies may generate culture risk from speed-driven decision-making and blurred accountability. Thus, cultural governance must be contextualized to the risk landscape intrinsic to the institution's operations. Institutions with a cross-border footprint must also address jurisdictional variations in cultural expectations, legal frameworks, and regulatory scrutiny—requiring cultural cohesion without enforcing cultural uniformity.

Control functions must also be scaled and equipped commensurately with the institution's actual degree of risk culture. Any institutions must ensure independent control, integrity of reporting lines, and cultural oversight. The key is functional sufficiency rather than structural replication, since control functions are required to be properly effective and not merely efficient. Cultural indicators, such as engagement surveys, incident reports, whistleblower activity, and KRI/KPI integration, should be deployed based on institutional maturity. High-frequency metrics may be essential in fast-moving environments, while narrative reviews and periodic pulse checks may suffice in more stable, relationship-based institutions.

Ultimately, a proportional approach to risk culture entails dynamic calibration: recognizing that institutions evolve, risks shift, and governance must adapt accordingly. Supervisory assessments, likewise, should reflect this dynamism—evaluating not only formal compliance but the cultural coherence and resilience of governance systems.

4 Executive Overview and Synthesis of Key Insights

4.1 Governance Actors in Cultural Oversight

The institutionalization of risk culture relies fundamentally on the actors tasked with its governance. Boards of directors, board-level committees, executive management, and the control functions each serve distinct yet interdependent roles in reinforcing a culture aligned with prudent risk-taking, regulatory integrity, and ethical conduct. This section maps their respective responsibilities, emphasizing the mechanisms through which culture is shaped, monitored, and corrected. In an attempt to outline a functional mapping of the various actors within the organisational structure of the financial institution, the following roles can be specified: Board of directors; board-level Committees; executive management; control function and organizational support.

1. *The Board of directors: Strategic Stewards of Culture*. The board of directors bears ultimate responsibility for shaping the institution's risk culture. This includes defining the tone from the top, approving the risk appetite framework (RAF), overseeing cultural indicators, and ensuring that senior leadership acts in accordance with declared values. Board members must collectively possess expertise not only in banking and finance but also in organizational behaviour, ESG concerns, and ICT governance. The diversity and independence of board composition are critical to avoid monocultural thinking and to foster challenge. Furthermore, boards should engage directly with risk and audit committees to review internal cultural diagnostics and ensure continuous improvement in ethical and control environments.
2. *Board-Level Committees: Anchors of Oversight*. Within the board, specialized committees play a key role in translating governance principles into structured oversight. The risk committee is typically tasked with reviewing the institution's risk profile, including culture-related risks, and advising on the alignment between strategy and cultural resilience. The audit committee provides assurance over the effectiveness of internal controls, including those that relate to behavioural compliance, tone from the top, and response to whistleblower concerns. In some governance models, an ethics or conduct committee may be convened to oversee integrity-related frameworks, particularly in institutions with elevated reputational exposure.
3. *Executive Management: Translators of Governance into Practice*. Executive leadership, including the CEO and C-suite officers, are the primary agents of cultural transmission. Their role extends beyond operational execution to include reinforcing strategic messages, exemplifying ethical standards, and holding teams accountable for behavioural performance. As said, the CRO functions as the linchpin between governance and operations. The CRO should have direct access to the board, independence from commercial pressures, and a mandate that includes oversight of cultural risks. Collaboration between the CRO, Chief Financial Officer (CFO), Chief Human Resources Officer (CHRO), and compliance leads is essential to ensure the alignment of control, financial sustainability, and organizational values.
4. *Control Functions: The Lines of Defence for Culture*. The risk management, compliance, and internal audit functions collectively underpin the institution's defence against culture risk. Each function contributes in distinct temporal and procedural dimensions: Risk Management operates in both ex ante and real-time capacities, identifying and assessing emerging culture risks, advising on mitigation strategies, and integrating cultural metrics into the broader RAF; Compliance ensures that internal policies align with regulatory and ethical standards, monitors behavioural adherence, and oversees training, conduct reporting, and disciplinary processes; Internal Audit serves as an ex post assurance mechanism, independently evaluating whether cultural expectations are embedded in decision-making, control practices, and organizational norms. Critically, these functions must operate with sufficient stature, independence, and resourcing. Structural subordination to business lines or inconsistent reporting lines can undermine their credibility and effectiveness. An empowered second and third line is a prerequisite for cultural accountability.

5. *Organizational Support and Human Resources*. While not formally classified as control functions, Human Resources (HR) and organizational development teams play a central role in embedding risk culture. From recruitment and onboarding to performance evaluation and leadership succession, these functions influence the values and attitudes brought into the institution and reinforced through daily work. Training programs, career incentives, and staff engagement initiatives should be explicitly aligned with risk culture objectives. Where culture risk is detected, HR must act as a partner in remediation adjusting policies, reinforcing expectations, and providing developmental feedback.

Together, these actors compose a cultural governance ecosystem. Their effectiveness depends not only on mandate clarity and technical competence, but also on mutual trust, transparency, and an institutional willingness to interrogate behaviours before they metastasize into systemic risks.

4.2 Governance Tools to Institutionalize Risk Culture

To embed and sustain a risk-aware culture, institutions must deploy an integrated set of tools that translate cultural intent into operational and measurable practice. These tools support the monitoring, reinforcement, and continuous refinement of cultural expectations across governance and business functions. They span performance measurement, internal reporting systems, escalation protocols, and cultural diagnostics.

1. *Cultural KPIs and KRIs: Aligning Performance and Risk Behaviour*. KPIs and KRIs are foundational instruments for tracking the alignment between cultural objectives and actual behaviour. KPIs should reflect not only financial or operational targets but also cultural benchmarks—such as employee engagement, incident reporting frequency, training completion rates, or conduct ratings from 360-degree reviews. KRIs, by contrast, offer early warning signals for emerging culture risks. They may include metrics such as turnover in control functions, spikes in compliance breaches, delayed issue remediation, or anomalies in incentive-linked behaviours. A coherent framework should link KPIs and KRIs to ensure that performance objectives do not undermine risk-conscious conduct. To maximize their efficacy, these indicators should be: relevant to the institution's strategic and risk profile; quantifiable where possible, but inclusive of qualitative assessments (e.g., behavioural audits); timely, allowing proactive responses to emerging risks and operationalized through dashboards accessible to both control and executive functions.
2. *Reporting Systems and Cultural Transparency*. Transparent, reliable, and bidirectional reporting systems are critical to effective cultural governance. Institutions should establish formal communication channels, such as risk culture reports, conduct dashboards, and culture-related heatmaps, that are periodically reviewed by risk committees, senior management, and internal audit. Cultural data should be embedded in enterprise risk reports and included as a regular topic in management committee agendas. In turn, leadership must close the loop by providing feedback on

reported issues and highlighting institutional responses, thus reinforcing the utility of reporting mechanisms.

3. *Escalation Protocols and Whistleblowing Frameworks*. The ability to escalate cultural concerns is a litmus test of an institution's behavioural integrity. Escalation protocols must be clear, confidential, and accessible, supported by formal whistleblowing channels that are actively monitored, protected against retaliation, and subject to periodic review. Staff must be trained in how and when to escalate issues, and data from escalation logs should be analysed for trends. Low levels of whistleblowing activity, in isolation, should not be interpreted as cultural health, particularly if other indicators – such as employee surveys – suggest fear or cynicism.
4. *Training, Induction, and Continuous Development*. Training programs must be designed not only to convey technical knowledge but to socialize risk culture values. Induction programs for new hires, particularly in risk-sensitive roles, should include exposure to the institution's cultural expectations, conduct case studies, and mentoring by cultural exemplars. Ongoing development opportunities – such as workshops, scenario analysis, and behavioural simulations – can reinforce culture across tenure levels. Ideally, training effectiveness should be measured not just by attendance but by shifts in reported attitudes, conduct metrics, or peer feedback.
5. *Cultural Audits and Self-Assessments*. Periodic culture audits, whether internal or facilitated by third parties, provide a structured means of assessing cultural alignment. These reviews should cover behavioural trends, organizational norms, incident case reviews, and the perceived integrity of leadership messaging. Self-assessment tools – such as culture pulse surveys, qualitative interviews, and risk attitude diagnostics – can supplement more formal audits. Results should feed into risk appetite adjustments, policy redesign, and performance management frameworks.

When implemented holistically, these governance tools transform risk culture from a rhetorical aspiration into an detectable, managed, and continuously improving institutional reality.

4.3 Operational Dimensions: Integrating Risk Culture into Risk Management Frameworks

A genuinely resilient risk culture can be sustained only when the abstract commitments articulated by the board are translated seamlessly into the quotidian routines of the institution's risk-management architecture, ranging from the earliest stage of risk identification to the final act of escalation.

At the identification stage, banks must widen the aperture of traditional risk scanning to capture behavioural and cultural fragilities, embedding qualitative diagnostics of weak control disciplines, inconsistent leadership signals and employee disengagement within enterprise-wide assessments, incident reviews and scenario analyses that expressly account for human fallibility and the normalisation of deviance. Comprehensive risk identification extends beyond the cataloguing of financial or

strategic exposures and must encompass behavioural and cultural vulnerabilities. Financial institutions should therefore design diagnostic frameworks capable of detecting incipient cultural erosion, manifested, *inter alia*, in attenuated control disciplines, contradictory leadership messaging or rising employee disengagement. These cultural diagnostics ought to be embedded within enterprise-wide risk assessments, post-incident reviews and root-cause analyses. Scenario analyses must likewise incorporate behavioural vectors, acknowledging that crises frequently originate not in technical malfunction but in systematic misjudgement, ethical default or the gradual normalisation of deviance.

The Risk-Appetite Statement constitutes the documentary – and, in a sense, even forensic – keystone of contemporary risk governance and, as such, it operates as a cultural covenant: drafted and periodically refreshed by the board, the CRO and senior management, it must couple quantitative thresholds with clearly articulated behavioural tolerances, thereby binding ethical expectations to strategic resource allocation and cascading those expectations through incentive schemes, policy frameworks and business plans. To serve as a credible instrument of cultural alignment, the Risk Appetite Statement (RAS) should articulate explicit thresholds for cultural and ethical risk, define expected standards of integrity and embed core organisational values into all risk-related decision paths. The drafting and periodic revision of the RAS demand the concerted engagement of the board, the CRO and senior management, thereby conferring institutional legitimacy. Once approved, the RAS must be promulgated throughout the organisation, with clear linkages to remuneration architecture, policy frameworks and strategic planning cycles.

Once articulated, cultural objectives must be rendered observable through the careful fusion of KPIs and KRIs – leading metrics such as training-completion or 'tone-from-the-top' scores situated alongside lagging indicators like compliance breaches or customer redress – so that dashboards reviewed in performance dialogues illuminate the nexus between conduct and enterprise value. KPIs and KRIs must be operationalised at business-unit granularity, uploaded to management dashboards and interrogated in tandem with individual performance and conduct evaluations. Such alignment mitigates the risk of metric myopia, whereby financial incentives eclipse ethical considerations, and preserves an appropriate risk-reward calculus. Robust frameworks connect leading indicators (e.g. completion rates for ethics training, 'tone-from-the-top' pulse-survey scores) with lagging indicators (e.g. substantiated compliance breaches, customer redress payments). The resulting data should inform both tactical interventions and the strategic recalibration of risk appetite.

Continuous surveillance of those metrics requires a hybrid toolbox in which traditional control testing is enriched by behavioural analytics, whistle-blowing data and sentiment tracking, all governed by predetermined escalation triggers that elevate emergent cultural anomalies to an executive forum or a dedicated culture committee. Risk-culture surveillance necessitates a hybrid toolkit that marries quantitative analytics with qualitative intelligence. In addition to traditional control testing and audit procedures, institutions should harvest behavioural data – such as whistle-blowing volumes, staff-survey sentiment and incident-reporting trends – to gauge cultural health.

Escalation protocols must be codified within the risk-management framework, stipulating objective thresholds that trigger independent review or remedial action. Many institutions have found it prudent to constitute a dedicated Culture Escalation Committee or, at minimum, to elevate cultural matters to a standing agenda item of the executive risk committee.

In this ecosystem, the CRO assumes a pivotal integrative role: empowered with unmediated access to the board, the CRO champions cultural metrics, challenges deviations and ensures that every strategic initiative is scrutinised for its cultural externalities, all while modelling ethical leadership in practice. Finally, robust data governance protocols, embracing integrity, transparency and proportional privacy safeguards, provide the informational substrate on which cultural assurance depends, enabling advanced analytics to correlate conduct patterns with risk outcomes and to surface vulnerabilities across business lines and geographies. The CRO is uniquely situated to fuse cultural oversight with orthodox risk governance. Beyond championing cultural metrics and challenging deviations, the CRO must advise on the cultural ramifications of strategic initiatives and capital allocations. Functionally, the CRO operates as the principal interlocutor between the second and third lines of defence and commercial units, ensuring that cultural risk is subjected to the same analytical rigour as market, credit or liquidity risk.

Efficacy in this role presupposes both institutional empowerment, that is to say direct and unmediated access to the board, and personal exemplarity in ethical leadership. Data integrity, transparency and accessibility are sine qua non for credible cultural governance. Institutions should therefore adopt comprehensive data-governance policies that facilitate the systematic collection, validation and analysis of cultural indicators, ranging from training logs and ethics-hotline activity to performance deviations and structured exit interviews. Advanced analytics (including machine-learning classification and network-analysis techniques) may be deployed to surface emergent patterns, correlate cultural indicators with adverse outcomes and segment insights across organisational strata. Such deployment must, however, respect the proportionality principle and comply with applicable privacy and surveillance laws, particularly where predictive behavioural modelling is involved.

When these elements cohere, risk culture ceases to be a rhetorical aspiration and becomes a hardwired dimension of enterprise-risk management, fortifying the institution's legal, prudential and ethical immunity in a progressively complex supervisory landscape. When effectively operationalised, the foregoing practices ensure that risk culture is not relegated to the periphery of reputational discourse but rather constitutes an integral stratum of the enterprise-risk management edifice. The concluding chapter synthesises the doctrinal and operational insights offered herein and proposes a forward-looking research agenda for the continual refinement of cultural governance amid accelerated regulatory, societal and technological evolution. When operationalized effectively, these practices ensure that culture is not relegated to the margins of compliance or reputational risk but is instead embedded within the core architecture of enterprise risk management. The final chapter offers conclusions and

strategic recommendations for sustaining and evolving cultural governance in light of ongoing regulatory, societal, and technological change.

5 Conclusion

This article has explored, from a doctrinal and managerial vantage-point, the conceptual bases, governance arrangements, operational mechanics and supervisory expectations that shape the cultivation of a sound risk culture and the attenuation of culture-related risk within credit institutions. The analysis supports some principal propositions, which could be seen as seminal guidelines for the management of culture risk.

Risk culture constitutes a strategic asset rather than a peripheral 'soft' concern; it conditions decision-making, moulds behavioural incentives and ultimately frames the institution's risk-return equation and must therefore be accorded evidentiary weight equal to that of traditional financial metrics in both strategic planning and performance appraisal. FIs must treat risk culture not as a compliance adjunct or reputational safeguard, but as a core determinant of institutional sustainability.

Cultural stewardship is a function of governance architecture and example: boards and C-level executives must translate rhetoric into conduct, preserve the independence of control functions and embed cultural vigilance as an explicit, non-delegable board mandate, recognising that leadership credibility is the *sine qua non* of cultural resilience.

While risk culture is not, in itself, amenable to direct measurement, culture risk most certainly is. Consequently, culture risk is also monitorable and mitigable. It is neither elusive nor unquantifiable; it should be identified, measured and managed through integrated KPI/KRI systems that capture behavioural signals, incident trends and whistle-blower intelligence, supported by pre-defined escalation triggers and subjected to periodic stress-testing within enterprise-wide risk assessments. Therefore, cultural diagnostics should become a routine component of enterprise risk assessments.

The principle of proportionality demands intelligent customisation, not attenuation: smaller or less complex institutions cannot invoke scale as a justification for cultural minimalism; rather, they must adopt tailored, but no less rigorous, mechanisms commensurate with their heightened exposure to governance fragility, while supervisory scrutiny remain equally exacting across LSIs, fintech entrants and legacy banks.

Responsible data governance is both a prerequisite and a proving ground for cultural integrity; institutions must invest in secure, transparent infrastructures capable of harvesting and analysing cultural data, ranging from sentiment analytics to behavioural patterning, while ensuring strict compliance with privacy and ethical standards.

Cultural governance is a dynamic enterprise: it must evolve in step with leadership transitions, strategic realignments and exogenous shocks. Accordingly, institutions should institutionalise continuous cultural self-assessment, and supervisors should cultivate an open, iterative dialogue that highlights exemplary practices, issues thematic guidance and embeds cultural indicators within the supervisory review and evaluation process. Consistently, culture risk constitutes an integral element of governance risk

within the ESG framework and ought, accordingly, to be appropriately incorporated into the Supervisory Review and Evaluation Process (SREP).

In conclusion, culture risk is neither abstract nor incidental. It is the mother of all risks, the condition from which poor governance, ethical breaches, and strategic failures emerge. Its mitigation is not the task of control functions alone, but of the entire governance architecture. In an era of complexity, scrutiny, and transformative change, institutions that invest in cultural maturity will be best positioned to sustain trust, navigate uncertainty, and achieve long-term resilience.

References

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. and A. Santomero. 1997. The theory of financial intermediation. *The Journal of Banking anf 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, and 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. and F. Metelli. 2025. Risk culture & culture risk: not a play on words. *Risk Management Magazine 21*(2): 4 – 17 .

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.

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.