RISK MANAGEMENT MAGAZINE

Vol. 20, Issue 2
May – August 2025

EXCERPT

https://www.aifirm.it/rivista/progetto-editoriale/

Risk Culture & Culture Risk: not a play on words

Rosa Cocozza, Fernando Metelli

Risk Culture & Culture Risk: not a play on words.

Rosa Cocozza (Università degli Studi di Napoli Federico II) – Fernando Metelli (Albaleasing)

Corresponding Author: Rosa Cocozza (rosa.cocozza@unina.it)

Article submitted to double-blind peer review, received on 13th May 2025 and accepted on 17th July 2025

***Disclaimer**: This work represents the collective efforts of the authors. However, the individual contributions to specific sections of the paper are as follows: Rosa Cocozza was responsible for sections 2, 3 and 4, while Fernando Metelli contributed to section 5 and all together to sections 1 and 6. The final manuscript was reviewed and approved by both authors. The authors declare that their contributions adhered to ethical standards for authorship and that no unauthorized assistance was utilized. The reflections outlined in this article are, in part, the result of considerations developed during the preparation of the AIFIRM Commentary for the public consultation on the Guide on Governance and Risk Culture (https://www.aifirm.it/commissioni-2/commissioni-attive/formulazione-dei-commenti-di-aifirm-alla-consultazione-pubblica-di-bce-guide-on-governance-and-risk-culture-deadline-16-ottobre-2024/), initiated by the European Central Bank in July 2024. The authors would like to express their gratitude to all members of the AIFIRM Commissions involved in drafting the Commentary and working on the forthcoming associated Position Paper (https://www.aifirm.it/wp-content/uploads/2025/06/2025-Position-Paper-48-Governance-e-Risk-Culture.pdf), for their valuable insights. The opinions expressed and conclusions drawn in this article are solely those of the authors and do not, in any manner, represent the responsibility or official position of AIFIRM with respect to the submitted Commentary (AIFIRM, 2024). Any errors or omissions are the responsibility of the authors collectively, and not of any institution associated with this work.*

Abstract

The purpose of this article is to suggest a primer for culture risk, aimed at outlining actionable and practical approaches distinguishing between 'risk culture' and 'culture risk'. The topic, originally addressed by the Financial Stability Board (FSB, 2014), has recently garnered renewed interest due to the Draft Guide on Governance and Risk Culture disseminated by the European Central Bank (ECB, 2024), setting out supervisory expectations, informed by the Capital Requirements Directive (CRD), European Banking Authority (EBA) guidelines, and international standards. Although the subject may be perceived as abstract, nevertheless it holds significant concrete relevance, despite the inherent challenges of measuring it. Therefore, the purpose is to move beyond the abstract boundaries of principled statements, striving instead to establish a framework that forms the logical foundation for properly managing the culture risk, which could aptly be described as the 'mother of all risks'. The stated insights may serve as a roadmap for risk managers who are tasked with addressing a significant and, in many respects, fundamental challenge. The remainder of this article, which is a theoretical paper based on conceptual analysis, is structured as follows: the first section explores definitions of risk culture and culture risk; the second outlines potential roles of corporate functions in mitigating culture risk. The third section examines the implications for the Risk Appetite Framework. The final section draws preliminary conclusions and sets the stage for future challenges.

Keywords: chief risk officer; corporate governance; corporate culture; tone-from-the-top; groupthink; effective communication; incentives; accountability; business ethics.

JEL codes: G21; G23; G28; G41; M14.

1. Introduction

Financial institutions have long been tasked with managing risks intrinsic to their role in the financial markets. Risk management, therefore, represents a core component of financial intermediation (Allen and Santomero, 1997). As financial markets grow increasingly complex, the demands placed on risk management continue to expand, necessitating ever more sophisticated methodologies and techniques. As a result, risk management is characterized by high technical intensity, requiring the Chief Risk Officer (CRO) to possess a deep understanding of quantitative methods, data analytics, and other technical domains often rooted in the hard sciences. The CRO's role has become pivotal in not only monitoring existing risks but also anticipating and mitigating emerging threats. This strategic position demands a blend of technical proficiency, forward-thinking leadership, and the ability to collaborate across all levels of the organization to ensure the institution's resilience and compliance with evolving regulatory standards.

One of the primary implications of this evolution lies in the necessity of integrating the culture of control with a robust culture of risk. While it is widely recognized that risks and controls represent two sides of the same coin (Cocozza, 2024), emphasizing the 'culture of control' focuses on remedial interventions (addressing risks after they have materialized), while emphasizing the 'culture of risk' underscores the importance and prominence of preventative activities (mitigating risks before they arise). It goes without saying that both are essential; however, the latter may prove to be more effective and cost-efficient.

Therefore, technical expertise alone is no longer sufficient for risk managers in contemporary financial institutions. Their frequent involvement in strategic decision-making forums necessitates the development of additional competencies, including strong communication skills, the ability to influence stakeholders, and a nuanced understanding of organizational dynamics. These capabilities enable risk managers to effectively contribute to broader strategic discussions while ensuring that risk considerations are integrated into decision-making processes, with the ultimate scope of good governance, fundamental for the stability and safety of financial institutions, aligning with the overarching goals of Supervisors.

The Draft Guide on Governance and Risk Culture disseminated in July 2024 by the European Central Bank (ECB, 2024) emphasizes that shortcomings in risk culture can serve as early warnings for financial instability, making sound governance essential for strategic resilience and sustainable business operations. Looking ahead, the role of Risk Management appears to be taking on a central position within corporate dynamics. No longer viewed as a cost centre, it is emerging as a critical element in the value creation chain. Effective risk control necessitates a dual focus on both returns and risks by business line leaders, as well as the full engagement of senior management. In this perspective the culture risk, a topic fundamental to financial institutions (FIs) management, forces senior

leadership to set the tone for the organizational culture and possesses tangible and effective tools to do so, including incentive plans, capital allocation decisions, investments in control structures and resources, and the role assigned to the CRO and other control functions. Additionally, leadership must adopt a proactive and 'intrusive' approach to the decisions made by units responsible for assuming risk.

Within this framework, clearly defining what constitutes 'risk culture' distinguishing it from 'culture risk', determining the functional corporate actors of primary importance, outlining their potential roles and duties, and conceptualizing metrics for measuring culture risk remain topics that are, to some extent, yet to be fully explored. The concept of risk culture originates from an initial intervention by the Financial Stability Board (FSB, 2014), following the early regulatory initiatives on the Risk Appetite Framework (RAF). The main objective of the FSB (2014) was the development of a comprehensive framework for understanding and assessing risk culture within Fis. The document outlined the foundational elements of a sound risk culture, highlighting seminal themes that were subsequently revisited by various stakeholders. (BCBS, 2015; EBA, 2021; EBA 2025), particularly concerning the corporate governance of banks ([1]). Moreover, consistent risk culture accounts for Environmental, Social and Governance (ESG) risks implemented within the institution in accordance with EBA (2021). As this subject evolved, attention has progressively shifted to the governance at the upper echelons of organizations, the role of management body, and the significance of the RAF. In this context, both the role of corporate functions and the specification of a comprehensive set of culture risk indicators remain underexamined. The latter represents a main challenge.

The purpose of this paper, a theoretical paper based on conceptual analysis, is to address these questions, with the aim of bridging the gap between fundamental principles and the effective implementation of the intended objectives. The article is structured as follows: after defining the concepts of risk culture and culture risk through a deductive logical process (Section 2) and the addressing of relevant drivers (Section 3), the focus shifts to the roles that can be attributed to corporate functions and their potential responsibilities (Section 4), culminating in the identification of criteria useful for developing and maintaining culture risk indicators. (Section 5) The last section (Section 6) draws preliminary conclusions on the topic, while acknowledging that the subject is still under investigation, as it is significantly influenced, among other factors, by varying cultural perspectives that may emerge across different contexts.

2. Culture risk: a weighty challenge.

Culture, in its broadest sense, encompasses the collective values, beliefs, norms, and practices shared by a group of people. It serves as a framework that shapes behaviour, decision-making, and interactions within a social system. Culture is transmitted across generations through socialization and institutionalized practices, evolving over time as it adapts to environmental, historical, and societal changes. Anthropologically, culture is both material and symbolic, influencing tangible expressions (artifacts, systems) and intangible aspects (ideologies, shared meanings). It provides a cohesive identity to groups, guiding behaviour and ensuring continuity amidst diversity.

Accordingly, corporate culture refers to the specific set of shared values, norms, and practices that characterize an organization. It is both a product of and a contributor to the organization's identity, shaping how members interact internally and externally. Corporate culture influences decision-making, communication, and the prioritization of goals, aligning individual behaviours with organizational objectives. It arises from leadership philosophies, operational strategies, and the historical and social contexts within which the organization operates.

The key dimensions of corporate culture include values and norms, behavioural expectations, leadership and management styles as well as symbols and rituals (Figure 1)

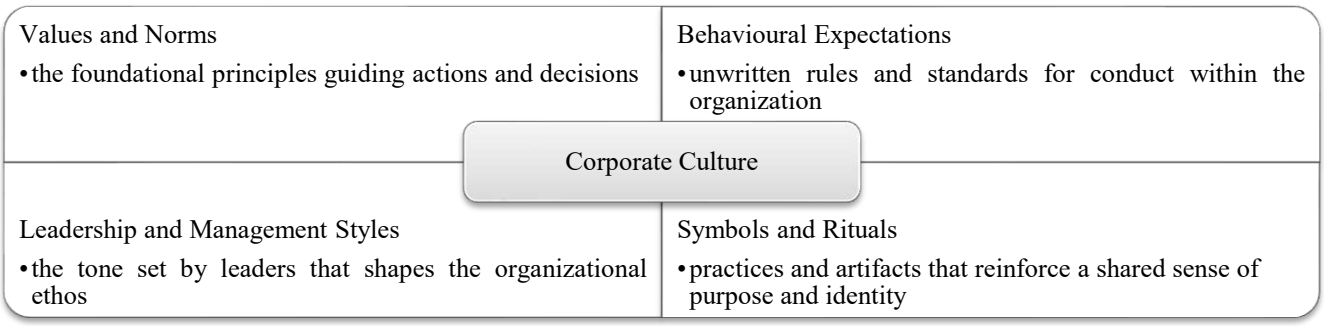

Figure 1: Dimensions of Corporate Culture

Corporate culture plays a critical role in organizational performance, influencing innovation, employee engagement, adaptability to change, and ethical behaviour. Strong corporate cultures foster alignment between organizational goals and individual motivation, while fragmented cultures may lead to conflicts and inefficiencies. In summary, as in the popular quote apocryphally credited to management consultant Peter Drucker, 'culture eats strategy for breakfast', emphasising that a powerful and empowering culture is a sure route to success.

Risk culture can be regarded as a subset of the corporate culture. It specifically pertains to the norms, attitudes, and behaviours related to risk awareness, assessment, and management within an organization. It encompasses how risks are perceived,

[1] For further insights on the published works on the subject, the following are recommended: Bockius et al. (2024); Carretta et al. (2024); Kunz and Heitz (2021).

communicated, and addressed across all levels, influencing the organization's capacity to identify, mitigate, and respond to uncertainties.

Characteristics of risk culture include risk awareness, behavioural norms, communication practices, as well as accountability and incentives (Figure 2).

Figure 2: Characteristics of Risk Culture

Given that banking activities, and financial intermediation more broadly, are inherently centred on risk – which, together with the financial resources collected, constitutes the core input of such activities – the presence of a robust risk culture is not merely desirable; it is a critical element actively pursued by supervisory authorities in their mission to ensure the ongoing safety and stability of banks. This necessity becomes even more pronounced in the current environment, where intermediaries face economic, competitive, and geopolitical challenges while simultaneously managing risks associated with climate change, environmental sustainability, and technological advancements. In fact, according to BCBS (2015, 2), recalling FSB (2014), risk culture is defined as «*a bank's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume*».

A strong risk culture aligns risk-taking behaviours with organizational objectives and regulatory expectations, fostering prudent decision-making and resilience. Conversely, a weak risk culture may result in misaligned incentives, insufficient risk controls, and an increased likelihood of operational or strategic failures. Leadership commitment, transparency, and continuous education are pivotal in embedding an effective risk culture within the broader corporate culture. Risk culture encompasses the collective mindset, norms, and behaviours that influence how risk is perceived, assessed, and managed within an organization. A strong risk culture aligns risk-taking conducts with organizational goals and regulatory expectations, fostering ethical decision-making and resilience.

Culture risk emerges when there is a divergence between the stated values of an organization and the actual practices and behaviours of its employees. This misalignment can lead to ethical lapses, operational inefficiencies, and reputational damage, ultimately compromising the institution's stability. Coherently culture risk may be referred to the potential adverse outcomes that arise from misalignments between an organization's stated values, norms, and principles and the actual behaviours, attitudes, and practices exhibited by its members. It encompasses risks stemming from deficiencies in fostering a cohesive and ethical culture that supports the organization's strategic objectives, regulatory compliance, and long-term sustainability.

Culture risk in financial institutions (FIs) can manifest in various forms, including ethical misconduct, operational inefficiencies, resistance to change as well as inadequate risk awareness, i.e. insufficient integration of risk management principles within the organizational culture, leading to poor decision-making or excessive risk-taking (Figure 3).

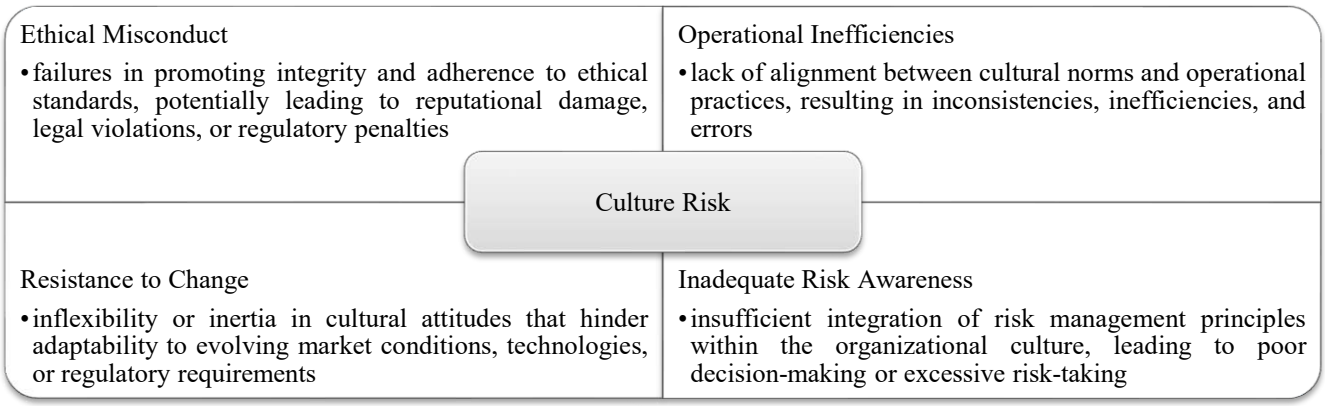

Figure 3: Culture Risk Instances

Supervisory authorities increasingly emphasize the management of culture risk as a fundamental component of FIs organizational governance, recognizing its critical role in mitigating broader operational, financial, and reputational risks.

Addressing culture risk requires ongoing leadership commitment, clear communication of values, and mechanisms for monitoring and reinforcing desired behaviours throughout the organization (Figure 4). In this respect, three fundamental pillars of culture risk management emerge as the foundation of the mechanism illustrated in Figure 4.

These pillars are:

- the leadership role, which must demonstrate profound risk awareness and a corresponding strong commitment, by communicating expectations clearly and consistently to reinforce a risk-aware culture;
- the effective communication throughout all levels of the organization, both top-down and bottom-up;
- the critical role of the organizational function, in addition to the corporate control functions.

Regarding the first pillar, the primary actors involved are the board of directors, board-level committees, and, where applicable, delegated executives. For the second pillar, it is essential to implement not only active speaking but also active listening (Cocozza, 2025). Finally, the third pillar requires the 'full maturity' of the organizational function, which serves as the primary safeguard of accountability, in conjunction with the human resources function (HR) for both incentives and induction and training programs.

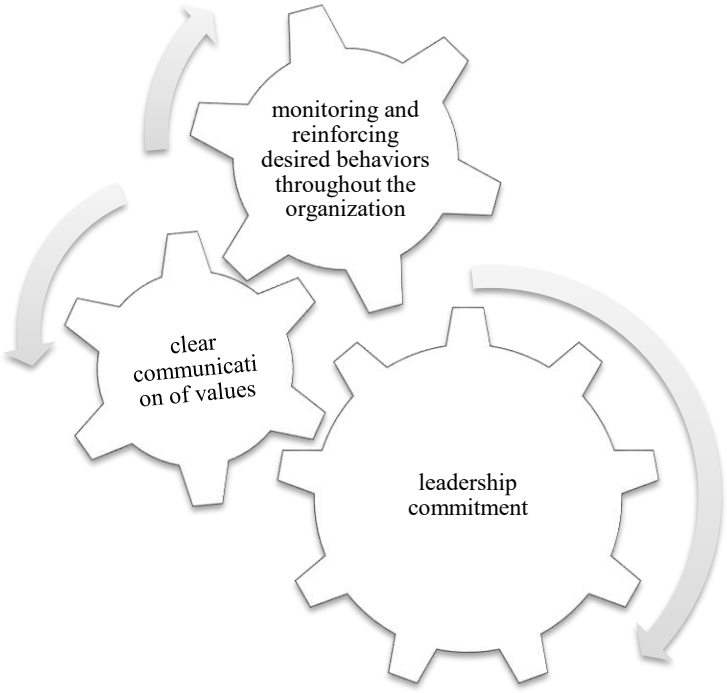

Figure 4: Foundational elements for addressing culture risk.

Therefore, the palindrome 'risk culture & culture risk' is not an elegant pun.

Risk culture refers to the shared values, attitudes, and practices regarding risk awareness and management within an institution. Culture risk, on the other hand, arises from misalignments between an organization's stated values and the behaviours exhibited by its employees. The lack of a robust risk culture gives rise to culture risk, which can prove to be detrimental or even fatal to bank's stability and sustainability.

3. Culture risk – and value – drivers.

The aforementioned lack of a robust risk culture becomes a risk factor that impacts corporate performance in complex and multifaceted ways, many of which are not easily quantifiable in terms of their effect. Hence, promoting a robust risk culture serves as a comprehensive preventive measure against culture risk and, as such, it constitutes a fundamental component of the culture risk management process.

Central to this preventive framework is the concept of the 'tone from the top', which encompasses the ethical climate, cultural values, and behavioural standards set by an organization's senior leadership. The latter includes the board of directors, executive team, and other high-ranking officials. The tone from the top reflects the attitudes, decisions, and actions of senior leaders, demonstrating their unwavering commitment to organizational values, effective governance, and sound risk management practices.

Consistently, according to foundational elements reported in Figure 4, three warning signs can be immediately identified: the lack of independence, signalling insufficient commitment from leadership; the absence of adequate whistleblowing mechanisms, indicative of ineffective communication; and weak accountability, reflecting deficiencies within the organizational lines.

Indeed, these main red flags can be immediately identified for risk culture shortcomings. By addressing these issues, institutions can build resilient frameworks capable of adapting to evolving risks.

According to the ECB (2024, 12), as reported in Figure 5, risk culture components include, apart from the already mentioned 'tone from the top', effective communication challenge and diversity, incentives and accountability for risks. Root causes of culture risk and are identified as «*cultural drivers*».

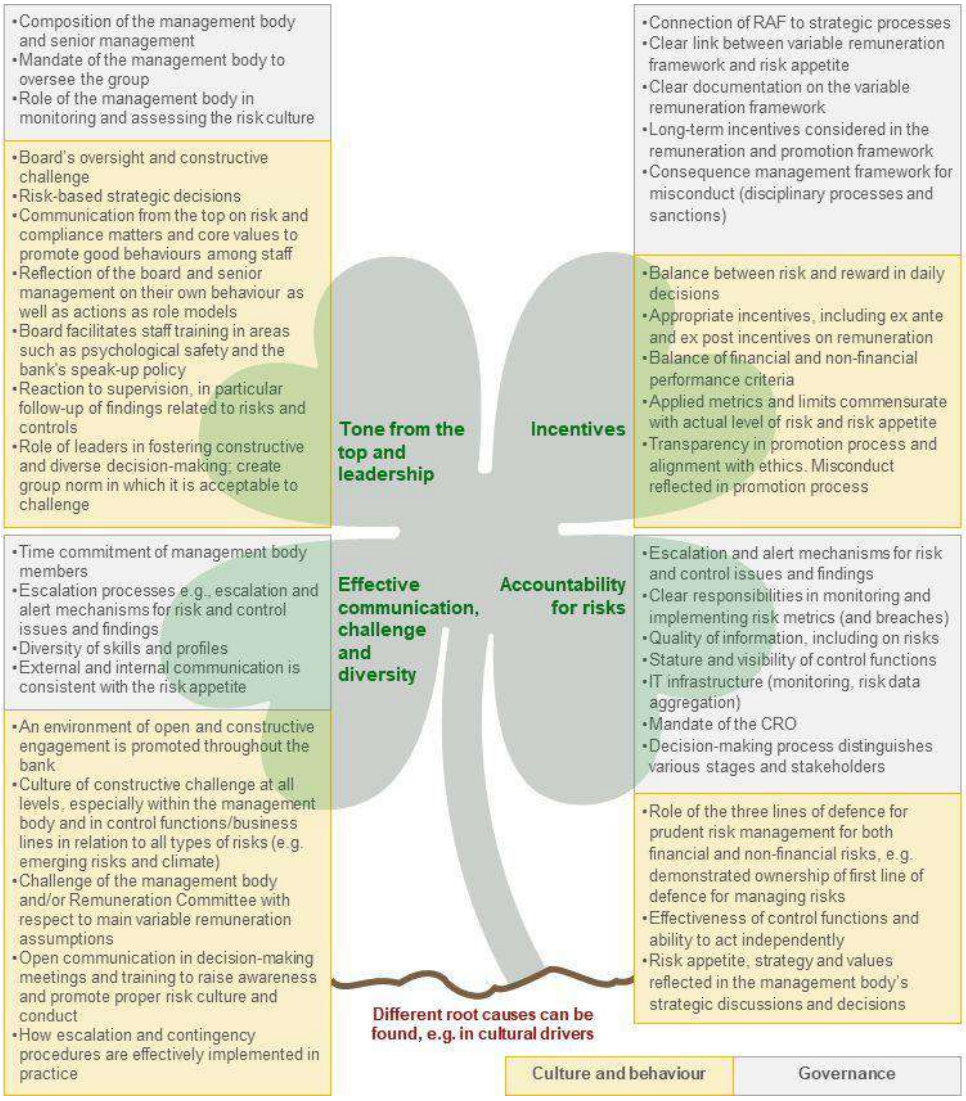

Figure 5: Map of risk culture components, connecting governance, culture and behaviour. Source: ECB (2024, 12).

As can be inferred from Figure 5, the ECB approach sets two main risk drivers for culture risk: 'governance' and 'culture and behaviour'. Consistently, the ECB (2024, 15) lists 'governance red flags' and 'behavioural and cultural red flags'. The occurrence of listed red flags, qualified «*non-exhaustive*», gives evidence of an inadequate risk culture and raises culture risk, as shown in Figure 6 and detailed in Figure 7.

Figure 6: Culture risk drivers.

The distinction between governance and behavioural and cultural risk drivers allows for further consideration on the individual cultural profiles of specific FIs. Smaller entities may be more susceptible to culture risk due to the traits of their governance structures and the impact of cultural and behavioural stratifications. Consequently, an inversion of the principle of proportionality may arise, suggesting heightened attention and caution, particularly in Less Significant Institutions (LSI). Therefore, it should in no way be construed as a plea for mitigating judgment. As a matter of fact, given the heightened complexity of implementing dedicated dashboards, LSIs must maintain a robust adoption process that is stringent yet free from undue bureaucratic encumbrances. Similarly, the adoption of a specific business model or a particular operational focus may serve as additional elements of individual profiling in relation to both control points and organizational structures. Similarly specific localization of activities, the prominence of cross-border operations, and the predominance of credit transactions characterized by peculiar contours can serve as significant factors in the customization of cultural risk profiles.

The proper conceptual framing of culture risk permits its classification within the category of governance risks, as defined by the EBA (2025). Culture risk can be conceptually situated within the broader category of governance risks – i.e., the 'G' component of ESG. The EBA explicitly define governance risks as encompassing deficiencies in executive leadership, ethical standards, and management practices, all of which can generate material financial risks that institutions are required to assess and manage. Although the term 'culture risk' is not explicitly employed, its conceptual features are clearly embedded within the EBA's treatment of governance: inadequate internal controls, insufficient board oversight, and failures in leadership behaviour are all identified as sources of governance-related vulnerabilities. The EBA further call for institutions to integrate ESG considerations into their standard risk management frameworks, emphasizing the role of ESG risks as potential amplifiers of traditional financial risk categories such as reputational, operational, and business model risks. In this context, the promotion of a sound risk culture – defined by effective communication, shared risk awareness, and clear accountability across all organizational levels – is deemed essential. In sum, the EBA's framework supports the interpretation of culture risk as an integral component of governance risk, insofar as it reflects the behavioural and ethical dynamics underpinning effective ESG risk management. This aligns with emerging technical literature (AIFIRM, 2025), which frames culture risk as a function of misalignment between formalized values and actual behaviours, highlighting its systemic implications for internal governance and institutional resilience.

Moreover, the capability to fully grasp risk culture shortcomings may also be shaped by the relevance the organisation and the board assign to 'risk and control' dimensions with respect to commercial aims. Although the academic perspective emphasises the equal importance of both, in corporate practice recognition of this equivalence sometimes encounters resistance. This may stem from differences arising from the depth and nature of experience in FIs management, as well as from the cultural and generational backgrounds of the individuals concerned.

Risk culture dimension	Governance red flags	Behavioural and cultural red flags:
Tone from the top and leadership	- Insufficient management body oversight of internal control functions and the management body in its management function - Low number of formally independent members - Insufficient subsidiary oversight - Inadequate escalation and consequence management framework in the case of risk, ethical or compliance issues - Inadequate conflict of interest policy and ethics framework	- Insufficient ownership of and responsibility for conduct risk - Unsatisfactory tone from the top from the management body to promote good behaviours among staff - Dismissive attitude among staff towards compliance, regulation and supervision - Inadequate tone from the top on the balance of risks and rewards - Concentration of power in a few members of the management - Unethical behaviours not sufficiently sanctioned by the bank and insufficient communication on these issues
Culture of effective communication and challenge and diversity	- Deficiencies in the whistleblowing process - Governance arrangements, including, committee structure and escalation process not facilitating debate - Inadequate diversity framework	- Lack of challenge and debate within the management body (discussion dominated by a few management body members) - Insufficient challenge of the management body in its supervisory function and/or its committees (e.g. remuneration committee) with respect to the main variable remuneration assumptions - Insufficient challenge from internal control functions (e.g. lack of a role for the risk management function or its head in challenging decisions) - Insufficient independence of internal control functions from the management body in its management function (e.g. filtering or review of information included in internal control function reports prior to the approval process) - A culture of fear leading to an unwillingness to report mistakes, risk breaches or material concerns - Lack of diversity (skills, gender, background) or inclusion, possibly contributing to "groupthink" - Lack of meetings and training to raise awareness and promote proper risk culture and conduct
Incentives	- Documentation underpinning the variable remuneration framework (e.g. KPIs) either missing or ambiguously worded - Lack of interplay between strategy and risk appetite - Framework to address behaviours not aligned with prudent risk-taking - Lack of link between variable remuneration framework and risk appetite - Impaired consequence management (e.g. malus and clawback clauses exist only as a formality) - Lack of individual accountability, including in the bank's remuneration and/or consequence management framework	- Incentive system does not incentivise desired behaviours - Promotion process does not reflect conduct/misconduct, ethics and behaviour - Applied metrics and limits are not commensurate with the bank's actual level of risk and its risk appetite - Imbalanced deployment of financial performance criteria versus non-financial criteria - Wrong incentives, e.g. remuneration of the CRO linked predominately to commercial objectives or connected with the performance of activities that the risk management function monitors
Accountability	- Low stature and understaffing of internal control functions - RAF not comprehensive or well implemented - Weak information technology (IT) and data aggregation framework - Lack of a comprehensive "lessons learned" process to identify and address similar risks	- Unbalanced application of the third line of defence, i.e. the first line of defence lacking a culture of accountability for risk, leaving this to the second and third lines of defence - Insufficient transparency in reporting (especially in the case of issues/concerns) - Risk management seen as a barrier to achieving business objectives

Figure 7: Risk culture red flags (non-exhaustive list). Source: ECB (2024, 15).

To provide practical application to the logical framework analysed here, it is appropriate to offer some concrete examples. The transition from theoretical postulation to practical applicability in the domain of culture risk necessitates a critical clarification concerning the measurability of the relevant constructs. In line with the managerial axiom that "what cannot be measured cannot be managed", it is imperative to delineate the object of measurement with precision. Specifically, it is not the degree or diffusion of risk culture per se that must be quantified, but rather the risk arising from its deficiency, i.e., culture risk. As previously argued, cultural inadequacies within an organization function as latent drivers of culture risk, which, like other risk categories, ultimately materialize through economic consequences, such as increased operational costs or reduced revenues. Accordingly, the operationalization of culture risk management must be anchored in the identification and deployment of appropriate Key Risk Indicators (KRIs), capable of capturing deviations from expected cultural norms and signalling potential misalignments before they escalate into broader governance failures.

Figure 8 presents, without claiming to exhaust the subject, a selection of processes that can be activated for the addressing of culture risk. Depending on the context, the outlined processes aim to establish an appropriate cultural climate, assess the current state within the individual organization, activate preventive mechanisms to mitigate exposure to culture risk, as well as implement traditional processes for identifying Key Risk Indicators (KRIs) and their corresponding monitoring.

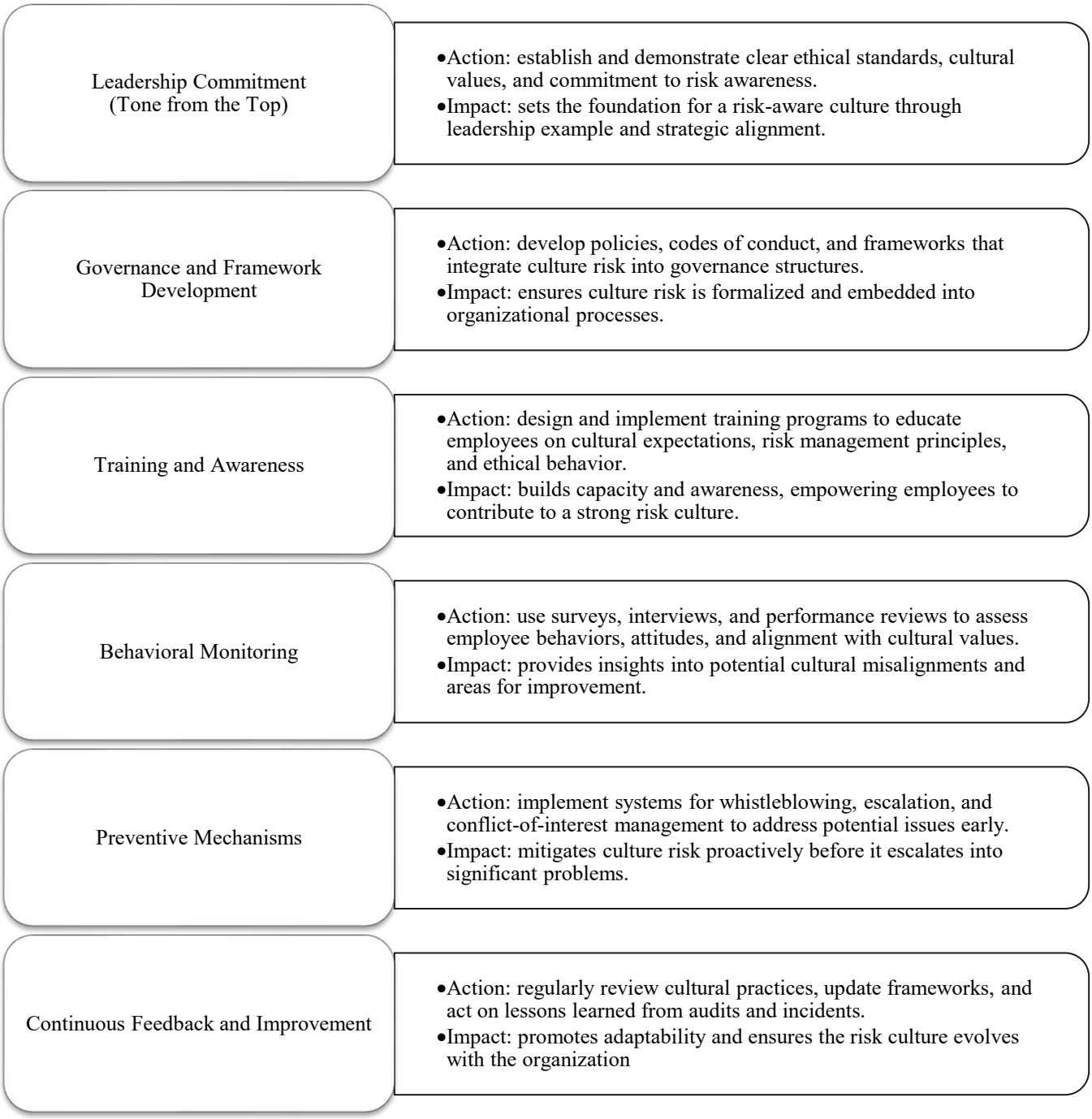

Figure 8: Processes for addressing culture risk.

4. Culture risk: who is responsible for what?

Once the culture risk has been identified, it is appropriate, following the logical process typically adopted for other risk categories, to try to identify responsibility for its mitigation and promotion within corporate functions (Section 1).

As far as the mitigation is concerned, the responsibility falls certainly– although not exclusively – within the domain of the Internal Control Framework (ICF). The ICF is a cornerstone of governance in banking institutions, serving to ensure compliance, manage risks, and safeguard organizational integrity. Beyond its operational mandates, the internal control system is pivotal in fostering a robust risk culture and addressing culture risk. As FIs face increasingly complex challenges – including regulatory scrutiny, technological disruptions, and ESG concerns – the internal control system must evolve to address these demands, including also behavioural dimensions. The internal control system appraises culture risks through audits, behavioural assessments, and whistleblowing mechanisms. Clear escalation protocols, effective conflict-of-interest policies, and active reporting mechanisms address cultural misalignments proactively. The alignment of culture risk with governance requires that culture risk is integrated into the institution's governance frameworks, including the RAF, to ensure systematic management. Hence, regular evaluations of cultural practices and lessons learned from incidents strengthen the institution's ability to mitigate culture risk effectively. Addressing these aspects requires a comprehensive approach where the control function of second and third level play distinct yet interrelated roles. The compliance function ensures adherence to regulatory requirements, ethical standards, and internal policies. By assessing codes of conduct, providing training, and monitoring conducts, the compliance function shapes the ethical foundation of the organization. It also identifies and addresses misalignments that contribute to culture risk, fostering an environment where employees understand and embrace risk-aware practices. Risk management identifies, assesses, monitors, and mitigates risks that could impact the institution's objectives. Beyond managing traditional risk categories, the function integrates culture risk into the RAF and broader governance structures. By promoting proactive risk awareness and embedding accountability, risk management strengthens the organization's capacity to address cultural challenges. Internal audit provides independent assurance on the effectiveness of the organization's governance, risk management, and control systems. It assesses whether risk culture is embedded across the institution and identifies gaps in cultural alignment. Internal audit also evaluates the effectiveness of measures taken to mitigate culture risk, ensuring continuous improvement and accountability.

The timing of actions executed by internal control functions – compliance, risk management, and internal audit – is strategically aligned with the stages of risk and control activity within an organization. These stages, delineated as *ex-ante* (preventive), real-time, and *ex-post*, define the distinct responsibilities and levels of engagement for each function. In the preventive stage, the objective is to anticipate and mitigate risks before they materialize, thereby reducing the likelihood of adverse events. At this stage, the compliance function plays a pivotal role, enforcing regulatory requirements, organizational policies, and ethical standards designed to proactively address potential risks. Concurrently, risk management contributes by identifying emerging risks, assessing their potential impacts, and defining risk limits within the institution's RAF. Internal audit, however, typically has minimal involvement at this stage, as its primary responsibility is to deliver retrospective evaluations and assurance. The real-time stage focuses on the active monitoring and management of risks as they arise, ensuring timely and effective responses to mitigate potential impacts. During this phase, risk management assumes a leading role, continuously monitoring risk exposures, maintaining alignment with established thresholds, and making necessary real-time adjustments. The compliance function supports these efforts by ensuring ongoing adherence to regulatory and organizational standards amidst dynamic operations. Internal audit, though less central, offers moderate involvement by providing immediate feedback on control effectiveness and participating in oversight where required. In the *ex-post* stage, the emphasis shifts to the thorough analysis, evaluation, and enhancement of processes and controls following the occurrence of a risk event or control failure. At this juncture, internal audit assumes a dominant role, conducting in-depth investigations to uncover root causes, recommending corrective measures, and driving initiatives to strengthen organizational resilience. Risk management evaluates the broader implications of the incident on the institution's risk framework, revising mitigation strategies as necessary. Simultaneously, the compliance function ensures that any regulatory violations are properly identified, reported to relevant authorities, and addressed through corrective actions. This systematic alignment of functional roles across the risk management continuum ensures a coordinated, effective approach to risk governance, fostering organizational resilience, regulatory compliance, and strategic alignment. By optimizing the interplay of these functions, institutions can establish a proactive, agile, and comprehensive framework for managing risks across all phases of their operations.

The temporal distribution of responsibilities highlights the interdependence of internal control functions, and their complementary contributions ensure a cohesive approach to promoting risk culture and mitigating culture risk. These functions collaborate to align insights, strategies, and actions, creating a unified framework for cultural resilience. The timing of action for internal control functions underscores the strategic alignment of their roles in addressing risks across all stages of organizational activity. This framework establishes a robust foundation for advancing both academic inquiry and practical innovation in understanding the interplay between control functions and risk management settings and decisions within modern organizational contexts. It further underscores the critical importance of fostering a cohesive and integrated approach to strengthening risk culture while proactively addressing and mitigating cultural vulnerabilities. Therefore, the scope of activities attributable to the control functions is contingent upon the extent of risk culture dissemination within the organization and, consequently, the organization's level of awareness regarding culture risk related matters.

During the development phase, the promotion of risk culture is paramount. The internal control system strengthens the role of leadership in establishing an ethical tone, strengthening behaviours that prioritize risk awareness and regulatory compliance. In the foundational phase, comprehensive training programs designed by compliance and risk management functions serve to educate employees on risk management principles and cultural expectations, thereby advancing training and capacity building. In the maturity phase, internal control functions actively monitor employee behaviours and attitudes, offering feedback and recommendations to ensure alignment with institutional values, thereby facilitating behavioural monitoring and feedback. Once pervasiveness is achieved, the internal control system embeds risk culture into governance frameworks and operational processes, ensuring consistency and accountability across all organizational levels and fully integrating risk culture into governance.

With this respect, the operating area of a bank, encompassing various functions such as operations, technology, and back-office support, plays a focal role in embedding and sustaining a robust risk culture. As the operational backbone, this area ensures the institution's strategic objectives are translated into day-to-day activities while mitigating culture risk. Its responsibilities extend beyond traditional operations to fostering accountability, promoting transparency, and aligning operational practices with the institution's risk culture. The enhancement of accountability begins with the establishment of clear roles and responsibilities for all operational staff, ensuring that individuals are fully aware of their contributions to risk management and cultural alignment. Furthermore, structured escalation mechanisms are implemented to identify and address risk incidents effectively, ensuring prompt resolution and minimizing potential impacts. The integration of risk culture into operational processes involves translating organizational policies and strategic goals into actionable procedures, fostering consistency in decision-making and adherence to regulatory and ethical standards as well as ensuring that risk management becomes an integral part of all operational decisions. Strengthening communication channels is another essential responsibility of the operating area. By developing transparent and efficient frameworks for the exchange of information, the operating area facilitates the flow of critical risk-related insights across organizational levels. This open communication environment not only enhances collaboration between operational staff and control functions but also encourages constructive dialogue and the escalation of concerns. Additionally, the operating area supports the establishment and utilization of whistleblowing mechanisms, ensuring that employees can report unethical behaviour or cultural misalignments in a secure and confidential manner. In promoting ethical practices, the operating area ensures that the leadership's commitment to fostering a strong risk culture is translated into tangible actions throughout the organization. Operational processes are designed to reflect and reinforce the institution's core values, aligning operational goals with ethical standards and strategic objectives. Tools and training programs are developed to support employees in making ethical decisions, particularly in complex scenarios where risks must be carefully balanced against opportunities. Finally, the operating area is instrumental in aligning incentives with the organization's risk culture. By integrating adherence to risk culture and operational discipline into performance evaluations, the operating area ensures that employees are rewarded for behaviours that align with the institution's ethical and risk management standards. Compensation and promotion frameworks incorporate risk-awareness metrics, creating incentives that prioritize long-term organizational success over short-term gains. Employees demonstrating exemplary alignment with the institution's risk culture and ethical values are recognized and rewarded, further reinforcing the importance of cultural adherence.

Through these responsibilities, the operating area not only supports the operationalization of the institution's risk culture but also acts as a vital conduit for embedding ethical and risk-aware practices at every level of the organization. Its efforts contribute to a cohesive and resilient organizational environment where cultural and risk management objectives are seamlessly integrated into operational realities.

5. Culture risk: KRIs and KPIs.

A proper risk-culture framework can be established and survive only if it is made visible through a disciplined cycle of measurement and reporting; otherwise, it remains an abstract corporate mantra. For this reason, the starting point for any CRO is to weave culture-related Key Performance Indicators (KPIs) and Key Risk Indicators (KRIs) into the bank's planning architecture and business-model definition, strategic targets, Internal Capital Adequacy Assessment Process (ICAAP) and the Internal Liquidity Adequacy Assessment Process (ILAAP) risk-profile analysis and, finally, the RAF. The resulting 'KPI/KRI management system' must be strictly aligned with strategic objectives so that cultural ambitions are translated into operational thresholds: if a KPI expresses what the institution wishes to achieve, the corresponding KRI signals how far the underlying cultural drivers may endanger that objective. In a strong risk culture, this alignment enables proportional graduation of risk, prioritisation of monitoring effort and corrective action, and, crucially, creates an auditable bridge between tone-from-the-top statements and day-to-day behaviour. Supervisors now expect such traceability; the ECB (2024) explicitly stresses that culture must be «measurable, verifiable and proportionate to size, complexity and business model», and regards the adoption of an integrated KPI/KRI dashboard as evidence of its verifiability. Hence, establishing clear culture metrics is no longer a voluntary exercise but part of the prudential perimeter.

Regulatory bodies have consistently advocated the application of clear KPIs for the assessment of individual managerial performance. This paper expands the scope of the discussion by proposing a unified and coherent framework aimed at the identification and management of both KPIs and KRIs, as depicted in Figure 9.

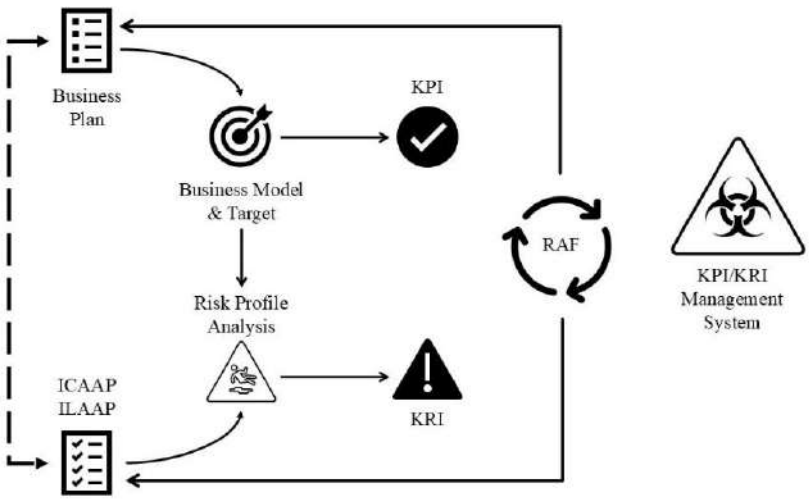

Figure 9: KPI/KRI framework.

Such a framework is posited as an essential component of robust corporate governance. Effective management necessitates rigorous planning, underpinned by an in-depth understanding of the organization, its operational mechanisms, target markets, and its exposure to potential risks, threats, and vulnerabilities. For the planning process to be truly comprehensive, it must also embody and communicate core values reflective of the organization's culture (Section 2).

The process of planning, defined as the articulation of business objectives within a specific business model, generates the essential data required to establish the institution's risk profile, as outlined in the ICAAP and the ILAAP. The effectiveness with which this process is executed constitutes the initial manifestation of an organization's risk culture. We emphasize the critical importance of a meaningful alignment between KRIs and KPIs, integrated within a coherent framework aligned with strategic goals. Such alignment is indispensable for the accurate classification and prioritization of risks, thereby enabling informed decisions regarding appropriate monitoring measures and potential mitigating actions. Obviously, KRIs aligned with KPIs must be pertinent (to the business model), measurable (in the most objective terms possible) and timely (reflecting environmental volatility and potential severity). In general, a sound KRI system is characterised by:

- details on the variables of the people-process-technology triad and on other corporate attributes most relevant to the proper functioning of the organisation in pursuit of strategic targets;
- classification of corporate assets according to their criticality for the bank;
- identification of the risks, threats and vulnerabilities the bank must face, based on probability of occurrence, operational and financial impact, and the organisation’s capacity to mitigate the event;
- subsequent classification of risks, threats and vulnerabilities in terms of potential damage;
- linkage between key corporate objectives/KPIs and the most significant risks, in order to identify areas requiring enhanced monitoring and control;
- definition of parameters that determine when and how an identified risk becomes a serious threat;
- codification of a continuous process for reviewing KRIs and their metrics so as to detect any changes that require review and/or corrective action.

As any other risk management process, the identification phase is anchored to the people-process-technology triad and proceeds in four logical steps. First, the CRO maps critical assets – human capital, core processes, IT platforms – against their relevance to cultural objectives. Second, potential threats and vulnerabilities are classified by probability, severity and organisational ability to mitigate; this turns qualitative cultural ambitions into risk-sensitive categories. Third, each material risk is linked to the strategic KPI it could derail, thereby highlighting areas requiring heightened monitoring; and fourth, quantitative or qualitative parameters are set that allow objective detection of early deviation.

The resulting menu of KRIs will typically include

- financial indicators (e.g. risk-adjusted revenue versus conduct events);
- human-resources indicators (e.g. regretted turnover in control functions or training-completion ratios);
- operational indicators (e.g. process-break rates, near-misses, override frequencies);
- technology indicators (e.g. percentage of critical systems with end-of-life components);
- cyber-security indicators (e.g. phishing-simulation failure rates).

For each KRI the CRO establishes tolerance thresholds and escalation triggers. Because culture risks evolve with ‘novel’ external pressures – ESG litigation, AI bias, geopolitical disinformation – KRIs must be reviewed at least annually, with ad-hoc revisions whenever the business plan or the regulatory environment changes. Embedding this architecture in governance is the responsibility of the board and its committees. Under the assumption of ‘full cultural maturity’, the board approves the list of culture KPIs/KRIs as part of the RAF and receives regular dashboard reports, thereby making cultural performance a standing agenda item. In this process, Risk Management owns the design and validation of indicators, Compliance tests alignment with regulatory conduct expectations and Internal Audit provides ex-post assurance on data reliability and on the effectiveness of escalation.

Active leadership participation is indispensable: senior executives must use the dashboard in performance dialogues, and business-line heads must feel personal accountability for deviations; only then do KRIs become ‘lived’ metrics rather than compliance artefacts. It is also recommended to embed KPI/KRI attainment into variable-remuneration scorecards and claw-back clauses: for example, failure to close substantiated whistle-blower cases within target time would reduce the bonus of the manager concerned. Equally, exemplary adherence – such as proactive challenge of group-think – triggers positive recognition, converting cultural principles into tangible incentives.

Monitoring and escalation complete the cycle. A robust data-governance backbone feeds automated dashboards – accessible online and offline on mobile devices – to all three lines of defence, ensuring timeliness and transparency. Threshold breaches are colour-coded (e.g. amber for tolerance limits, red for breaches) and routed through predefined channels: first line rectifies operational issues; second line validates remediation and, if systemic, proposes RAF reviews; third line assesses lessons learned. Parallel whistle-blowing statistics, staff-survey sentiment scores and diversity metrics complement hard data, addressing ECB concerns that a ‘culture of fear’ could suppress early signals. Where red flags accumulate, for instance, weak management-body challenge, poor conflict-of-interest disclosure, or inadequate variable-pay documentation, the CRO must initiate a culture-risk incident report, triggering board scrutiny and, when necessary, supervisory notification. This closed-loop process proves vital in LSI, where proportionality must not reduce

vigilance; indeed, the inversion principle, as noted, warns that smaller entities may require greater indicator granularity, as informal governance can mask early cultural erosion.

The system described is complex and, to be robust and thus effective, must be based on a very solid process capable of managing the 'KRI life-cycle' (identification, assessment, monitoring, reporting to recipients). This calls for a precise allocation of responsibilities which, returning to Figure 9, could fall to the drafter of the RAF, allowing a centralised management of the implementation issues that arise in this field. Numerous points warrant attention. First, active participation by senior figures in the use of KRIs as an integral part of an enterprise risk-management programme must be ensured, without neglecting all other stakeholders in business and staff areas. Involving people – a qualitative building-block of an organisation's culture – facilitates the sharing of ideas and the use of indicators that are well understood by all. This requires identifying parameters that are «*measurable*» and «*comprehensible*»: dashboards are an effective means of presenting information and facilitate its use. A continuous activity must also be defined to monitor, measure and analyse any changes in the metrics. Finally, the system must ensure that actions are generated whenever deviations from KRI metrics occur. This represents the ultimate confirmation that the system is effectively in use and that risk culture is not an abstract element in corporate culture.

Regular monitoring of KRIs is essential, but the frequency depends on the nature of each indicator. Some KRIs may require daily attention, while others can be reviewed monthly or quarterly. It is vital to establish a routine that corresponds to the potential impact and probability of the risk, once again in relation to organisational complexity and business model.

In conclusion, designing an effective system of KRIs aligned with KPIs entails several challenges. The main one, in our view, is not to overlook the need to align KRIs with KPIs; conversely, the risk of a lack of responsiveness to periodic measurements must also be managed, often justified by the absence of thresholds. Naturally, the greater the organisational complexity, the more technological challenges arise: the possibility of working through dashboards is based on system integration, often hampered by obsolescence and fragmentation of systems. We can summarise the foregoing by recalling that 'corporate culture' cannot be separated from the 'culture of reporting', which covers the entire process from KPI identification and data processing to presentation and active use.

Admittedly, the embryonic stage of development in this field does not yet allow for a fully articulated framework that extends beyond the best practices outlined in the Guide (ECB, 2024), an observation extensively discussed in the dedicated AIFIRM Position Paper (2025), that we recall here for a more detailed examination. Building on the conceptual architecture developed in the present contribution, several lines of inquiry warrant further attention in order to advance the theoretical robustness and operational applicability of culture risk frameworks. First, the proposed alignment between KPIs and KRIs calls for empirical validation across diverse institutional contexts, with a view to assessing its predictive efficacy and practical enforceability. In-depth case studies of cultural failures in financial institutions, aimed at tracing observable misconduct or governance lapses back to early cultural warning signs and deficiencies in oversight mechanisms, could serve as a valuable support in the practical definition of indicators. At the organizational level, further research should interrogate the behavioural drivers of cultural integrity, including leadership tone, groupthink dynamics, psychological safety, and the structuring of incentives.

From a governance perspective, the integration of culture risk into the RAF requires greater technical articulation, particularly concerning the calibration of tolerance thresholds, the linkage to capital planning, and the definition of escalation protocols. In parallel, the ongoing digital transformation of financial services raises urgent questions about how culture risk manifests in algorithmic environments and technology-led business models, especially among fintech entities operating outside traditional governance structures. Finally, the incorporation of qualitative data streams, such as employee sentiment analysis, whistleblowing metrics, and behavioural surveys, into formal risk governance frameworks may offer a promising path toward the early detection of cultural vulnerabilities, provided that appropriate safeguards for data integrity, confidentiality, and accountability are in place. Collectively, these research directions offer a coherent agenda for advancing the state of the art in culture risk management, moving the field beyond principled aspirations toward verifiable, actionable, and institutionally embedded practices.

6. Conclusions

If culture risk constitutes – as actually is – a genuine risk category, it must be addressed on par with other risk types. Identification, measurement, and management should serve as the foundational elements for developing an effective mitigation of this specific risk category. In this way, the FI's strategy can be nourished and strengthened by a well-established risk culture, setting a way of creating organizations that are flexible and innovative and where individuals take responsibility for results – moving away from bureaucratic silos where formulaic approaches dominate. In other words, risk culture represents shared norms, attitudes, and behaviors toward risk management and awareness at all levels.

In the end, the 'risk manager of last resort' is the Chief Executive Officer (CEO), who bears ultimate responsibility for both results and risks. It is only from the top that a successful strategy and a corporate culture genuinely grounded in the understanding and control of risks can be effectively established and enforced. Nevrtheless, an effective culture-risk architecture hinges on a disciplined KPI/KRI ecosystem that transforms ethical aspirations into measurable managerial practice.

The translated framework underscores four imperatives:

1. embed KPI/KRI design in strategic planning so that risk-profile analysis (ICAAP/ILAAP) informs – and is informed by – the Risk Appetite Framework;
2. align every KRI with a corresponding KPI, thereby enabling graded risk prioritisation and proportionate corrective action;
3. maintain a dynamic life-cycle for indicators – definition, validation, monitoring, escalation – supported by clear ownership, dashboard-based transparency and thresholds that trigger timely intervention;

4. balance quantitative and qualitative signals across finance, human resources, operations, technology and cyber-security, with special vigilance for emerging 'novel risks'. When senior leadership visibly employs this dashboard in performance dialogues, the bank converts abstract cultural principles into operational discipline, ensuring that 'what gets measured gets managed' remains true even for the elusive domain of corporate culture.

Finally, implementation must respect proportionality while preserving comparability. Two design principles remain universal: bidirectional integration implying that KRIs flow into strategic KPI assessment, and KPI shifts trigger KRI re-validation; and actionability, that is to say every indicator must have an owner, a documented escalation path and a predetermined management response. When these principles are honoured, cultural-risk metrics cease to be a regulatory burden and become a strategic asset: they enable management to balance innovation and prudence, reassure supervisors, and, ultimately, protect stakeholder confidence in a volatile environment. As practitioners know, *what gets measured gets managed: culture risk is no exception*.

References

AIA (2015). *La cultura del rischio*. https://www.aiiaweb.it/la-cultura-del-rischio.

AIFIRM (2024). *Comments to ECB Guide on governance and risk culture.* Available at: 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*. Available at: https://www.aifirm.it/wp-content/uploads/2025/06/2025-Position-Paper-48-Governance-e-Risk-Culture.pdf.

Allen F. and Santomero A. (1997), The theory of financial intermediation, *Journal of Banking & Finance*, 21, pp. 1461-1485.

BCBS (2015). *Corporate governance principles for banks*. Available at: https://www.bis.org/bcbs/publ/d328.pdf.

Bockius H. and Nadine Gatzert N. (2024). Organizational risk culture: A literature review on dimensions, assessment, value relevance, and improvement levers, *European Management Journal*, 42 (4), pp. 539-564. https://doi.org/10.1016/j.emj.2023.02.002.

Carretta A., Fattobene L., Graziano E. A. and Schwizer P. (2024). Errors and Misbehaviors in banking and finance: a Systematic Literature Review and an Integrative Framework, *Journal of Management Governance*. https://doi.org/10.1007/s10997-024-09727-7. Available at: https://rdcu.be/d5VNQ.

Cocozza R. (2024). Fattori critici di successo del Risk Management: qualche istruzione per l'uso, *Rivista Bancaria Minerva Bancaria*, 3-4, pp. 57-84. https://dx.doi.org/10.57622/RB2024-03-C-04.

Cocozza R. (2024). Risk management, the board and the C-suite: The adaptive art of communication in times of change, *Journal of Risk Management in Financial Institutions*, 18, pp. 14-25. https://dx.doi.org/10.69554/nyap5618.

EBA (2021). *Guidelines on internal governance under Directive 2013/36/EU*. Available at: 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 (2025). *Guidelines on the management of environmental, social and governance (ESG) risks*. Available at: 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*. Available at: 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.* Available at: 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*. Available at: https://www.fsb.org/uploads/140407.pdf.

Kunz J. and Heitz M. (2021). Banks' risk culture and management control systems: A systematic literature review. *Journal of Management Control*, 32, pp. 439-493. https://doi.org/10.1007/s00187-021-00325-4.

Romito F. (2012). L'evoluzione del Risk Management nelle banche: non solo misurazione, in P. Prandi (a cura di), Il Risk Management negli Istituti di Credito. Come affrontare le sfide in scenari di incertezza, FrancoAngeli, Milano pp.19-26.