KPMG

# Risk Culture in the Financial Service Industry

## A Hidden Strategic Asset

Whitepaper

2026

# Contents

# 1. Navigating a New Risk Reality

### Uncertainty as the New Normal

An elevated level of uncertainty has become become the defining context for financial institutions. This places organisational culture, especially its risk-related dimensions, firmly at the centre of attention. Geopolitical tensions, economic pressures, climate shocks, and cyber threats create a landscape of persistent volatility. Organisations face a **continuous stream of interconnected risks rather than isolated disruptions**. Traditional risk controls and fragmented governance frameworks struggle to keep pace with today's complexity.

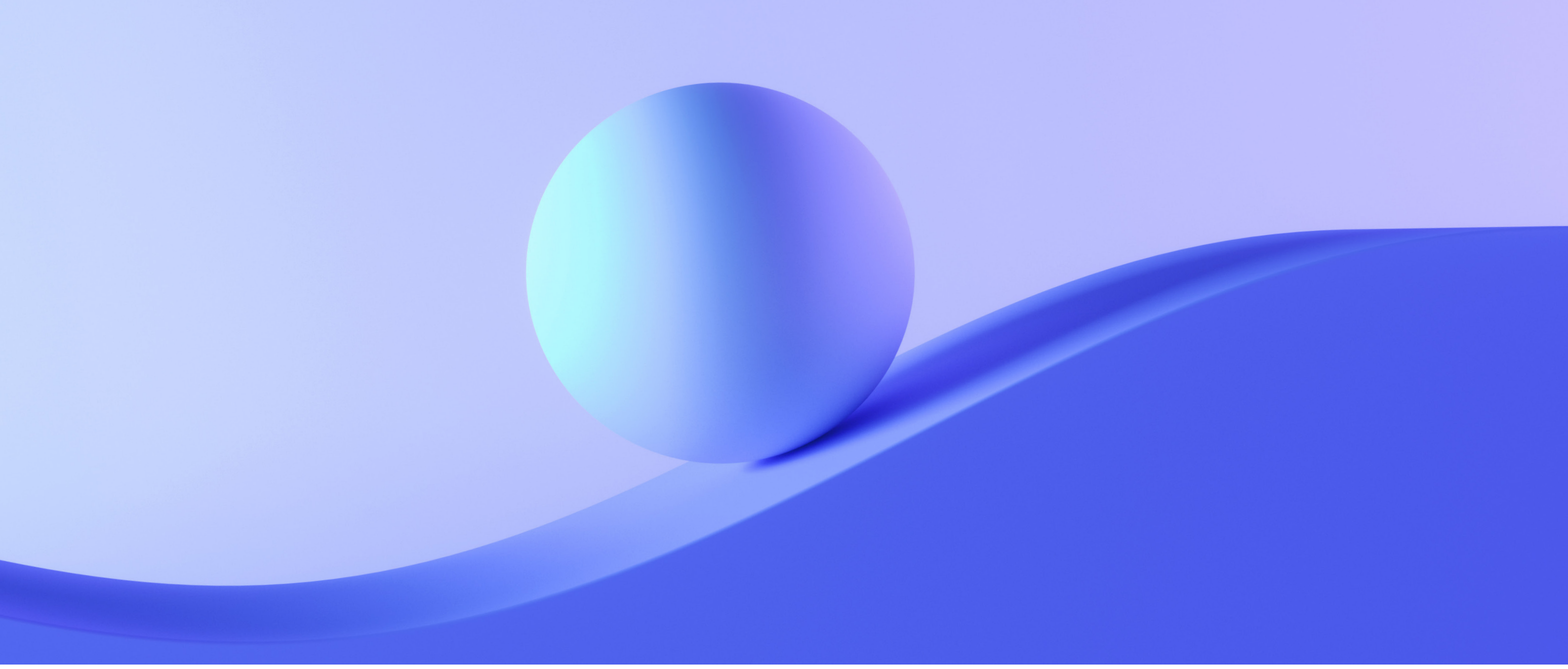
In this environment, our **behaviour is decisive**. How do leaders make decisions when market conditions shift overnight, and existing risk management frameworks no longer align with the new reality? How do teams respond when a cyber incident unfolds? How does a relationship manager handle a client request that raises ethical concerns outside formal policy guidance? These **moments of judgement reveal the strengths** and weaknesses of an organisation's risk culture.

Organisational culture and risk culture cannot be viewed in isolation. **Risk culture is an integral part of organisational culture.** The same values, norms, and behavioural expectations that **guide everyday collaboration also shape how people perceive, escalate, and manage risks. Risk culture is tangible:** it can be measured and managed. Research shows it can be strengthened through leadership role modelling, aligned incentives, and structured interventions (ECB Draft Guide on Governance and Risk Culture, 2024; Kunz & Heitz, Journal of Management Control, 2021).

A strong risk culture encourages employees to raise concerns early, weigh trade-offs responsibly, and act with confidence under uncertainty. Weak risk cultures foster silence, shortcuts, and uncontrolled risk-taking. **Risk culture is key for resilience, and it can be assessed, influenced, and continuously improved.**

### Three Reasons to Care About Risk Culture

- First, **every organisation has a risk culture**. It exists whether it is consciously managed or not. The real question is whether it is strong enough and aligned with long-term goals, values and risk appetite. A robust risk culture reduces misconduct, encourages learning and innovation, and improves performance.
- Second, having **a strong risk culture is a solution to navigate complexity**. In fast-moving environments, rules cannot anticipate every scenario. Therefore, organisations need employees to act with initiative and sound judgement. A strong risk culture shapes consistent decision-making when formal frameworks reach their limits.
- Third, **new technologies shift employees from performing routine tasks to** making **higher-stakes decisions** about automated outputs. This raises the importance of sound judgement. A strong risk culture ensures that employees remain vigilant, question anomalies, and apply ethical reasoning when interacting with AI-enabled systems.



**Regulatory focus reinforces the importance of risk culture.** Supervisors increasingly view risk culture as essential for sound governance. The ECB's forthcoming Guide on Governance and Risk Culture reflects this trend. While emphasis may differ, risk culture is becoming part of supervisory assessments – underscoring its strategic importance.

### The Business Case for a Strong Risk Culture

Organisations with a strong risk culture do more than avoid losses or meet compliance requirements – they create value. They make better decisions, build stakeholder trust, accelerate innovation, and reduce unwanted incidents. A strong risk culture is dynamic and can be actively shaped. Through structured assessments, targeted interventions, and continuous development, risk culture becomes a lever that brings governance to life.

## In short: a robust risk culture is a hidden strategic asset.

## Key Takeaways

### Strong risk cultures create value, not just protection

Organizations with resilient, well-embedded cultures consistently outperform peers in decision quality, stakeholder trust, and crisis response. A mature risk culture does more than prevent failure: it supports ethical growth in complex environments, encourages innovation, and helps attract and retain top talent in an increasingly competitive landscape.

### Risk culture is dynamic and can be shaped and managed.

It develops over time through everyday decisions, interactions, and leadership behaviour. Structured assessments help organisations understand where they stand and provide a foundation for targeted actions to strengthen its risk culture.

### Risk culture brings business and operating model to life

Risk culture is always present, embedded in leadership, decision-making, and control structures. When intentionally aligned with the organisation's Risk Appetite and formal frameworks such as the Three Lines of Defence, it becomes a strategic asset that strengthens resilience and accountability. Left unmanaged, it can just as easily undermine governance through inconsistent behaviours and weakened oversight.

# 2. What Is Risk Culture and Why Does It Matter?

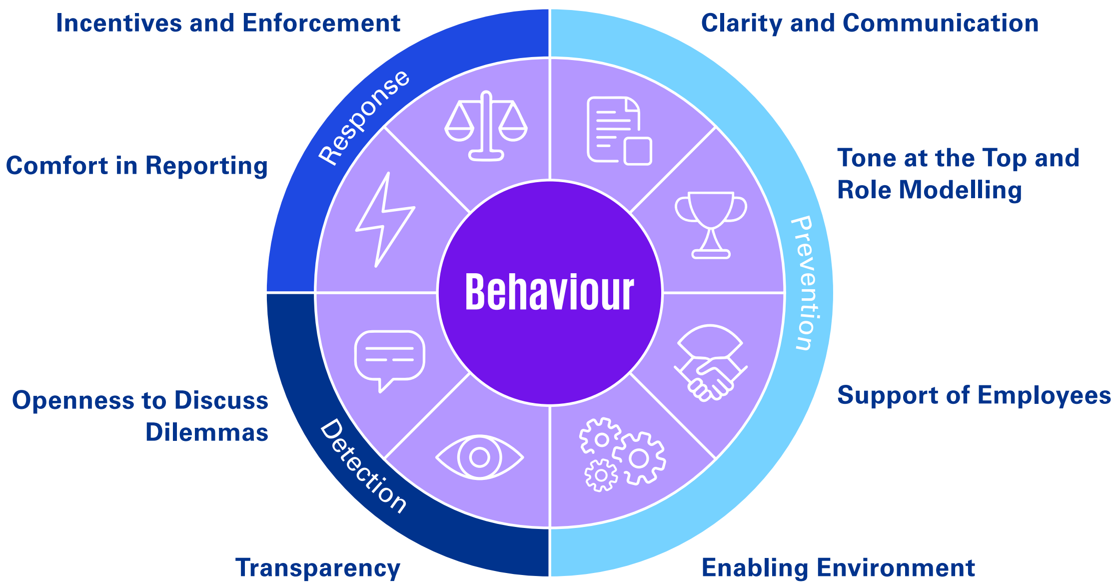
> **Risk culture is a bank's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and controls that shape decisions on risks.**
>
> (Basel Committee on Banking Supervision (BCBS))

As part of organisational culture, **risk culture** reflects the **collective mindsets, shared norms, and everyday behaviours** that shape how risks are managed across the entire client and product lifecycle, and operating model supporting business activities.

It guides responsible decision-making beyond rules and policies, influencing how employees respond to uncertainty, escalate concerns, and balance risk with opportunity. **Risk culture** is **dynamic and evolves** with internal developments and external influences.

KPMG has developed a practical and comprehensive risk culture model. This model is based on scientific analysis of 150 cases of organisational misconduct. It is underpinned by research that identifies eight cultural dimensions as significant influencers of behaviour within organisations:

Figure 1:
**KPMG's Risk Culture Model**




*Source: KPMG, 2026*

**Clarity and Communication** refer to how accurate, concrete, and complete the expectations of desired and risk-conscious behaviour for employees are, including their understanding of values and norms.

**Tone at the Top and Role Modelling** refers to the degree to which management and leadership set a good example (role model) for employees on risk culture.

**Support of Employees** pertains to whether employees endorse the proper risk behaviour and actively consider the interests of leadership and stakeholders.

**Enabling Environment** concerns the degree to which employees are enabled to meet expectations regarding desired and risk-conscious behaviour.

**Transparency** concerns the extent to which misconduct or reckless behaviour of employees and its effects are visible.

**Openness to Discuss Dilemmas** refers to the degree to which employees talk about desired and risk-conscious behaviour and dilemmas.

**Comfort in Reporting** refers to the degree to which employees can raise concerns about alleged misconduct or excessive risk-taking and provide constructive challenges.

**Incentives and Enforcement** refer to the degree to which employees are incentivised for misconduct and rewarded and sanctioned for desired and risk-conscious behaviour.

By enhancing these dimensions, organisations increase the likelihood of fostering desired behaviours and reduce the risk of reckless or undesirable actions. Each dimension reinforces the others; therefore, gaps in one area can weaken the overall effectiveness of the framework. The KPMG risk culture model is **scientifically validated**.

Having established what risk culture is, the next question is: why does it matter? The following sections outline five reasons why a strong risk culture is essential for financial institutions.


In particular, in the context of managing complex and not fully understood risks (emerging risks) risk culture becomes a "game changer", as highlighted in the whitepaper "Emerging Risks" by KPMG Germany.

# The Backbone of Value Chain Risk Management

Risk culture shapes how risks are managed throughout the entire value chain. From acquisition and onboarding to monitoring, restructuring, and termination, employee decisions are guided by an organisation's risk culture.

This is especially true in banking, where credit and operational risks **do not arise at a single** point in time, but build up over time through processes. For example, a customer's journey doesn't end with onboarding; it begins there. And risk costs (e.g., credit losses, behavioural risks, operational errors) arise **throughout the entire client and product lifecycle** and often extend beyond it.

Driving the desired risk culture requires clear governance and alignment with the Three Lines of Defence (3LoD). When these lines work in harmony together, risk culture becomes a lived practice across the value chain, not just a statement in a governance document.

# Aligning Risk Appetite with Strategy

In financial institutions, risk enters through a combination of product, client, and employee decisions. It matters which customers are served, whether the product fits the client, and whether exposures remain within the defined risk appetite. Ultimately, employees make these decisions – and this is where **the strength of a robust risk culture becomes visible**.

A clearly articulated risk appetite works best when supported by a risk culture that promotes consistent decision-making and accountability across all levels of the organisation. In practice, a **strong risk culture acts as the behavioural enabler** that ensures the organisation's stated risk appetite is understood, embraced, and applied in daily activities.

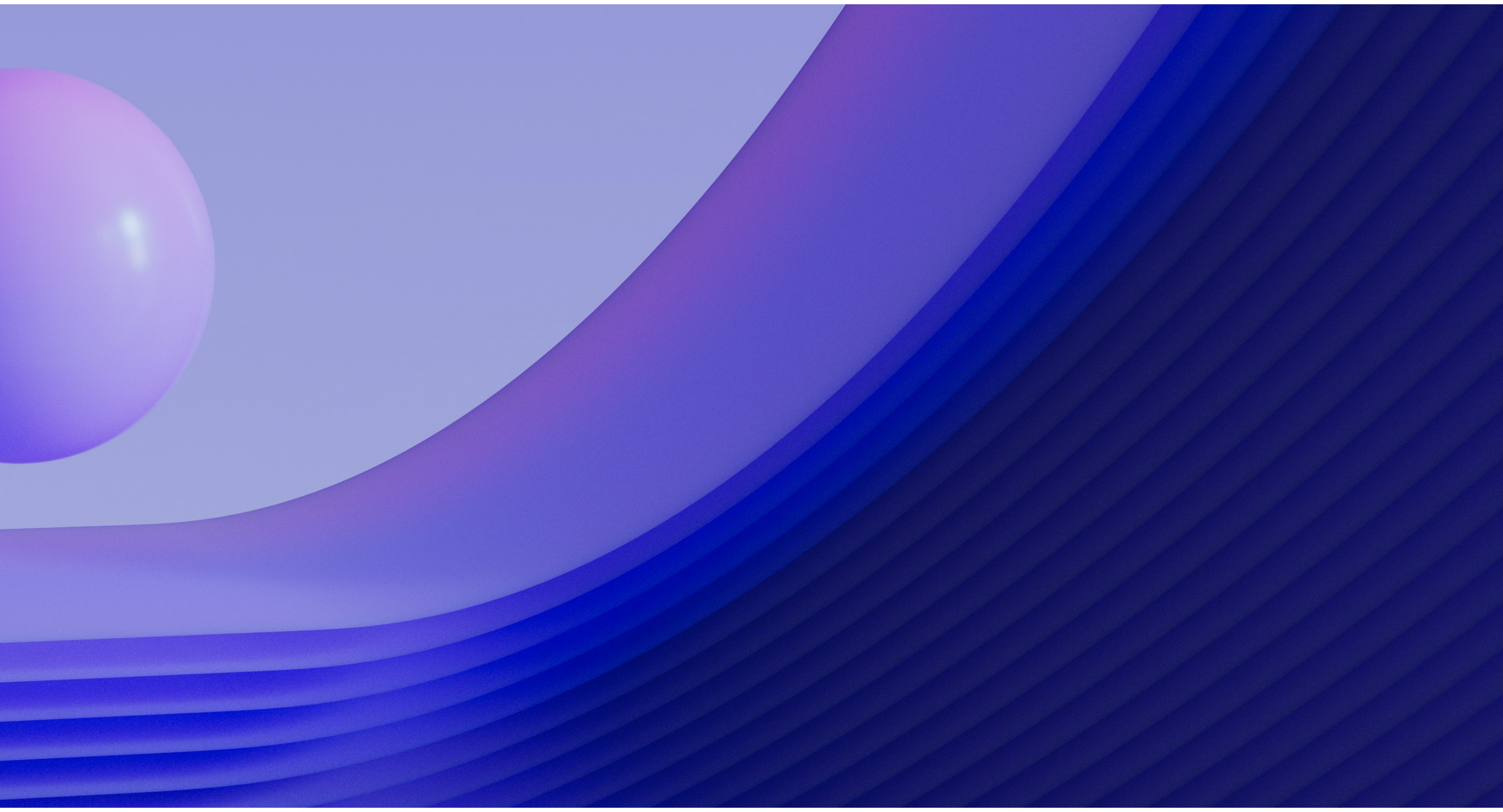
# Robust Risk Culture Stabilises Earnings

**Embedding a strong risk culture within a client-centric strategy** enhances both client selection and ongoing client care. By applying sound risk principles during client onboarding, the bank ensures alignment with long-term strategic objectives and mitigates reputational and financial risks. At the same time, a risk culture that promotes sound judgement and accountability in client interactions fosters trust, transparency, and sustainable relationships.

It is therefore essential that **leaders and employees share a common understanding of which risks should be taken, and which should not**. This shared mindset turns strategy into consistent execution.

A strong risk culture is a real **performance driver.** Empirical research (Bianchi, Carretta, Raina & Fiordelisi, Journal of Banking & Finance, 2021) shows that banks with a well-developed risk culture have **significantly stronger performance metrics**, such as higher ROA, ROE, and return per unit of risk (e.g., using RWA-based masures). These effects remain significant even when controlling for factors like size, capitalisation, and market environment, demonstrating that risk culture acts as an **independent performance factor**.

This research confirms what many leaders intuitively experience: when shared values, norms, and behavioural expectations consistently guide how people identify, discuss and deal with risk, **decision-making improves across the value chain**. Investments become more targeted, portfolios more profitable, and growth opportunities are captured more systematically. In short, a strong risk culture directly supports **top-line growth**.



# The Key to Effective Governance

Financial institutions operate within a well-defined governance architecture: The "hardware" of risk management. These governance mechanisms clarify accountability, reinforce oversight, and standardise decision-making. They are essential for achieving strategic goals and building resilience in a complex, competitive environment. Yet governance only works when supported by a strong risk culture.

Our experience in managing risk within financial institutions shows that governance mechanisms alone rarely determine how risks are managed in practice. **Their true impact depends on how people behave within and around these frameworks** – the cultural norms that shape daily decisions, communication, and accountability.

Boards, executives, and staff share responsibility for embedding this culture across the value chain. Collaboration strengthens transparency, participation, and ethical governance, creating an environment where responsible behaviour and sound risk decisions become the norm.

These cultural drivers set the tone for risk management. They influence whether employees feel empowered to raise concerns, how issues are escalated, and whether risk is genuinely considered or reduced to a box-ticking exercise. When aligned with governance mechanisms, they amplify oversight and decision quality; when misaligned, they create blind spots no policy can fix.

A **strong risk culture** ensures that **governance frameworks are not just implemented but truly embedded**. It connects strategic intent with operational behaviour, enabling institutions to navigate uncertainty with consistency and integrity.

**Examples of how risk culture enhances governance mechanisms:**

- **Strategic Alignment and Risk Appetite:** A robust risk culture ensures that strategic goals and risk appetite are reflected in daily decisions. It fosters transparency in balancing risk and opportunity. Example: When launching a new product, teams fully assess risks against the defined appetite, avoiding misaligned exposure.

- **Process Definition and Risk Mapping:** A strong risk culture drives proactive risk identification and ownership. It supports clear documentation and control implementation. Example: In procurement, risks such as supplier failure are mapped, and controls such as dual approvals are embedded.

- **Roles and Responsibilities Across the Three Lines of Defence:** A mature risk culture reinforces clarity and collaboration across the First, Second, and Third Lines. Example: Business units own risks, risk/compliance functions guide, and internal audit independently assesses controls.

- **Integrated Risk and Control Assessment Tools:** A robust risk culture enables meaningful use of tools such as Risk and Control Self-Assessment, supporting continuous improvement. Example: A digital platform allows process owners to evaluate controls and report residual risks to senior management.

A sustainable risk culture emerges when **governance mechanisms and behavioural drivers align**. Structures guide behaviour; strong culture ensures those behaviours are lived and resilient. Together, they embed risk awareness, encourage responsible decision-making, and maintain operational strength.

# Human Judgement in the Age of New Technologies

As financial institutions increasingly **adopt new technologies** such as advanced automation and GenAI, **employees shift from executing manual steps** in the value chain **to overseeing, validating, and interpreting machine-driven outputs**. This technological evolution further elevates the **importance of human judgement**. When automated processes take over routine tasks, the remaining decisions typically involve higher complexity, ethical considerations, or ambiguous scenarios that cannot be fully codified.

**Strong risk culture becomes the anchor that ensures employees apply sound judgement** when interacting with AI-enabled systems. It guides how staff challenge automated outcomes, escalate anomalies, and make decisions when models behave unpredictably or when data limitations create uncertainty. In environments where technology accelerates execution, a strong risk culture provides the behavioural guardrails that prevent over-reliance on automation and foster responsible use of new technologies.

# Risk Culture Under Increased Supervisory Scrutiny

Supervisory scrutiny of governance and risk culture has intensified across Europe, reflecting a broader shift from evaluating formal structures to assessing the effectiveness of behaviours and decision-making in practice.

The ECB's 2024 Draft Guide on Governance and Risk Culture introduces **"culture as evidence"** as a cornerstone of prudential assessment. Institutions must demonstrate how governance arrangements, escalation mechanisms, and accountability norms translate into measurable outcomes within the risk appetite framework. This marks a significant development: a strong risk culture is now a quantifiable factor directly linked to financial resilience.

Many EU member states are aligning with the ECB's "culture as evidence" approach, integrating behavioural assessments into prudential reviews and supervisory dialogues. This reflects a broader shift from structural compliance to **evaluating how governance translates into decision-making and ethical conduct in practice**, making risk culture a tangible and auditable component for regulatory supervisors (e.g. BaFin in Germany, ACPR in France, CONSOB and the Corporate Governance Committee in Italy, etc.).

Beyond Europe, **global regulators have also sharpened their focus on risk culture**, embedding behavioural expectations into supervisory frameworks. The Australian Prudential Regulation Authority (APRA) has introduced a comprehensive framework of 10 Dimensions of Risk Culture, covering leadership tone, decision-making, escalation, and alignment with values. The Federal Reserve (US) also integrates cultural factors into its supervisory assessments. This highlights the importance of behavioural indicators, escalation mechanisms, and board effectiveness in maintaining safety and soundness.

By **linking internal culture with external transparency obligations**, regulators signal that cultural strength is inseparable from overall organisational accountability and long-term resilience.

Ultimately, there is only one reason **why risk culture matters: it is good by design**. A strong risk culture equips employees to speak up, learn from mistakes, and act with integrity: Driving resilience, trust, and sustainable success.

# 3. From Insight to Action: Steering Risk Culture

Risk culture is a **dynamic phenomenon** within any organisation: One that will evolve, either by design or by default. Steering it intentionally is essential to ensure it aligns with strategic objectives, supports sound decision-making, and reinforces ethical conduct. As a **living system**, it can be **actively shaped** using principles from design thinking – through iterative exploration, stakeholder engagement, and effective problem solving. Structured assessments reveal levers for change and areas of weakness, enabling targeted interventions and continuous development.

This five-step framework – **Define, Assess, Improve, Implement, and Monitor** – guides organisations through the process of aligning their risk culture with their strategic ambitions. Each step builds on the previous one, **translating cultural aspirations into concrete actions and measurable outcomes**.

Figure 2:
**KPMG Model of Change**


**Make it clear**
Align organisational strategy with your ethical values to determine where the organisation wants to be positioned from a culture perspective; define desired risk culture.

**Make it known**
Understand current risk culture and compare it with desired risk culture; identify gaps as well as behavioural enablers; leadership call to action.

**Make it real**
Define the steps needed to achieve your desired risk culture (i.e. roadmap); apply culture change frameworks. This may include revising relevant policies and procedures, conducting interviews, and identifying opportunities for targeted enhancements.

**Make it happen**
Implement the roadmap and define the measures of success at an initiative and enterprise level. Ensure execution through hands-on involvement in key activities that reinforce risk culture, ensuring alignment across the organisation.

**Make it stick**
Measure progress against the roadmap (initiative level) and the evolution of organisational risk culture (enterprise level). This ongoing assessment helps to ensure that changes are embedded and sustained over time.

*Source: KPMG, 2026*

# Make It Clear: Define Your Desired State

Every successful cultural transformation starts with a **clear, shared understanding of what the desired risk culture looks like**. Organisations must define how employees are expected to act when facing uncertainty and risk. Without a common understanding, efforts to influence behaviour will fail.

Key questions to address:

- How do we want people to act when making decisions about risk?
- Which behaviours are acceptable, and which are not?
- What do we want employees to do, or avoid doing, when managing risks?

### Defining What "Good" Looks Like

Establishing a target risk culture means identifying the behaviours that align with the organisation's risk appetite and values. **Design thinking methods** can help by engaging employees early in the process to ensure ownership and practical relevance. This approach fosters:

- **Clarity:** creating shared interpretations of risks, roles, and expectations.
- **Role modelling:** when leaders actively communicate and embody these principles, they signal that a strong risk culture is a strategic priority.

Together these elements provide the foundation for consistent decision-making and credible leadership signals across the organisation.

### Design Thinking

Design Thinking is a human-centred, collaborative approach that can help organisations co-create a shared vision of a strong risk culture by focusing on people, behaviours, and values.

Why is Design Thinking unique?

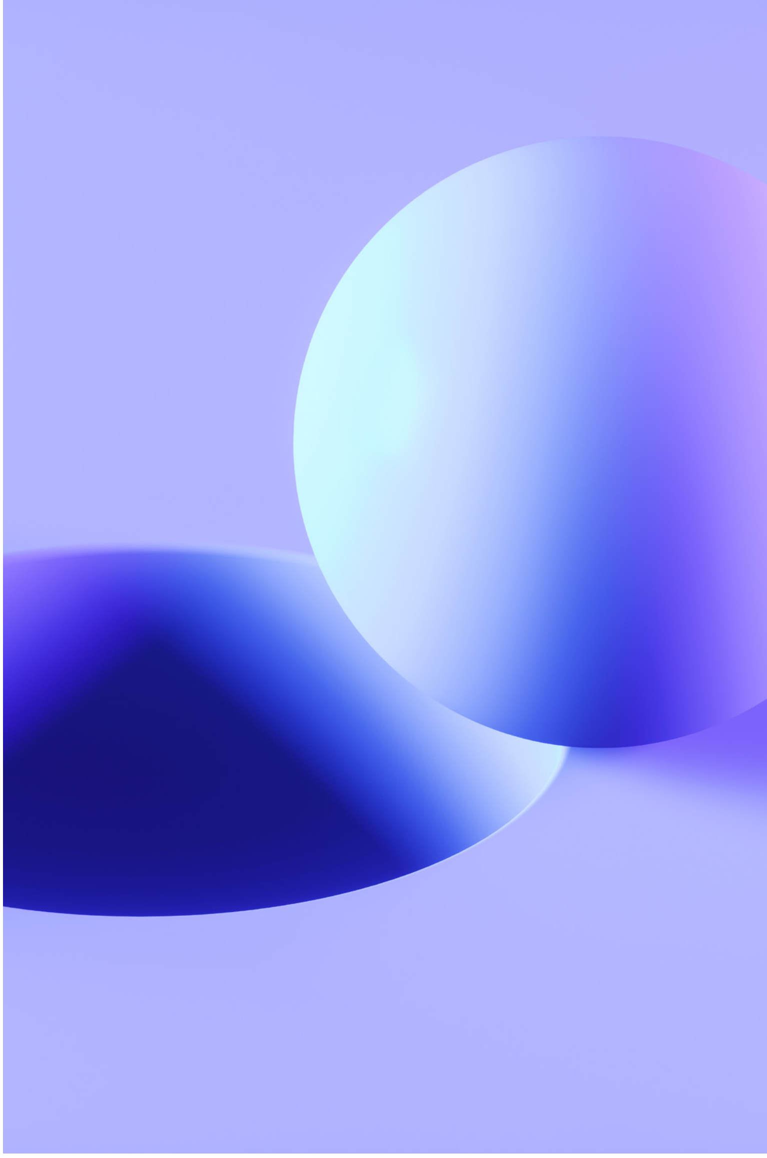
- It breaks away from silo thinking and narrow specialisation by fostering cross-functional collaboration.
- It uses hands-on, experiential methods – such as sketching, role play, and prototyping – because thinking with your hands sparks creativity and clarity.
- It transforms complexity into tangible, actionable ideas, accelerating progress and engagement.
- It values both outcome and experience: the process itself builds commitment and shared understanding.

Core Principles Applied:

- Empathy – Understand current perceptions and attitudes toward risk.
- Collaboration – Involve diverse stakeholders to capture multiple viewpoints.
- Creativity – Explore innovative ways to express and embed cultural elements.
- Iteration – Refine ideas through feedback and discussion.

Expected Outcome: A well-defined target risk culture framework that serves as a foundation for future initiatives, communication, and governance.

# Make It Known: Measuring Risk Culture



As already mentioned, **risk culture continuously adapts to changing environments, emerging threats, and organisational priorities**. The research of Guillem Casoliva (2024) shows that risk culture, and therefore norms of interaction and openness, can also differ significantly across teams within and organisation.

Therefore, treating it as a static, one-time framework can expose organisations to significant vulnerabilities. Organisations must be able to assess their current state, identify gaps, and monitor progress over time. A structured approach to measuring risk culture provides the foundation for targeted interventions and long-term cultural resilience.

## Measuring What Matters: The KPMG Risk Culture Model

Without a structured framework, leaders often rely on intuition or anecdotal evidence, missing blind spots and inconsistencies. A model provides a common language and reference point across the organisation, enabling leadership to assess current behaviours, benchmark progress, and identify areas for improvement. It also supports regulatory expectations by linking culture to governance, conduct, and resilience. Ultimately, measuring culture through a model empowers organisations to steer it intentionally, ensuring alignment with strategic goals rather than drifting towards unintended outcomes.

The **KPMG Risk Culture Model**, introduced on page 6, identifies eight dimensions of risk culture that are **observable, measurable, and influenceable**. In addition to its sound scientific foundation, it leverages 30 years of experience in assessing, measuring, and monitoring the risk culture of financial institutions and leading corporates.

The Risk Culture Model has been widely adopted by regulators such as the **European Banking Authority (EBA)** and the **Dutch Central Bank (DNB)** as well as leading financial institutions and corporates across sectors. It captures both behavioural and governance aspects, making it a valuable tool for measuring and improving risk culture.

# Measuring The Gap Between Current and Desired Risk Culture

To enhance risk culture, organisations need to understand where they stand versus where they need to be. The goal is to identify cultural misalignments that could undermine risk appetite and strategic objectives.

### The Tools

A robust diagnostic approach combines scale, depth, and foresight through complementary methods:

- **Surveys and Benchmarks** – Validated instruments assess risk culture dimensions, enabling bench-marking across teams, business units, and peer institutions. Surveys provide scalable insights and longitudinal tracking.

### Survey and Benchmarks for Scale

Surveys provide a scalable, cost-efficient view of cultural strengths and weaknesses, supporting longitudinal tracking and clustering analysis. Integration into existing feedback channels ensures minimal disruption while maximising reach.

KPMG's survey tool, Sofy, enables robust measurement through structured employee feedback. This survey allows for statistical analyses and internal and external benchmarking, which provides insights into employees' perceptions towards risk culture, integrity and compliance. In addition, it provides insights into the extent to which undesirable risk behaviour takes place in the organisation and the effectiveness of speak-up policies and procedures.

Benchmarking allows companies to compare the results of their own risk culture assessment with industry standards, competitors, or best-in-class organisations. This comparison highlights strengths and weaknesses, offering a clearer picture of where the organisation stands.

The results of Risk Culture Assessments conducted over the past 25 years have been incorporated into KPMG's benchmark database. The benchmark includes data from 70+ organisations and more than 285,000 respondents. The data covers all sectors and includes global insights.

- **Observations** – Directly watching behaviours and interactions reveals how risk culture manifests in practice. Examples include communication styles that indicate either openness or defensiveness, the tone of discussions about risk, and whether dissent is welcomed or suppressed.

### Observations for Context

Communication Styles: How leaders and teams communicate about risk reveals much about the underlying culture:

- Tone and Transparency: Are discussions about risk open and candid, or defensive and superficial? Boards and executives that encourage a "culture of inquiry" foster constructive challenge and avoid groupthink.
- Language Used: Frequent use of compliance-driven language ("tick-the-box") may indicate a rules-based mindset, whereas dialogue focused on outcomes and accountability suggests a more mature risk culture.
- Openness to Dissent: Healthy cultures invite diverse perspectives and debate. Suppression of dissent or over-reliance on consensus can signal cultural weaknesses.

Board Dynamics: Boardroom behaviour is a strong indicator of organisational risk culture:

- Quality of Debate: Effective boards balance challenge and support, avoiding extremes of micromanagement or rubber-stamping. How far directors ask probing questions about risk appetite and resilience is a key indicator.
- Inclusivity and Engagement: Boards that actively value different viewpoints and backgrounds tend to make better decisions and manage risk more effectively. Lack of inclusion can lead to blind spots and poor oversight.

- **Interviews** – Structured conversations uncover blind spots, tensions, and root causes behind cultural misalignments.
- **Advanced Analytics** – Machine learning techniques (clustering, anomaly detection, sentiment analysis) transform raw data into predictive insights.

### Interviews for Insight

Numbers only tell part of the story; conversations reveal the rest. Structured interviews across leadership and frontline roles uncover blind spots, tensions, and root causes behind cultural misalignments. Independent facilitation ensures openness and surfaces dynamics often invisible to internal teams.

KPMG's experts are trained to conduct structured, confidential interviews that go beyond surface-level responses to explore behavioural norms, perceptions of leadership, and the lived experience of corporate values around risk. These interviews are designed to identify misalignments between stated policies and actual practices, helping organisations detect early warning signs of misconduct or misalignment. KPMG's interviewing methodology emphasises psychological safety, neutrality, and consistency, ensuring that interviewees feel secure in sharing candid feedback while maintaining the integrity of the findings.

### Advanced Analytics for Foresight

Machine learning techniques – clustering, anomaly detection, sentiment analysis – transform raw data into actionable intelligence: these tools identify latent cultural patterns and predict areas of potential misalignment before they become critical.

Through its proprietary Culture Assessment Survey, KPMG employs digital diagnostics to capture employee sentiment, behavioural norms, and perceptions of integrity across organisational layers. These results are then benchmarked against industry standards and peer organisations, allowing clients to contextualise their cultural strengths and vulnerabilities.

### Voices That Matter: Good Practices in Listening to Risk Culture

In practice, structured interviews and surveys have proven to be more than just diagnostic tools – they are catalysts for cultural reflection and engagement. One notable good practice is the use **of interviews as a source of strategic impulse**. Insights gathered during interviews have sparked intense and sometimes uncomfortable discussions at board level. These conversations have often revealed blind spots or cultural tensions that had previously gone unnoticed, prompting leadership to re-evaluate priorities and take ownership of cultural development.

Another key practice is the **inclusive nature of perception-based diagnostics**. Employees consistently report feeling more heard and valued when they are invited to share their views, whether through surveys or interviews. While surveys offer broad coverage and comparability, interviews allow for deeper exploration of individual experiences. Many participants have expressed appreciation for the opportunity to speak openly, so their perspectives could be voiced and considered.

These practices not only enhance the quality of cultural insights but also contribute to trust, transparency, and psychological safety – critical ingredients for a resilient risk culture.

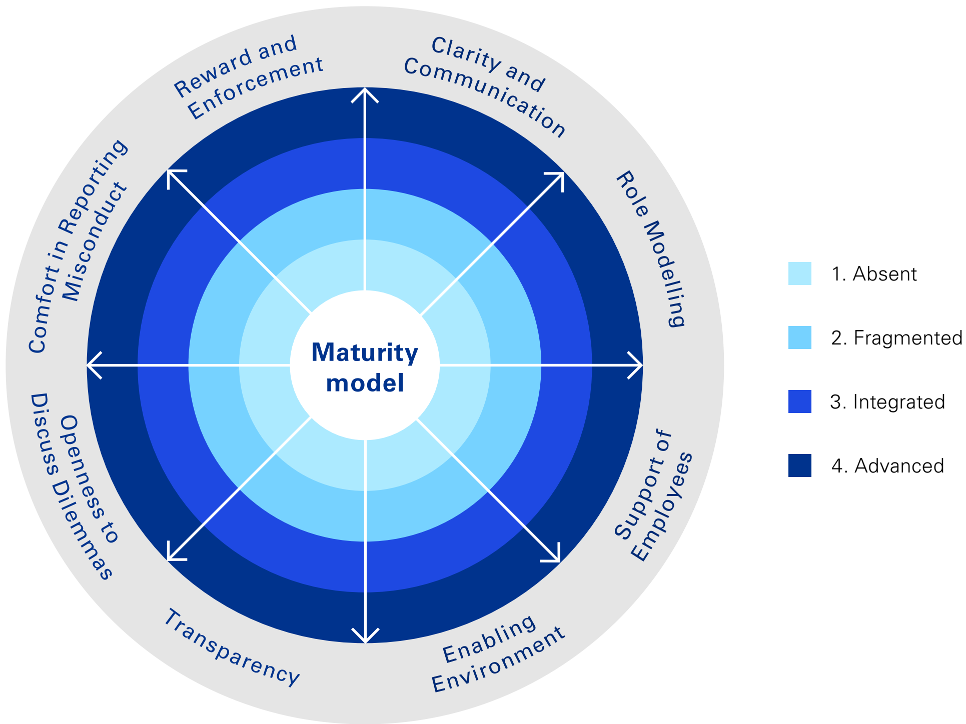
### The Outcome

The combination of methods aims to deliver a comprehensive picture of the existing risk culture and its maturity level. These insights into cultural gaps and strengths are necessary for steering risk culture in the right direction: designing targeted interventions that can ultimately create a cohesive risk culture, a requirement for resilient and high-performing organisations.

# Diagnosing Risk Culture: The KPMG Risk Culture Maturity Model

The KPMG Risk Culture Maturity Model assesses how well risk culture elements are developed and managed. It evaluates the effectiveness and robustness of an organisation's risk management practices and cultural attitudes towards risks. The model helps identify strengths and weaknesses in risk culture and can help ensure that an organisation meets regulatory requirements and stakeholder expectations towards risk management. It consists of four layers:

Figure 3:
**KPMG Risk Culture Maturity Model**




*Source: KPMG, 2026*

**01** **Absent – No defined risk culture; reactive approach to incidents.**
Indicators: No internal reporting lines and minimal awareness of risk culture. Risk culture is irrelevant to internal decision-making and there is a reactive approach to incidents, with most incidents being unreported full stop at end.

**02** **Fragmented – Awareness exists but is inconsistent; policies not uniformly applied.**
Indicators: Internal reporting lines for risk culture are rarely used, and the importance/awareness of risk culture is compliance driven. Risk culture is rarely included in internal decision-making and incidents are only reported in some cases.

**03** **Integrated – Coherent risk culture embedded in operations; proactive risk management.**
Indicators: Internal reporting lines for risk culture are integrated in the second line and the organisation is intrinsically motivated to work on its risk culture. Risk assessments are proactively conducted, and employees feel empowered to speak up and report incidents.

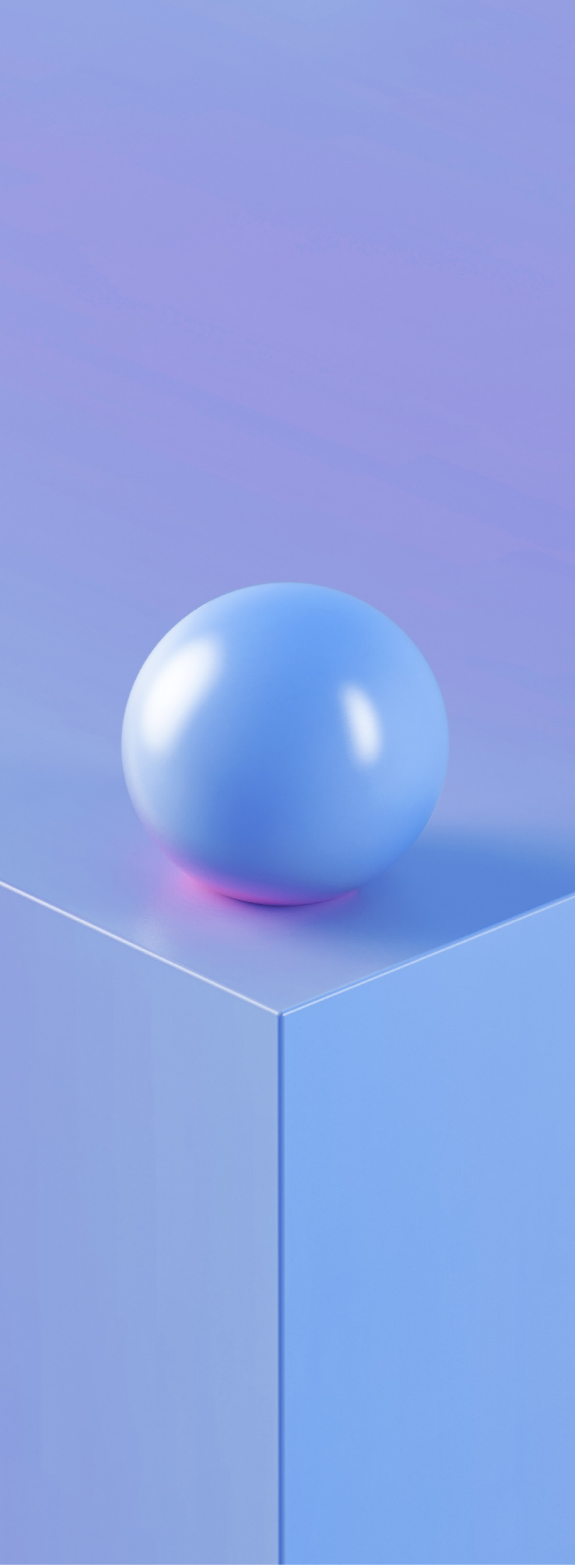
**04** **Advanced – Risk culture fully embedded in decision-making; continuous assessment and learning.**
Indicators: Internal reporting lines for risk culture are integrated in the first line and the organisation considers risk culture a key success factor. Risks are continuously assessed and (nearly) all incidents are reported and seen as a learning opportunity.

Leaders can gain a first insight into the maturity of their risk culture and where it stands today without needing to deep dive into the technical aspects and theories behind it. This grid offers a practical starting point for board members to reflect on their organisation's risk culture. Each row translates complex cultural concepts into observable behaviours and governance practices, making it easy to spot strengths, gaps, and areas for improvement. Whether you are assessing how decisions are made, how risks are escalated, or how ethical conduct is encouraged, the framework helps you build a grounded, first impression of your organisation's cultural maturity in managing risk.

Figure 4:
**Exercise: Where does your organization's risk culture stand?**

| | Level 01: Absent | Level 02: Fragmented | Level 03: Integrated | Level 04: Advanced |
|---|---|---|---|---|
| **Defining risk culture** | No model for risk culture | Using different models accross the organization | Using one pre-defined model | Developing and using own model |
| **Role modelling** | Leaders are disconnec-ted from the team | Risk behaviour discussed during events | Risk culture values brought into decisions | Leadership in risk management |
| **Available resources for risk culture** | No resource for risk culture | Resources allocated when incidents occur | Fixed resources | Risk-based resources |
| **Perceived importance risk culture** | Risk culture is not important | Compliance driven: Meet regulatory expectations | Risk motivated: Culture impacts risk | Value driven: Risk cult-ure is a key success factor |
| **Assessing risk culture** | Risk culture is/was never assessed | Every 3 years or more | Annually | Continuous monitoring |
| **Sharing dilemmas** | Dilemmas are not shared | On ad-hoc basis, top-down | Periodically, top-down | Proactively, retrieved from accross the organization |
| **Reporting concerns** | No internal reporting framework | Reporting line in place, but not being utilised | Frequent use of reporting line | Structural learning from reported incidents |
| **Risks and decision making** | Risk culture is considered irrelevant | Risk culture principles are invoked during incidents | Risk culture principles embedded in key decisions by 2nd Line | Risk culture principles embedded key decisions by 1st Line |

*Source: KPMG, 2026*



# Make It Real: Define the Path to Change

Turning aspirations into action requires a clear roadmap for cultural change. This step focuses on defining practical measures to achieve the desired risk culture and embedding them into daily operations. It involves applying structured change frameworks and translating high-level principles into tangible initiatives.

A well-designed change plan serves as the roadmap for bridging the gap between the current state and the desired risk culture. It helps to keep the focus on those strategic priorities that can address the cultural misalignments identified during the risk culture assessment phase. These priorities should be linked to measurable outcomes and embedded into governance structures.

**Key steps to defining the path to the desired risk culture:**

- **Identify priority areas**. Using the insights obtained during the **Make It Known** step (see page 14), identify which areas of the risk culture can have the highest change impact and which have the most urgency:  high-risk behaviours or processes that could lead to compliance breaches, areas with strong influence on decision-making (e.g., leadership tone, incentives).

- Translate the gaps identified into **specific cultural outcomes** (e.g., stronger accountability, improved openness to challenge).

- **Identify enabling capabilities** such as governance structures, policy frameworks, and risk reporting systems.

- Ensure objectives are **aligned with risk appetite, business strategy, and regulatory expectations**.

# Make It Happen: Blaze the Trail

**Transforming risk culture is a journey** – it requires deliberate action, sustained effort, and the right instruments. There are various methods for embedding and strengthening the desired risk culture in the long term.

For example, organisations can strengthen their risk culture by **embedding values, clarity, and accountability into everyday structures and interactions**.

This includes establishing a value-driven communication and escalation framework, maintaining a coherent and accessible policy framework, and standardising decision-making protocols that promote transparency and thoughtful judgement.

Recruitment processes should incorporate cultural alignment through structured skill matrix assessments, while governance bodies adopt colleagiate working principles to encourage constructive challenge and improve decision quality as part of an **enabling environment**.

Leadership visibility, through listening tours, and a constructive error culture further reinforce trust, psychological safety, and **role modelling** across the organisation.

To sustain cultural integrity, incentives, role design, and recognition systems must reward risk-aware behaviour and responsible decision-making, while boards provide active cultural oversight grounded in **transparency** and robust challenge.

Extending cultural expectations beyond organisational boundaries, into product governance and third-party oversight, ensures that values and risk principles are consistently applied across the full value chain. Together, these interventions create an **enabling environment where norms, behaviours, and controls are aligned**, reinforcing a resilient and sustainable risk culture.

This list is not exhaustive, and many more ways to actively steer risk culture are currently implemented – as illustrated by three examples of practical implemention.

**Insights from KPMG Project Experience**

- Tone at the Top and Role Modelling
  Challenge: "Lack of Leadership Commitment"

  Without visible and consistent support from top management, cultural initiatives lose momentum. The solution is to ensure leaders model desired behaviours and integrate risk culture into strategic priorities and performance metrics. You should reinforce clarity through role modelling and communication – tone from the top matters.

- Incentives and Enforcement
  Challenge: "Short-Termism in Decision-Making"

  Pressure for immediate results often undermines prudent behaviour and long-term resilience. Therefore, you should link risk-aware thinking to career development, rewards, and success stories. Embed risk culture objectives into incentive structures and communicate that cultural change is a continuous, long-term investment.

- Clarity and Communication
  Challenge: "Cultural Resistance to Change"

  Change often triggers scepticism or inertia. To overcome this, it is important to involve all stakeholders to build ownership and understanding. Engage employees through design thinking workshops to foster authentic mindset shifts. External facilitation can add fresh perspectives and credibility, reducing biases and hierarchy effects. Internally moderated workshops often risk limited openness, as participants may hesitate to voice concerns or challenge existing norms.

# Make It Stick: Monitor Progress Towards Desired State

The final step is to monitor progress over time. Once gaps have been identified and interventions initiated, organisations must track cultural development.

### Where we are now

Assessing whether the initially identified gaps between current and desired risk culture have been closed can be achieved by performing a follow-up measurement with consistent methodologies (see page 15). This can be conducted, for example, through a comprehensive survey that measures each of the risk culture dimensions and the extent to which they were impacted through the change programme.

Alternatively, a pulse survey can be used, with a narrower but more focused scope to measure targeted cultural change initiatives, for instance within a specific governance structure (e.g., targeted management layer, specific team or department), model dimension or components (e.g., tone at the top, psychological safety, speak-up culture, value alignment, etc.).

### Where we are going

Key performance indicators (KPIs) can be used to gain continuous insights into risk culture dynamics by tracking attitudes, observable behaviours and systemic changes. KPIs can be tailored to each dimension of the risk culture model and designed in line with the risk culture maturity level.

The list below is a non-exhaustive set of indicators that can be operationalised and structured within a continuous monitoring framework that is fit for purpose in each organisation. Taking into consideration its risk culture goals, an organisation may decide to focus on one or more of its risk culture dimensions.

#### Clarity and Communication

- **Policy Awareness Score:** Assesses how familiar employees are with key risk-related policies.
- **Risk Awareness Score:** Measures how well employees understand risk and how they perceive the effectiveness of risk awareness programmes.

#### Tone at the Top and Role Modelling

- **Role Modelling Index**: Measures if leaders are seen actively demonstrating ethical behaviour.
- **Peer Recognition Index:** Assesses if employees are recognised by peers for risk aware behaviour by peers.

#### Support of Employees

- **Compliance With Risk Policies and Code of Conduct:** Tracks the level of adherence to the organisation's formal policies and code of conduct.

#### Enabling Environment

- **Training Effectiveness Score:** Measures employee perceptions of the usefulness and efficiency of risk awareness training.
- **Decision-Making Confidence:** Assesses how confident employees feel in making risk-aware decisions at work.

### Transparency

- **Risk Culture Gaps Resolved on Time:** Measures the efficiency of the organisation in addressing risk behaviour issues, dilemmas or gaps that are formally escalated.
- **Values Alignment with Third Parties:** Measures the effort made to ensure that the ethical standing of third parties align with the values upheld by the organisation.

### Openness to Discuss Dilemmas

- **Participation in Culture Surveys:** Tracks employee engagement in surveys related to ethical values and risk culture.
- **Psychological Safety Index:** Measures how safe employees feel speaking up without fear of negative consequences.

### Comfort in Reporting

- **Trust in Reporting Channels Score:** Measures employee confidence in the integrity, confidentiality, and effectiveness of reporting mechanisms.
- **Retaliation Perception Rate:** Measures the proportion of employees who fear or experience retaliation after reporting concerns.

### Incentives and Enforcement

- **Risk Culture Embeddedness Score:** Evaluates how well risk culture values and principles are integrated into business processes such as performance reviews and promotions.
- **Pressure to Compromise Standards:** Measures prioritisation of risk culture values by looking at the perceived pressure to meet other business goals at all costs.

Ongoing monitoring ensures that the values of an organisation and the desired behaviours are embedded in daily practices, enabling organisations to adapt, improve, and sustain a strong risk culture over time.

By combining perception-based diagnostics with behavioural KPIs, organisations can build a multi-dimensional picture of their risk culture – one that is both measurable and meaningful. This enables not only reactive correction but also **proactive cultural stewardship**, ensuring that risk culture remains aligned with strategic goals, regulatory expectations, and ethical standards.

# 4. Conclusion

A strong risk culture is a **critical capability for financial institutions seeking resilience and sustainable growth** in an environment characterised by persistent uncertainty, regulatory scrutiny, and accelerating technological change. As described at the outset of this paper, banks and insurers increasingly operate in conditions where risks emerge across the entire value chain and cannot be fully anticipated by rules, models, or controls alone.

Governance frameworks and technology provide essential structure and efficiency. However, in financial institutions their effectiveness ultimately depends on how professionals exercise judgement when facing trade-offs between risk and opportunity in daily decision-making. **A robust risk culture** ensures that **leaders set the right tone**, that **employees share a clear understanding of risk appetite and behavioural expectations**, and that they feel both **empowered and accountable to act responsibly** when formal guidance reaches its limits.

As supervisory expectations evolve towards assessing **"culture as evidence"**, organisations can no longer afford to treat risk culture as an abstract concept. Financial institutions need to **actively measure, manage, and steer their risk culture, anticipate change, and adapt quickly**. When risk culture is intentionally embedded into governance mechanisms, it creates clarity in expectations across roles, consistency in decisions throughout the organisation, and credibility in oversight and challenge.

This integration transforms risk management from a predominantly technical discipline into a **strategic asset that supports trust, financial performance, and long-term resilience**. By explicitly linking cultural ambitions with governance elements such as the Risk Appetite Framework and the Three Lines of Defence, institutions align strategy, behaviour, and control across the full client and product lifecycle.

Building and sustaining such a risk culture requires deliberate and continuous effort: visible leadership, structural alignment, and ongoing reinforcement. When done well, the result is not only stronger compliance and control, but **better judgement, more resilient decision-making, and sustainable value creation in an increasingly complex financial system**.

### How KPMG can help

KPMG enables organisations to steer with intention and ensures that the behaviours they promote enable rather than hinder the organisational response to complexity. Based on their defined cultural goals, KPMG can help organisations embed their risk culture into governance frameworks and decision-making processes, generate resilience, trust, and encourage long-term value creation.

Leveraging the KPMG Risk Culture Model, KPMG helps organisations through:

- **Risk Culture Diagnostics and Benchmarking:** Comprehensive assessments to identify cultural strengths and gaps, benchmarked against industry standards and regulatory expectations.

- **Maturity Assessment and Roadmap Design:** Structured evaluations of current practices with actionable roadmaps for improvement and alignment with governance and risk appetite frameworks.

- **Board and Leadership Engagement:** Facilitation of board dynamics reviews, leadership coaching, and tone-from-the-top interventions to reinforce cultural priorities.

- **Behavioural Change Programs and Targeted Interventions:** Organisation-wide initiatives focused on psychological safety, speak-up culture, and constructive challenges to strengthen decision-making.

- **Incentive and Performance Alignment:** Advice on remuneration structures and performance management systems to reward prudent risk-taking and ethical behaviour.

- **Data-Driven Insights and KPIs:** Development of measurable indicators to monitor cultural health and track progress over time.

- **Root Cause Analysis:** In-depth investigations into cultural breakdowns and conduct issues to uncover underlying drivers, enabling targeted remediation and sustainable change.

- **Data and AI Risk Culture Integration:** Strengthening the Data and AI risk management framework by embedding responsible data use, model oversight, and ethical AI principles firmly within the organisation's cultural norms, behaviours, and decision-making routines.

- **Emerging Risk Frameworks and Scenario Deep-Dives:** Designing and implementing structured emerging risk frameworks, including in-depth scenario analyses to assess strategic implications and impacts on financial and non-financial resources, enabling proactive and forward-looking risk management.

# About the authors

## Paul Hulshof

Partner,
Integrity & Compliance Forensic,
KPMG Netherlands

With extensive experience in strengthening integrity, risk culture and compliance across the financial sector, Paul focuses on how behaviour, leadership and decision-making shape risk outcomes across the entire value chain. His work centres on translating strategy, risk appetite and regulatory expectations into sound judgement and everyday behaviour, particularly where rules or models reach their limits. A key theme in his approach is the role of risk culture as a strategic driver of effective governance and resilience. He emphasises that strong cultural foundations enable constructive challenge, timely escalation and consistent decision-making, reinforcing frameworks such as the Three Lines of Defence and the Risk Appetite Framework. Paul has led numerous risk culture assessments and change programmes for major European financial institutions. Combining behavioural science with qualitative and quantitative diagnostics, he helps organisations turn cultural insights into targeted, measurable and sustainable improvements. He also regularly lectures and facilitates board-level dialogues on risk culture, ethics and leadership.

## Nicolas Coudrieau

Director,
Risk & Compliance Financial Services,
KPMG France

With nearly two decades of experience in shaping operational risk and internal control frameworks across French G-SIBs, Nicolas brings a deep understanding of governance, risk assessment, internal control and regulatory expectations. He has led major Risk remediation and transformation programs, integrating Risk & data governance, front-to-back process reviews, and LoD1/LoD2 framework enhancements. He combines hands-on delivery, benchmark-driven insights, and a pragmatic approach to embedding robust control mechanisms, automation, and risk culture across complex organizations.

## Stefan Lell

Senior Manager,
Risk & Treasury Financial Services,
KPMG Germany

With extensive experience in enterprise-wide risk management and strategic bank steering, Stefan works at the intersection of quantitative modeling, qualitative risk analysis , governance and regulatory frameworks. He takes a scenario-based, integrated perspective considering the value chain across the overall business and operating model, including financial and non-financial resources and associated risks. The objective is to optimise risk costs and strengthen institutional resilience to severe and emerging risk scenarios. He places particular emphasis on the development of risk culture as a key enabler of effective risk management. A strong risk culture aligns strategy, risk appetite and governance with everyday decision-making, strengthens accountability and transparency, and supports sound judgement in situations where rules or models alone are insufficient.

## Ana Calin

Manager,
Integrity & Compliance Forensic,
KPMG Netherlands

With over nine years of hands-on AML and compliance experience in the banking sector, Ana has supported major financial institutions and fintech's in strengthening their governance, controls, and risk management frameworks. Her work spans across the three lines of defence, giving her a deep understanding of how organizational culture shapes risk outcomes. Ana has helped institutions redesign target operating models, governance and processes, enhance accountability, translating regulatory expectations into daily practice. As a champion of ethical culture initiatives across KPMG Global network, she advocates for risk mature environments where integrity, accountability, and responsible leadership guide every layer of the client organizations.

# About the authors


## Kerstin Englhardt

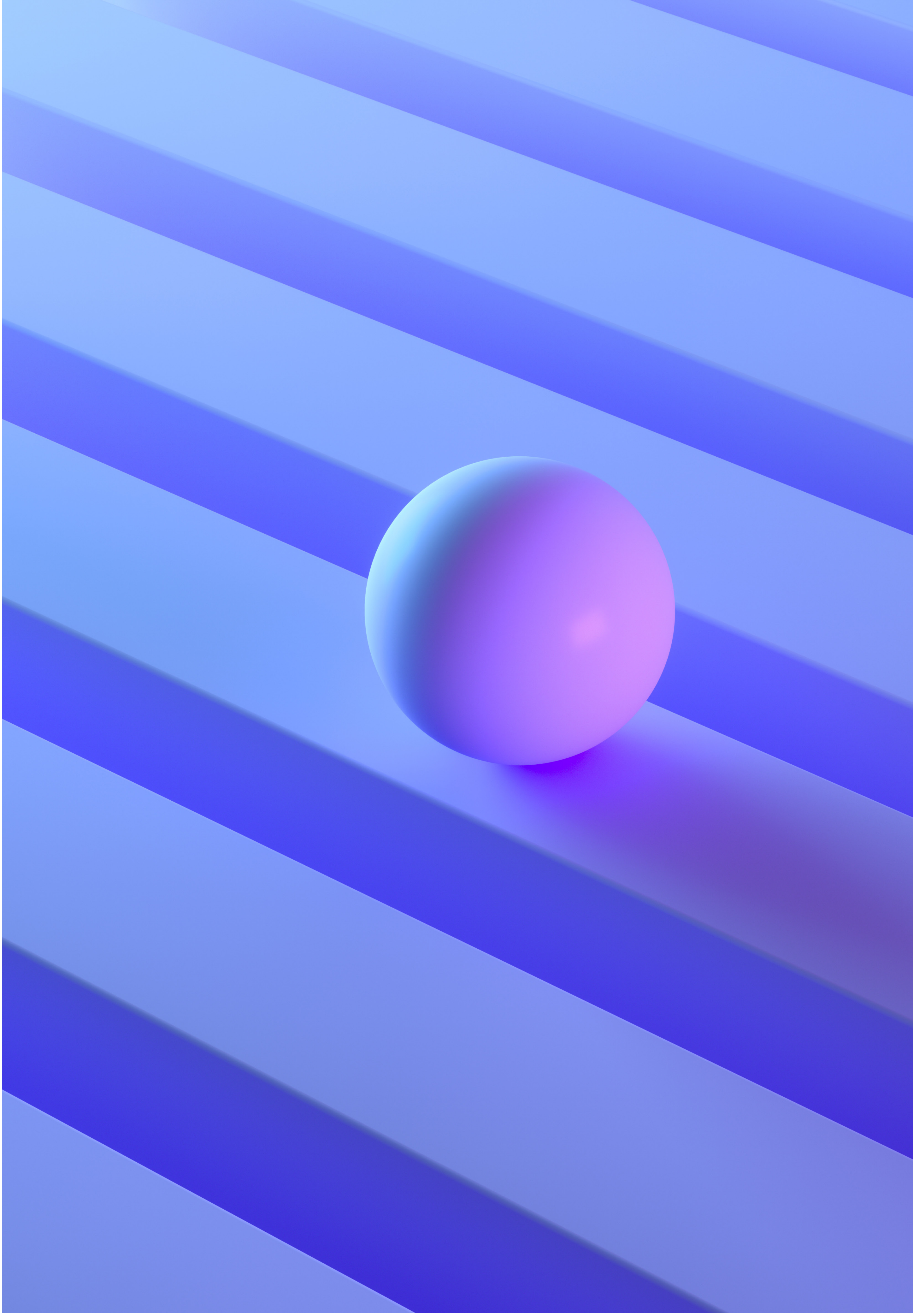
Assistant Manager,
Risk & Treasury Financial Services,
KPMG Germany


With a background in psychology and several years of professional experience in the public sector, she brings a strong interdisciplinary perspective to governance and risk-related advisory work. Her focus lies on strengthening the qualitative dimensions of risk management – particularly risk culture, non-financial risk, risk governance and emerging risks. She combines analytical expertise with a deep understanding of organisational behaviour, helping clients translate regulatory expectations into effective cultural and behavioural practices. Kerstin also brings experience in talent development, assessment and coaching, supporting organisations in shaping leadership, communication and error-management behaviours that drive sustainable risk culture.


## Maxime Rapin

Assistant Manager,
Risk & Compliance Financial Services,
KPMG France


With several years of experience in internal control and operational risk management, Maxime has supported multiple financial institutions in strengthening risk frameworks, enhancing control plans, and aligning governance across second-line functions. He has led risk-based control plan design, optimized RCSA methodologies for banks, and driven remediation programs responding to regulatory expectations.



**Contact**

KPMG Wirtschaftsprüfungsgesellschaft


**Markus Quick**
Partner,
Financial Services,
KPMG Germany
T +49 69 9587-4687
markusquick@kpmg.com

**Stefan Lell**
Senior Manager,
Financial Services,
KPMG Germany
T +49 221 2073-6945
stefanlell@kpmg.com

**Paul Hulshof**
Partner,
Forensic,
KPMG Netherlands
T +31 206 568610
hulshof.paul@kpmg.nl

**Muel Kaptein**
Partner,
Forensic,
KPMG Netherlands
T +31 206 567794
kaptein.muel@kpmg.nl

**Stéphane Salabert**
Partner,
Financial Services,
KPMG France
T +33 155687339
ssalabert@kpmg.fr

**Nicolas Coudrieau**
Director,
Financial Services,
KPMG France
T +33 155686233
ncoudrieau@kpmg.fr


Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

**www.kpmg.de**

**www.kpmg.de/socialmedia**