Non-Financial Risk

Enterprise-wide risk management approach

Spotlight Review

August 2026

About us

Financial Markets Standards Board

Financial Markets Standards Board Limited (FMSB) is a private sector, market-led organisation created in light of the recommendations in the Fair and Effective Markets Review (FEMR) Final Report in 2015. One of the central recommendations of FEMR was that participants in the wholesale markets should take more responsibility for raising standards of behaviour and improving the quality, clarity and market-wide understanding of trading practices. Producing guidelines, practical case studies and other materials that promote the delivery of transparent, fair and effective trading practices will help increase trust in wholesale markets. FMSB brings together people at senior levels from a broad cross-section of global and domestic market participants and end-users. In Committees and Working Groups, industry experts debate issues and develop FMSB Standards and Statements of Good Practice and undertake Spotlight Reviews that are made available to the global community of financial market participants and regulatory authorities.

Spotlight Reviews

Spotlight Reviews encompass a broad range of publications used by FMSB to illuminate important emerging issues in financial markets. Drawing on the insight of Members and industry experts, they provide a way for FMSB to surface challenges market participants face and may inform topics for future work. Spotlight Reviews will often include references to existing law, regulation and business practices. However, they are not intended to set or define any new precedents or standards of business practice applicable to market participants.

Find out more about the Financial Markets Standards Board at **fmsb.com**.

Contents

Executive Summary

Non-financial risk (NFR) emerged as firms sought to manage risks that sit outside traditional financial risk disciplines such as market, credit, liquidity and investment risk, which might apply to a varying degree depending on the firm's business model. In many institutions, its development was closely linked to operational risk management frameworks and evolving supervisory expectations. As business models, technologies and operating environments have evolved, NFR's scope and significance has grown. Across banks, asset managers, market infrastructures and other market participants, increasingly interconnected risks relating to technology, governance, conduct, culture and third-party dependencies can have significant prudential, financial and reputational consequences, reinforcing the need for a more integrated and forward-looking enterprise-wide risk management approach.

Firms have invested significantly in governance frameworks, controls and supporting infrastructure. As a result, firms' NFR management reflects differences in business models, organisational structures, regulatory environments and investment in supporting capabilities. While significant progress has been made across the industry, challenges remain in achieving consistent enterprise-wide integration, forward-looking risk identification and effective translation of risk insights into decision-making and outcomes.

This challenge is particularly important because NFR sits at the intersection of financial and conduct outcomes. Weaknesses in governance, operational resilience, technology, culture or behaviour often originate as non-financial issues but may ultimately crystallise into financial loss, regulatory intervention, and reputational damage. Effective management of NFR is therefore increasingly recognised as a core component of organisational resilience, financial soundness and sustainable performance.

This Spotlight Review examines how NFR is managed in practice, where common challenges remain, and the characteristics associated with more effective approaches.

Drawing on discussions with practitioners, the main observations are:

1. **Ownership and accountability**
   Effective NFR management anchors ownership with the decision-makers closest to the risk creation, supported by expert second-line oversight and challenge. Where responsibility is instead distributed across teams within the first and second lines without clear end-to-end accountability, issues may persist or recur.

2. **Balance between controls and judgement**
   Capability depends as much on expertise, character and sound judgement as on controls, processes and tools. Firms that respond to events mainly by expanding controls risk building extensive, manual and backward-looking frameworks that generate reporting volume without enhancing decision-making insight.

3. **Investment in systems and infrastructure**
   More effective approaches invest in systems, data and NFR infrastructure proactively and selectively, keeping pace with how business models, technologies and risk profiles are evolving. Where investment follows mainly from incidents or regulatory findings, firms are left responding to risks rather than anticipating them.

4. **Incentives and performance frameworks**
   Sound risk management is reinforced where remuneration and performance frameworks reflect NFR consistently alongside financial outcomes. Where NFR remains only partially reflected or marginal within performance management, expectations around escalation and accountability may not be consistently reinforced.

5. **Visibility of risk interactions**
   NFR introduced at earlier stages of the transaction lifecycle – including product design, onboarding or outsourcing – may crystallise later and across multiple risk dimensions. Where these linkages are not clearly understood, issues may escalate before being identified and contained.

6. **Culture and behavioural capability**
   Firms broadly recognise the role of culture and behaviour in shaping risk outcomes. However, this is not consistently supported by behavioural expertise, nor translated into day-to-day practice, root cause analysis or a deeper understanding of the drivers shaping judgement.

7. **Leadership tone**

   Leadership behaviour is a multiplier for risk culture: how challenge is received, how escalation is encouraged and how sound judgement is exercised and modelled under pressure. Leaders shape governance design, escalation routes and incentives so that stated values translate into day-to-day practice. Where leadership behaviour is not consistently aligned with stated values, escalation weakens and exposure increases.

This Spotlight Review outlines three stages of development to support reflection and peer benchmarking. Progress is neither linear nor uniform. A practical indicator of maturity is the extent to which risk culture supports the translation of risk information into timely and effective decisions, particularly in how judgement is exercised in practice.

1. Introduction

What is NFR?

Non-financial risk describes the set of enterprise-wide risks that remain after separating out financial risk (market, credit, liquidity and investment risk). NFR is broader than operational risk. While operational risk concerns loss from failed processes, people, systems or external events, NFR also captures risks arising from behavioural, culture and governance failures, technology and third-party dependency, and strategic missteps.

The key value of the NFR lens is the ability to consider these risks holistically, understand how they interact, and support coherent decision-making and accountability across the organisation.

Unlike financial risks, NFR often does not crystallise through immediate financial loss, instead it materialises through customer harm, service disruption, loss of trust or regulatory intervention, which can still carry significant financial and strategic consequences.

Firms adopt different approaches to defining the scope of NFR. Some take a broad view, encompassing all risks outside traditional financial risks, while others emphasise specific risk types based on materiality or regulatory focus. These approaches often coexist, reflecting differences in business models, structures and supervisory contexts. Effective approaches balance a holistic view for aggregated firm oversight with sufficient granularity at business, desk, asset class or activity level to ensure risks are identified and managed where they arise.

Why is NFR a priority now?

NFR management has become more challenging as products, technologies, regulatory priorities and geopolitical conditions shift, leaving firms to navigate risk environments that are more interconnected, data-dependent and operationally complex.

In practice, these dynamics are being reinforced by several concrete developments, including:

- **AI adoption across operational processes and control activities** (for example, surveillance, monitoring, triage and automation), deepening reliance on data integrity, model governance and effective oversight of automated decision-support.[1]
- **Proliferation of electronic connectivity across venues, counterparties and service providers**, increasing interdependencies between systems, functions and external parties, and amplifying operational complexity.
- **Growing attention to third-party and outsourced arrangements for critical services**, raising resilience, accountability and concentration challenges. Combined with rising dependency on data, technology infrastructure and heightened cyber risk, means failures or weaknesses can propagate quickly across the organisation.

Regulatory focus

Supervisory focus has increasingly incorporated a cultural or behavioural risk perspective, recognising this as a mechanism through which governance and risk appetite operate and support sound risk management and conduct outcomes. As the scope of non-financial risk has expanded, it increasingly encompasses risks driven by culture and behaviours, shaping how risks are identified, discussed and managed. Regulators have also focused on resilience, cyber risk and the need to evidence that appropriate controls and monitoring are in place.[2]

[1] Financial Stability Board, Sound Practices for Responsible Adoption of Artificial Intelligence (AI): Consultation Report, 10 June 2026.

[2] Prudential Regulation Authority, *UK Deposit Takers Supervision: 2026 Priorities*, 15 January 2026.

Some jurisdictions have moved towards outcomes-based regulation, while rising reliance on data has often expanded control and reporting mechanisms – sometimes at the expense of forward-looking insight.[3]

NFR events are often triggered in one part of an organisation but materialise elsewhere, spanning operational, conduct, reputational and financial dimensions. Differences in supervisory approaches across jurisdictions, including definitions, priorities and assessment methods, add further complexity, influencing how firms balance outcome-focused risk management with more defensive or control-driven approaches. This has created tension between the cost of control frameworks and the value they deliver.

Across jurisdictions, supervisors consistently emphasise four elements of risk culture: (i) tone from the top (and within), (ii) clear accountability and escalation, (iii) effective communication and challenge, and (iv) incentives aligned with risk appetite.[4] These determine whether frameworks translate into risk management outcomes, including how underlying behavioural drivers, social norms, operating environments and sound judgement influence day-to-day practices.

Definitions

Definitions and terminology for non-financial risk vary across firms and jurisdictions. Those used here are practical working definitions and not a substitute for existing regulatory, supervisory or firm-specific definitions. Where appropriate, definitions are aligned with terminology commonly used across existing regulatory frameworks.

Figure 1: Glossary of Terms

Glossary of Terms	
Enterprise-wide risk management	A fully integrated framework to identify, assess and manage the full universe of risks arising from a firm's activities.
Financial risk	Market, credit, liquidity and, where applicable, investment risks arising directly or indirectly from exposure to financial assets.
Non-financial risk (NFR)	NFR describes the set of enterprise-wide risks that remain after separating out financial risk. NFR consists of multiple components – operational, conduct, compliance, reputational, technology, third-party and strategic risk – together with behavioural risk, which shapes how these risk types are identified, assessed and managed in practice.
Non-financial misconduct	Actions or omissions by individuals or groups that fall below expected standards of integrity, behaviour or accountability and result in harm to individuals, firms, clients, counterparties or the effective functioning of financial markets.
Behavioural risk	The risk of adverse outcomes arising from how individuals and groups behave in practice, shaped by organisational, social and systemic factors. Behavioural risk is expressed through day-to-day decision making, including how sound judgement is exercised, how challenge and escalation occur, and how accountability is applied.

[3] Starling Insights, Deeper Dive: Supervisors on Supervision, November 2025.

[4] European Central Bank, Draft Guide on Governance and Risk Culture, July 2024.

Glossary of Terms	
Holistic risk & control assessment	Structured processes that draw on insights from across the organisation to identify current and emerging risk to organisational purpose, strategy, resilience and business sustainability. These are often supported by systematic risk & control assessment, e.g. Risk Control Self-Assessment (RCSA), thematic, monitoring or audit reviews.
Organisational culture	The shared values, norms and expectations that influence how people think, behave and make decisions within an organisation.
Risk culture	The elements of organisational culture that shape how risk is identified, assessed, challenged and managed in practice, including behaviours, incentives, accountability and decision-making norms. The effectiveness of risk culture is reflected in whether these behaviours and decision-making patterns support the firm's risk appetite and lead to sound risk management outcomes or give rise to adverse outcomes.

2. Management of non-financial risk

Current approaches

Set out below are certain common features of existing approaches to NFR.

Governance and organisational structure

- Most large financial institutions now reference NFR within their overall risk management frameworks, having invested significantly in governance, specialist capabilities, data and infrastructure to strengthen its management.
- Organisational responses commonly include dedicated non-financial or operational risk teams, often led by a Head of Non-Financial Risk or Head of Operational Risk, supported by governance, reporting and escalation structures.

Balancing firm-wide oversight with business-level granularity

- Approaches to managing NFR vary across business models and activities.
- For example, wholesale and trading activities often require more granular risk assessment at business, product or asset class level, while firm-wide frameworks provide a consolidated view for governance, reporting and oversight.
- Effective NFR management depends on combining a firm-wide view with sufficient granularity to capture business, desk or asset-class-specific processes, controls and risk drivers.

Frameworks, tools and risk appetite

- Current approaches rely on formal policies, taxonomies and control frameworks (supported by aggregated data such as KRIs, issue inventories and thematic assessments) to identify, monitor and report non-financial risks across the organisation. When effective, these mechanisms are anchored in a clearly articulated risk appetite that is translated into thresholds, early warning indicators and defined actions, rather than high-level or absolute 'zero-tolerance' statements that are hard to apply in practice. Where embedded in this way, risk appetite becomes a practical decision tool, supporting accountability, traceability and consistent risk management. Examples of NFR risk indicators may include significant operational incidents, cyber resilience metrics, unresolved audit findings, third-party dependency thresholds, conduct breaches, customer remediation trends or indicators relating to escalation, challenge and accountability.
- Not all non-financial risks can be fully quantified, and some metrics act as imperfect proxies.[5] Firms therefore complement quantitative indicators with qualitative and sound judgement to ensure that risk appetite remains relevant and aligned to decision-making.

Extending the operating boundary to third parties

- Firms increasingly recognise that their effective operating boundary extends beyond the legal entity to include third-party providers and outsourced services. As a result, NFR management often incorporates assessments of technology resilience, data integrity and third-party dependencies, particularly where critical services are involved.[6] This reflects a shift towards managing NFR as an end-to-end concern rather than a series of discrete control activities.

[5] Basel Committee on Banking Supervision, Revisions to the Principles for the Sound Management of Operational Risk, March 2021.

[6] Australian Prudential Regulation Authority, *CPS 230 Operational Risk Management*, July 2023.

Key challenges

Despite increased attention and investment, firms continue to face persistent challenges in managing NFR effectively. These challenges arise from how frameworks interact with organisational structures, incentives and decision-making processes, rather than from the absence of policies, processes and controls.

1. **Ownership and accountability remain fragmented:**
   Responsibility for NFR is often distributed across functions and the three lines model, with limited clarity over end-to-end ownership. While subject matter expertise is well developed, fragmented ownership can make it difficult to form a coherent view where issues cut across functions, business lines or stages of the transaction lifecycle.

   Fragmentation is often most apparent at the point of failure. Where ownership is not clearly anchored in the first line, supported by an effective second line, issues can persist or recur.

2. **Controls and processes can become a substitute for judgement:**
   Firms frequently respond to NFR issues by expanding controls and reporting. Adverse outcomes often arise from how risks are anticipated, interpreted and escalated, as well as from control design (for example automation, timing and hand-offs).

   Enhancements are often reactive, resulting in complex, manual and backward-looking control stacks that generate volume rather than insight and do not evolve with underlying processes. A related challenge is the "use test" where NFR tools and processes are not used or understood by front-line decision makers, they become purely compliance-driven and less effective.

3. **Regulatory-driven granularity and resource intensity (RCSA / legal-entity focus):**
   In some jurisdictions, supervisory expectations require granular RCSAs at legal-entity level. These strengthen documentation and visibility but are often time-intensive, manual and methodology-dependent. This can create duplication across functions and divert attention from judgement-based risk assessment and forward-looking prioritisation.

4. **Investment can be reactive:**
   Investment in systems, data and NFR infrastructure is often driven by regulatory findings or specific incidents, rather than forward-looking alignment with evolving business models and risks. This can leave firms exposed as new risks emerge or existing risks interact.

5. **Incentives are not always fully aligned:**
   Although firms emphasise judgement-based, outcome-focused risk management, remuneration and performance metrics often prioritise financial outcomes. Where NFR outcomes are weakly reflected, expectations around behaviour, escalation and accountability are not consistently reinforced.

6. **Risk interactions are not always fully visible:**
   NFRs introduced at early stages, such as product design, onboarding or outsourcing, can crystallise later through execution, servicing or exit, often interacting with other risks. Where these linkages are not well understood, issues can escalate before they are identified or addressed.

7. **Culture and behavioural capability not consistently translated into day-to-day practice:**
   Culture and behavioural capability play a central role in how risks are understood and managed, including sound, judgement-based decision making. This is often under-reflected in NFR management, which can default to process and technical fixes rather than addressing the drivers of human behaviour that ultimately shape risk outcomes. Where culture remains aspirational rather than embedded in day-to-day decisions, behavioural drivers and

weaknesses in judgement can persist even in firms with extensive frameworks.[7] Gaps often arise where escalation is discouraged, accountability diffused at key hand-offs, challenge does not influence outcomes, or incentives continue to prioritise delivery over risk-adjusted performance.

Increasing AI adoption across operational and control processes adds a further dimension, including risks specific to agentic AI such as unauthorised or erroneous autonomous actions that may only surface once deployed. As AI becomes embedded in decision-making, risk culture increasingly reflects human–agent systems rather than people alone, giving rise to distinct behavioural risks: bias amplification leading to judgement drift ('echo chambers'), unquestioning acceptance of AI outputs ('cognitive surrender'), reduced human effort and accountability when working alongside AI ('commitment deficit'), and diffusion of responsibility for ethically questionable actions delegated to AI ('moral distance').[8]

Taken together, these challenges explain why NFR events often exhibit multiple root causes and span operational, conduct, reputational and prudential dimensions. This highlights the need to move beyond control completeness towards clearer ownership, stronger integration and more effective use of behavioural insight and sound judgement in decision-making.

[7] Group of Thirty, Banking Conduct and Culture: A Permanent Mindset Change, 2018.

[8] KPMG, A New Frontier for Risk Culture: How AI Could Change How We Think About Banking Risk Culture, May 2026.

Principles of effective management

More effective NFR management depends less on the volume of controls, and more on how clearly risks are identified, owned and acted upon through sound judgement. Improvements in outcomes are most evident where NFR management is embedded in decision-making, rather than treated as a downstream assurance or reporting exercise.

1. **Embedding NFR within the business model:**
   Clear corporate purpose and strategy are associated with stronger outcomes only where they are embedded across the organisation and translated into explicit priorities and trade-offs. Where individuals understand how day-to-day decisions contribute to resilience, sustainability and client outcomes, expectations around character and sound judgement in risk management are more likely to be internalised. Strategic decisions are more robust where NFR considerations, particularly resilience, trust and business model sustainability, are addressed directly rather than through downstream control activity.

2. **Clear ownership and accountability for risk outcomes:**
   First-line ownership is most effective where it sits with decision-makers closest to risk creation (for example, desk heads or product leads), rather than resting only at senior management level. The second line adds most value as an embedded subject matter partner, providing challenge, expertise and read-across without duplicating first-line activity. In some firms, elements of oversight sit within a more stand-alone risk function; where this occurs, it is most effective when it complements business ownership. This combination supports clearer line of sight to outcomes and more consistent management across the transaction lifecycle.

3. **Integration of NFR at key decision points:**
   Key decisions such as investment, change programmes, outsourcing, risk mitigation actions and incident response are often taken through separate functional lenses, making cumulative exposure harder to assess. Stronger outcomes are associated with clearer integration at decision points, supported by consistent escalation and cross-risk dialogue.

4. **Forward-looking identification of emerging risks:**
   Managing NFR requires more than periodic reviews and post-incident remediation. More resilient firms emphasise earlier identification and prioritisation through risk horizon scanning, thematic reviews and forward-looking assessments. This supports better anticipation of how risks interact and escalate, particularly in more interconnected environments.

5. **Balance between controls, judgement, behaviour and incentives:**
   More effective approaches review the control environment dynamically to ensure it remains proportional and fit for purpose – testing whether each control genuinely mitigates the risk or has instead become a compensating mechanism for addressing behavioural drivers or a lack of risk-informed judgement. This is reinforced where performance management frameworks and incentives reflect non-financial risk outcomes and support risk-informed decision-making over time.

   Approaches also focus on the value delivered by controls relative to their cost. Where controls become complex, duplicative or detached from underlying processes, they are simplified or redesigned so that risk management activity supports decisions rather than generating volume.

   Behavioural capability further supports understanding of how decisions are made in practice, including how challenge is raised, how escalation occurs, how character and judgement are exercised, and how risk is normalised under pressure. Firms develop this capability alongside the use of root cause analysis to identify underlying behavioural and contextual drivers and strengthen prevention rather than just response.

6. **Simplification and proportionality within the control framework:**
Control environments often expand, while ineffective controls are rarely removed. This can lead to manual, detective-heavy processes that generate noise rather than insight. More effective approaches focus on control effectiveness, proportionality and clearer interpretation of risk signals.

7. **Learning loops:**
Progress often follows significant events, but improvement is sustained only where insights change behaviour and strengthen character and sound judgement. Effective learning loops link incidents and near misses to practical improvements in decision-making and escalation, supported by training grounded in real cases.

8. **Leadership behaviours:**
Tone from the top matters, but outcomes are shaped by the judgement leadership exercised day-to-day, at every level. Independent research across UK financial services found that character (the virtues shaping how leaders govern themselves, exercise judgement and engage others) accounts for 55% of the features practitioners identify as central to good leadership, more than competence or interpersonal skills alone[9].

Beyond acting as role models, leaders shape governance design, escalation routes and incentives so that stated values translate into practice. Where constructive challenge is encouraged and consistently acted upon, risk appetite becomes a practical decision tool; where leadership behaviour is misaligned, escalation weakens and exposure increases.

[9] Oxford Character Project, *Character in UK Finance*, October 2023.

3. Development pathway

Progress towards the principles of effective management set out above is uneven across firms, reflecting differences in starting points, supervisory history and investment in people and infrastructure. This section sets out three stages of development, from fragmented and reactive practice to full strategic integration, to help firms locate their own position against those principles. Firms rarely sit neatly within a single stage with progress along the pathway being neither linear nor uniform, and organisations may display attributes associated with more than one stage at the same time. The pathway is a lens for dialogue and peer benchmarking, rather than a definitive assessment of institutional quality.

Key Attributes	Stage 1 Unconnected and reactive	Stage 2 Coordinated silos	Stage 3 Strategic integration
1 Purpose	• Vague at firm or individual level • Rarely features in live discussions	• Insufficiently aligned with strategy • Siloed discussions	• Aligned and well communicated • Drives long term sustainability
2 Strategy and NFR	• Strategic decision making isolated • Little to no NFR consideration	• Strategic decision making siloed • Holistic NFR view not yet possible	• Holistic strategic decision making • Enterprise-wide NFR strategy
3 First Line Ownership	• 1st line leads in some roles only • Overall control sits in the 2nd line	• 1st line ownership is asserted • Duplication and controls persist	• 1st line ownership fully recognised • Active cooperation and alignment
4 Internal connectivity	• Staff stay within bounds • Speak-up relates to red flagging	• Formal cross-unit conversations • Pursuing engagement encouraged	• Open channels in all directions • Safe environment understood
5 Silo oversight and drivers	• All units overseen within bounds • Limited cross-unit knowledge	• 3rd line observations leveraged • Thematic reviews develop	• Career pathing across silos • Root cause analysis dominates
6 Holistic risk & control assessment	• Narrow reviews for financial, risk and regulatory reporting	• Periodic reviews include staff from other functions	• Formal firm-wide exercises • Extra reviews tiggered by events
7 Risk identification	• Many discrete units and risks • Weak strategic connections	• Some forward-looking risks • Some scenario-based analysis	• Thematic approach to risk • Integrated root cause analysis
8 Behaviour vs controls	• Controls totally dominate • All decisions centrally escalated	• Heavy control environment • Some behavioural expertise	• Moderating control environment • Advanced behavioural expertise
9 Learning	• Slow response to events/incidents • Ad hoc staff development plans	• Fast response to crystallised risk • Tailored training quickly rolled out	• Continual learning embedded • Judgement treated as a key skill
10 Leadership	• Leadership behaviour not consistently aligned with risk outcomes	• Tone from the top is clearer but inconsistently applied in practice	• Tone reinforced consistently across leadership levels

Stage 1 – Unconnected and reactive

Description

The organisation underplays non-financial risk as a concept, with management activity largely driven by incidents, regulatory requirements or external pressure. Efforts are primarily focused on avoiding penalties or reputational damage rather than on proactive, outcome-driven risk management.

Key attributes (*numbered for ease of reference only*)

1. Corporate purpose is unclear or not translated into individual roles or decision-making.
2. NFR is rarely considered in strategy, product development or business planning.

3. Ownership remains fragmented, with over-reliance on second line functions for control and oversight.
4. Risk identification is discrete, backward-looking and primarily driven by incidents, audits or regulatory findings.
5. Risk scanning is limited and largely embedded in periodic or regulatory processes rather than continuous assessment.
6. Cross-silo interaction, information sharing and escalation are constrained and centralised.
7. Accountability is focused on control frameworks rather than on end-to-end risk outcomes.
8. Controls, reporting and remediation activity are emphasised over judgement, behavioural insight and decision-making quality.
9. Incident response is often slow and weakly linked to learning, capability development or behavioural change.
10. Leadership messaging is not consistently aligned with risk management expectations, and tone from the top has limited practical effect on day-to-day behaviour.
11. Incentives and performance management remain largely driven by financial outcomes; escalation is perceived as risky and accountability is not consistently reinforced.

Strategic considerations

- NFR implications are rarely considered in strategic deliberations.
- Risk appetite is undefined, vague or expressed in generic terms.
- Risk thresholds and limits for NFR are not established or operationalised.
- Cultural issues (behaviour, accountability, character and judgement) are addressed reactively, after problems arise.
- Roles across the first, second and third lines overlap, duplicate or remain unclear.

Joining the dots

Risks are identified and monitored but remain largely discrete, with little or no aggregation. This results in an absence of meaningful enterprise-wide risk assessment.

Stage 2 – Coordinated silos

Description

The organisation adopts a more coordinated approach to NFR, integrating it into governance, decision making and performance management processes. However, unprompted interaction across organisational units remains inconsistent and sub-optimal.

Key attributes

1. Corporate purpose is articulated and promoted but not fully embedded in strategy or decision-making.
2. NFR is increasingly reflected in governance, strategy discussions and risk appetite frameworks.
3. First-line ownership is strengthening, though duplication, gaps and unclear accountability persist.
4. Cross-silo engagement is improving, supported by thematic reviews and broader participation.

5. Scenario-based and thematic risk assessments exist, but remain partial, inconsistently forward-looking and weakly linked to strategy.
6. Risk identification expands beyond incidents but remains uneven, with limited read-across and integration.
7. Behavioural considerations are recognised, but specialist behavioural expertise and sound judgement are not consistently embedded, and control frameworks remain dominant, often manual, detective and rarely retired.
8. Events and regulatory triggers drive enhancements, including reporting, training, risk mitigation and change programmes.
9. Tone from the top is clearer, with defined target behaviours, but application is inconsistent across business lines and weak at key hand-offs.
10. Escalation, accountability and incentives are improving but remain uneven, particularly across the transaction lifecycle.

Strategic considerations

- NFR is considered in strategy, product design, outsourcing and growth initiatives.
- Risk appetite statements incorporate behavioural, operational and reputational dimensions.
- Some thresholds and limits are in place for key non-financial risks.
- Leadership increasingly recognises that NFR events can drive material financial outcomes.
- A limited set of risks is addressed within familiar categories, with partial consideration of interconnections.

Joining the dots

Some risk interconnections are identified and monitored, and limited aggregation supports elements of enterprise-wide risk assessment.

Stage 3 – Strategic integration

Description

NFR is fully embedded within organisational management and planning. Oversight extends beyond controls to include behaviour, resilience, trust and long-term value creation.

Key attributes

1. Corporate purpose is clearly understood and embedded, with individuals aligned to organisational objectives.
2. NFR is recognised as a strategic capability supporting both resilience and long-term value creation.
3. Ownership is clearly anchored in the first line, with organisational structure, capability and infrastructure aligned accordingly.
4. Risk culture is strong, supported by psychological safety, effective challenge, accountability, professional character and high-quality judgement.
5. Cross-silo collaboration, root-cause analysis and knowledge-sharing are embedded and systematically applied.
6. Forward-looking risk identification is well-developed through horizon scanning, analytics, stress testing and early warning indicators.

7. Decision-making integrates NFR alongside financial considerations, supported by data, technology, specialist expertise and SME judgement.
8. Control frameworks are proportionate and outcome-focused, balancing prevention, detection and informed risk-taking.
9. Behavioural and cultural drivers are actively managed, supported by appropriate expertise and capability, with consistent reinforcement through training and recognition.
10. Leadership actively models professional character and sound judgement, with tone from the top consistently reinforced at all levels of management.
11. Incentives, accountability and escalation are aligned with sustained risk outcomes, reinforcing risk-informed decision-making.

Strategic considerations

- Boards and senior management engage regularly with NFR topics as strategic assets rather than as cost centres.
- NFR management is leveraged as a competitive differentiator (e.g. trust, brand strength, customer loyalty).
- Strategic decision-making balances growth, sustainability, social licence and NFR considerations.
- The organisation anticipates emerging risks (e.g. AI ethics, conduct, workforce well-being).
- Infrastructure is streamlined and right sized to align with strategy and business model.

Joining the dots

Multiple risks and thematic concerns are identified through regular horizon scanning in a joined-up approach involving business risk owners and SMEs. Risk aggregation provides a more holistic enterprise-wide view, while simultaneously enabling effective risk management at business, product or asset class level through partnership between second line specialists and relevant front office teams.

4. Conclusion

Non-financial risk is a central factor shaping the resilience, credibility and sustainability of financial institutions. As operating environments have become more complex, uncertain and interconnected, weaknesses in areas such as conduct, operational risk, technology, data and third-party management can escalate rapidly across organisational, reputational and prudential dimensions.

This Spotlight Review highlights that the challenge for firms lies less in the absence of frameworks, policies or controls, and more in translating these into effective decision-making and day-to-day behaviours. Fragmented ownership, control-heavy responses and limited integration across business and transactional activities continue to hinder timely identification and management of NFR, particularly where risks interact.

More effective approaches are characterised by clear ownership, integration of NFR at the point of decision, and an appropriate balance between controls and judgement. Where these are in place, NFR supports not only governance and conduct objectives, but also prudential soundness and financial resilience by reducing the risk that non-financial weaknesses amplify into financial loss or undermine confidence.

For firms, this implies a shift in emphasis from framework completion to operating effectiveness. Developing non-financial risk management as a core capability requires clear ownership at the point of decision, stronger integration across business activities, and consistent use of judgement supported by appropriate incentives and behavioural capability. Firms that strengthen these areas are better positioned to identify risks earlier, respond more effectively under pressure and maintain trust with clients, markets and regulators. In an environment characterised by greater complexity and uncertainty, this is not only a risk management priority, but a source of resilience, strategic capability and long-term stability.

Looking ahead, practitioners have identified possible deep-dive work on the evolution of NFR frameworks, including:

- **Ownership and accountability,** including practical guidance on the effective discharge of accountability and decision-making;
- **Risk culture, character leadership and behavioural capability,** including the role of challenge, escalation and judgement in supporting sound risk outcomes;
- **Interconnectivity of financial and non-financial risk,** including how interdependencies are identified, monitored and managed in practice; and
- **AI adoption**, **governance and risk management,** including effective oversight of automated decision-making and alignment with evolving industry best practice.

This could help translate the Spotlight Review's themes into practical guidance in the form of good practices strengthening implementation and further embedding NFR into business decision-making.

Appendix 1 – Case studies

These case studies illustrate how NFR interacts with financial outcomes in practice, drawing on real-world scenarios and bilateral discussions across member firms. They explore how weaknesses in non-financial risk management can translate into financial loss, regulatory intervention, client detriment or loss of confidence – and, conversely, how more integrated, forward-looking approaches have supported better financial and strategic outcomes. The case studies reflect attributes across the different stages of development and themes explored in this review. The case studies are illustrative only, intended to draw out elements of the narrative developed in the main body of this paper. They explore areas that are subject to existing regulation and supervisory guidance, which will always prevail.

Case study 1: System outage in markets

Scenario

Two separate Markets businesses are pursuing growth through higher client activity, increased volumes and expanded product coverage. As part of this strategy, the business heads, as risk owners, assess how growth may change the firms' risk profiles.

At both firms, it is identified that resilience risk will increase due to greater reliance on core trading systems, higher transaction volumes and reduced tolerance for disruption during market stress. The businesses develop a plan to strengthen core systems, improve trade capture controls and reduce reliance on manual processes, aligned to planned growth.

Firm A implements this plan fully ahead of the growth in activity, establishing clear ownership, coordinated cyber and technology oversight, and tested fallback processes. Firm B's implementation lags behind the pace of growth, leaving ownership less clearly defined and technology and cyber oversight less well integrated at the point the following incident occurs.

During a trading day, a core front-office trade booking system becomes unavailable. This system is the sole source of record for the firm's FX trading and supports downstream processes. Automated hedging is disrupted, client electronic trading is constrained, and trade capture becomes unreliable.

As a result, risk, P&L and operational data are incomplete, limiting the firm's ability to accurately assess or hedge exposures during a volatile period. The root cause is initially unclear, and a cyber compromise cannot be ruled out. The outage degrades operational capability, weakens normal control processes and places pressure on decision-making, forcing the firm to rely on manual workarounds while determining whether and how trading activity can safely continue. Financial outcomes such as P&L volatility, unmanaged exposures, hedging losses and reduced profitability are potential consequences of these non-financial risk drivers.

Risks crystallised

Risk type	How the risk crystallised
Operational risk	An outage may cause immediate disruption by potentially creating trade capture gaps, which could force reliance on manual processes, informal records and workaround solutions that, in some cases, may not be adequately controlled. Under pressure, teams may continue trading with limited visibility of exposures, and staff may be unclear on who has authority to restrict trading, approve manual processes or escalate issues.

Risks crystallised	
Risk type	**How the risk crystallised**
Technology risk	Pressure to restore systems could reintroduce vulnerabilities and expose confidential information. When trading is disrupted, there may be strong pressure to restore service quickly, and if Technology and Cyber teams are not empowered to challenge that pressure, the firm may prioritise speed over safe recovery. Multiple, inconsistent data sources could also emerge across functions, limiting consistency of information: teams may rely on local views and defend their position rather than reconcile differences, which may result in management being unable to determine the firm's risk position accurately, reducing the firm's ability to respond to the issue.
Compliance risk	An outage may increase the risk that trades are executed without complete and accurate records, leading to weakened surveillance capabilities, delays in regulatory reporting and insufficient evidence to support decision-making. This may result in regulatory scrutiny regarding the firm's operational resilience. While a firm may document its decisions, without a culture where teams are empowered to challenge, there is a risk that these decisions are not robust enough.
Conduct risk	There is a risk that clients receive different quality outcomes, for example, delays and inconsistent pricing. During disruption, staff may be tempted to provide overly reassuring messages, avoid difficult conversations or prioritise certain clients without clear criteria.
Reputational risk	Inconsistent client treatment of the kind described above could result in deterioration of client confidence.

Firm A v Firm B: Comparative response		
Risk type	**Firm A**	**Firm B**
Operational risk	Establishes clear ownership and a shared operating view across functions. Uses controlled fallback processes and restricts activity where risk is not understood, prioritising control over continuity.	Desks develop local workarounds and continue trading based on partial information. Ownership is unclear and escalation is delayed, with pressure to maintain activity overriding risk visibility.
Technology risk	Treats the outage as potentially cyber-related from the outset. Engages Cyber team early and takes coordinated decisions based on risk understanding rather than urgency. Continually invests in cyber security capabilities. Establishes a single agreed view of trades, exposures and uncertainties and real-time monitoring via integrated systems which enable prompt detection. Decisions are made with clear understanding of data limitations across functions.	Treats the issue as a technical failure. Cyber team involvement is delayed, and decisions are driven by pressure to restore trading quickly. Invests in cyber security capabilities only when incidents or losses occur or supervisory action arises. Operates with fragmented data and competing views. Decisions are delayed and inconsistent due to lack of a common risk picture.

Firm A v Firm B: Comparative response		
Risk type	**Firm A**	**Firm B**
Compliance risk	Escalates early, assigns clear decision ownership and records key decisions. Can demonstrate how risks were assessed and decisions were made.	Escalation is inconsistent and ownership unclear. Decisions are taken locally or too late, with limited evidence of coordinated judgement.
Conduct risk	Provides consistent and transparent communication with clear ownership and oversight. Client treatment is aligned to defined principles rather than local judgement or commercial pressure.	Communication varies across desks with inconsistent messaging. Some clients are prioritised, leading to uneven treatment.
Reputational risk	Consistent, transparent communication under clear ownership helps contain reputational exposure rather than allowing it to build through inconsistent treatment.	Uneven treatment and inconsistent messaging, of the kind described above, lead to loss of confidence.

Before disruption occurs (preventative)

- Has the firm pre-agreed who owns the decision to continue, restrict or pause activity, rather than leaving this to be resolved once systems are already under strain?
- Has the firm defined, in advance, what level of operational, conduct, cyber and market exposure is acceptable while system capability is degraded?
- Are Front Office, Operations, Technology, Market Risk, Compliance, Cyber and senior management already positioned to work from the same information, and has this been tested?
- Are people trained and encouraged to escalate uncertainty early, rather than only discovering under pressure whether they feel able to?
- Are fallback processes simple, usable and understood, and has this been tested, rather than assumed, leaving staff to improvise?
- Is the firm's incident framework designed, from the outset, to treat this type of event as an enterprise risk issue, rather than a narrow technology failure?
- Does the firm use root cause analysis of near misses and past incidents to identify vulnerabilities that may apply to other risk types or businesses, before they crystallise elsewhere?

Once disruption occurs (reactive)

- Who is exercising the decision to continue, restrict or pause activity, and is that single point of ownership clear to all functions involved?
- Are Front Office, Operations, Technology, Market Risk, Compliance, Cyber and senior management working from the same information in real time?
- Are people escalating uncertainty early, or are they under pressure to keep trading?
- Once the incident is contained, what vulnerabilities does the event demonstrate, what is the root cause of the issue, and do these vulnerabilities apply to other risk types or businesses within the firm?

Lessons learned

- The same system outage can lead to very different outcomes depending on the strength of non-financial risk management. Firm A contains the event through clear ownership, coordinated decision-making and disciplined response under pressure, while Firm B experiences a broader breakdown driven by fragmented ownership, weak escalation and inconsistent decision-making.
- Non-financial risk capability is demonstrated not by the volume of controls, but by the firm's ability to understand risk, align responses across functions and act decisively under stress.

Case study 2: Automated trading – operational risk, control and governance

Scenario

Two firms are pursuing growth through increased use of automated trading. As part of this growth strategy, the business heads, as risk owners, assess how greater reliance on automation may change the firms' risk profiles.

At Firm A, it is identified that greater use of automated trading creates increased dependency on models, data, technology and automated decision-making. At Firm B, the trading strategies are viewed primarily as an efficiency tool without sufficient consideration to the additional non-financial risks they may present.

During a period of market volatility, an automated trading strategy begins generating trades and exposures that are inconsistent with the firm's intended investment or execution objectives. The strategy uses automated decision-making to identify trading opportunities based on large volumes of market and non-market data.

The issue is triggered by a combination of flawed market data and changes in market conditions that were not well represented in training datasets. As market conditions evolve, the automated strategy identifies patterns that lead it to increase exposures in ways that traders did not anticipate. The model rapidly increases positions across multiple markets, creating unintended concentrations, liquidity exposures and market risks before the issue is identified.

The immediate financial outcomes include trading losses, increased transaction costs, forced position unwinds and underperformance. However, the underlying event is a non-financial risk event with issues arising from weaknesses in model governance, control design, monitoring, escalation and decision-making.

Risks crystallised	
Risk type	**How the risk crystallised**
Operational risk	The strategy may generate trading activity that cannot be supported by existing risk and control function capability or capacity and is therefore outside the firm's intended risk appetite. Traders and support functions may be required to intervene quickly to understand exposures, restrict trading activity or unwind positions while operating under market pressure and uncertainty. The firm may also not fully understand to what extent automation has contributed to decision-making, given the pace at which it has been adopted across the organisation. 'Human in the loop' is often treated as a reliable safeguard, but this assumes the human retains the expertise and judgement to challenge the system effectively. Increasing reliance on automation may, over time, erode human capabilities relating to judgement, challenge and critical thinking, reinforcing the importance of maintaining appropriate accountability, expertise and oversight.
Technology risk	The volume and speed of trading generated by the automated strategy may exceed the capacity of the trading system. Processing backlogs may emerge, trade records may be delayed or incomplete, and Operations teams may lose visibility over the firm's true positions and exposures. Incorrect, incomplete or stale data may further distort investment decisions and create uncertainty regarding positions, exposures and performance; during the incident, different functions may have inconsistent views of positions, exposures and potential losses, reducing management's confidence in the accuracy of risk, portfolio and operational information during a critical period.
Compliance risk	The firm may struggle to demonstrate that the strategy was appropriately tested, approved, monitored and governed. Regulators may scrutinise model governance, automated trading controls, investor protection and risk management practices.
Conduct risk	There is also a risk that trading activity is significant enough to undermine market integrity and lead to volatility.
Reputational risk	Clients may question whether the firm exercised appropriate judgement and oversight once emerging concerns were identified. Decisions to continue operating the strategy despite warning indicators may create perceptions that performance objectives were prioritised over market outcomes, weakening confidence in the firm's governance and investment process.

Firm A v Firm B: Comparative response		
Risk type	**Firm A**	**Firm B**
Operational risk	Identifies automated execution as a material operational risk, with clear ownership, escalation routes and intervention procedures in place before launch. The models underpinning the trading strategies are subject to validation, independent review, stress testing, periodic reassessment and ongoing monitoring, with key assumptions, limitations and failure scenarios documented and understood across Trading and Risk. Maintains an inventory of where automation is used across investment, operational and risk management processes, enabling the firm to understand the role automation played in an incident and respond appropriately. Maintaining this level of independent challenge and named ownership is what guards against human agency disengagement as automation scales.	Exposure is not fully understood, and uncertainty exists regarding who can stop the strategy and how escalation should occur. Has more limited visibility of where automation is used across the organisation; rapid adoption has outpaced robust governance, making it difficult to determine whether automation contributed to the incident or the scale of the resulting risks. This combination of reduced scrutiny and diffused accountability for automated decisions is consistent with the lack of human agency and ownership risk highlighted in the review.
Technology risk	Understands that an automated trading strategy can impact downstream systems, monitoring trading volumes against system capacity with circuit breakers and escalation triggers linked to STP, trade capture and settlement processes. Establishes a single view of positions, exposures and model performance, escalating data issues quickly.	Focuses on the algorithm rather than downstream impacts; trading volumes exceed system capacity, creating processing backlogs, reconciliation issues and reduced visibility of positions and exposures. Different groups hold different views of exposure, delaying decision-making.
Compliance risk	Can evidence how the strategy was approved, governed and controlled, and how decisions were made during the incident.	Documentation, accountability and decision-making trails are less readily evidenced. Approach may fail to meet regulatory rules or guidance including around model risk management and automated trading controls.
Conduct risk	Considers conduct risks during model design and testing. Uses limits, oversight and surveillance to identify potentially inappropriate trading behaviours.	Focuses primarily on investment performance. Potential conduct concerns are identified only after they have generated regulatory, investor or reputational issues.

Firm A v Firm B: Comparative response		
Risk type	**Firm A**	**Firm B**
Reputational risk	Clients retain confidence because the firm can demonstrate that governance, independent challenge and human oversight operated alongside investment controls.	Clients lose confidence once it becomes apparent that performance was prioritised over governance and oversight.

Before deployment (preventative)[10]

- Does the firm have a clear, firm-wide view of where automation and model-driven decision-making are used across the business, and how that picture evolves as strategies scale?
- Is independent challenge built into how new automated strategies are developed?
- Is ownership and accountability for the strategy's ongoing performance and risk clearly anchored, including who is responsible for identifying and acting on emerging concerns?
- Are governance and oversight arrangements proportionate to the pace and scale at which automation is being adopted, and revisited as reliance grows?
- Does the firm maintain the judgement, expertise and challenge capability needed to intervene effectively, recognising that oversight can be eroded by increasing reliance on automation over time?
- Are lessons from automation elsewhere in the business drawn on to inform how new strategies are governed, rather than treating each as a standalone initiative?

Once behaviour becomes abnormal (reactive)

- Are Risk, Technology and Front Office working from the same information as positions accumulate?
- Are people encouraged to escalate concerns when behaviour appears abnormal?
- Who has authority to pause or disable the strategy, and can they act quickly enough?
- Following the event, do similar vulnerabilities exist elsewhere in the investment platform?

Lessons learned

- Effective non-financial risk management is demonstrated by a firm’s ability to understand where automation creates exposures, challenge assumptions, intervene rapidly when behaviour becomes abnormal and apply lessons across the broader investment platform.
- Left unmanaged, increasing reliance on automation can erode the judgement, challenge and sense of ownership that 'human in the loop' oversight depends on - even where no single control has failed. Sound judgement and clear accountability need to be actively maintained, not assumed, as automation scales.

[10] This is in addition to the implementation of applicable model risk management and automated trading controls.

Case study 3: Non-financial misconduct

Scenario

Two separate Markets businesses are pursuing growth through the launch of a new rates structured product.

Several months post-launch, second line monitoring observe a growing number of cases where product performance and payout characteristics diverge from the assumptions made for the target market, and risk characteristics described in manufacturing marketing documentation. Control functions escalate this concern and recommend restricting marketing and distribution while a review is performed. Some Front Office leaders argue that the product has already been approved, is generating significant revenue and should remain available. At both firms, reward and performance frameworks continue to weigh revenue generation heavily relative to conduct, culture and risk-management behaviours. Reinforced by desk leadership, this creates a day-to-day incentive to prioritise commercial performance over challenge.

One employee remains concerned that the post-sales MI reviewed by the Structured Products Committee shows performance and payout outcomes that are not consistent with the target market and risk assumptions made during product approval, and that these findings have not been escalated or acted upon with the same rigour as the product's revenue performance. The employee raises the concerns during a one-to-one discussion with their Head of Desk. Following the discussion, the employee experiences increasingly inappropriate behaviour from their manager including their judgement being questioned publicly, being excluded from discussions relating to the product and being criticised for being unwilling to support the business. This behaviour reflects the desk-level pressure described above to prioritise commercial performance over escalation and occurs at both firms despite each having stated values around speaking up and non-retaliation - illustrating a gap between tone from the top and its translation into day-to-day desk-level practice. What differs materially between the two firms is not whether this behaviour occurred, but how leadership responds once it comes to light, as set out below.

Once the concern is raised, Firm A's response reflects a well-established speak-up culture. Multiple escalation channels are available, including management, HR, Compliance and an independent whistleblowing process. Regular communications from senior leadership, reinforced at desk-level, emphasise that challenge and escalation are expected behaviours and that retaliation will not be tolerated.

The employee reports the behaviour through the firm’s whistleblowing channel. A coordinated investigation involving HR, Compliance and senior management is initiated. The employee receives appropriate support throughout the process and steps are taken to ensure their anonymity and protect them from retaliation. The allegations are substantiated, disciplinary action is taken against the manager and lessons learned are incorporated into leadership training and performance management processes, including how conduct and client-outcome measures are weighted within scorecards. The firm also reassesses the product concerns that originally triggered the escalation and restricts distribution while a review is completed.

In Firm B, the response follows a different pattern: a whistleblowing channel exists but is not well understood by employees and there is limited confidence that concerns will be handled effectively. The employee chooses not to escalate further because they fear negative consequences. The manager’s behaviour remains unchallenged, product concerns are not fully investigated, and commercial considerations continue to drive decision-making. Employees’ day-to-day experience is shaped more by desk-level commercial pressure than by the values the firm states formally.

The non-financial risk event is the behaviour that emerged when concerns were raised and the firm’s response to that behaviour.

Risks crystallised	
Risk type	**How the risk crystallised**
Conduct risk	Employees may be subjected to bullying, harassment or retaliation after challenging decisions or raising concerns. This may discourage future escalation and weaken the firm's ability to identify risks early.
Compliance risk	Regulators may question whether the firm responded appropriately to allegations of harassment, retaliation and non-financial misconduct, as well as the underlying business concerns.
Operational risk	Employees may lose confidence in leadership and become reluctant to challenge decisions, particularly where concerns involve profitable business activities or senior individuals – reinforced where performance scorecards do not weight conduct and client-outcome measures with the same rigour as revenue.
Reputational risk	Product concerns may remain unresolved, and stakeholders may perceive that the firm prioritised commercial objectives over client outcomes, employee welfare and effective challenge.

Firm A v Firm B: Comparative response		
Risk type	**Firm A**	**Firm B**
Conduct risk	Leadership reinforces that challenge is expected and retaliation is unacceptable. Non-financial misconduct is clearly defined and understood across the firm.	Staff perceive that challenging profitable activity is unwelcome. The definition of non-financial misconduct is unclear.
Compliance risk	The firm can demonstrate that allegations were investigated, employees were supported and appropriate actions were taken.	The firm struggles to evidence how concerns were managed and why behaviours were allowed to continue. Reliance on an informal, manager-level conversation as the primary detection route rather than a trusted formal channel reflects the reactive pattern that is typically the most common way firms identify non-financial misconduct across the sector.
Operational risk	Tone from the top promotes speaking up, inclusion and psychological safety, reinforced at desk level. Multiple escalation channels are available and trusted by employees, and scorecards weight conduct and client outcomes as rigorously as revenue.	Commercial pressures dominate. Employees receive mixed signals about challenge and escalation and lack confidence in available channels; conduct measures on scorecards are easily outweighed by revenue performance.

Firm A v Firm B: Comparative response		
Risk type	**Firm A**	**Firm B**
Reputational risk	Product concerns are reassessed and distribution is adjusted where necessary. The firm's response reinforces confidence in its governance and culture.	Product concerns remain unresolved and the firm appears to prioritise revenue over employee welfare, challenge and client outcomes.

Before concerns are raised (preventative)

- Do incentives encourage challenge, good conduct and appropriate client outcomes, with scorecards weighting conduct and client-outcome measures as rigorously as revenue?
- Are leaders held accountable, through appraisal and promotion decisions, for their behaviour and the culture and day-to-day experience they create for their teams?
- Are escalation channels clear, accessible and trusted – tested regularly for employee understanding and confidence, not just for existence?
- Is retaliation explicitly prohibited and monitored, with training that uses real examples rather than referencing policy alone?
- Does the firm monitor for early behavioural indicators such as exclusion, public undermining, informal client dissatisfaction before they escalate into formal complaints or whistleblowing cases?
- Does the firm invest in firm-led detection, such as culture monitoring, exit interview analysis or surveillance, rather than relying mainly on reactive routes such as grievances – given that around half of reported incidents across the sector are typically first identified this way?[11]
- Does the firm have a consistent basis for deciding when a finding of non-financial misconduct should also trigger remuneration adjustment, rather than defaulting to no action – given that remuneration is rarely adjusted following such findings across the sector, and mostly only against unvested variable pay when it is?

Once a concern or retaliation is raised (reactive)

- Do employees feel genuinely comfortable raising concerns?
- Are concerns assessed objectively, or through a commercial lens?
- Are allegations of bullying, harassment and retaliation investigated consistently?
- Does the firm provide support to employees who raise concerns, and is the underlying business or product concern reassessed on its own merits?

Lessons learned

- Non-financial misconduct often crystallises through behaviours that suppress challenge, discourage speaking up or create fear of retaliation. Mature firms create an environment where employees are supported when raising concerns and where challenge is viewed as a control that strengthens both decision-making and client outcomes.

[11] Financial Conduct Authority, *Culture and Non-Financial Misconduct Survey: Findings*, 2024 (updated March 2026).

- Where balanced scorecards do not weight conduct and revenue with comparable rigour, incentive misalignment persists regardless of how clearly non-financial misconduct is defined in policy.
- Tone from the top is only as effective as its translation by line managers into employees' day-to-day experience; culture is set locally as much as centrally.
- Across the sector, disciplinary or other action follows a finding of non-financial misconduct in fewer than half of reported cases[12], and remuneration is rarely adjusted even then; a firm's response in this case study is only genuinely mature if it goes beyond the sector norm, not merely in line with it.

[12] Ibid.

Appendix 2: Risk taxonomy

The taxonomy below provides a common reference framework to support discussion, comparability and read across of the themes explored in this Review. It is provided for illustrative purposes only. Certain drivers of risk, including cultural, behavioural and governance-related factors, may operate across multiple risk categories and are therefore best understood as cross-cutting influences rather than standalone risk classes.

The taxonomy is broadly consistent with the Basel Committee's operational risk framework, within which technology, third-party and similar risks are typically treated as sub-components of operational risk. This Review separates them into distinct categories to reflect their growing scale, interconnectedness and strategic significance, and to support clearer ownership and more granular oversight in practice.

Financial risks

Risk type	Definition	Sub-categories
Market risk	The risk of loss arising from changes in the value of the firm's assets and liabilities due to movements in market variables such as interest rates, exchange rates or credit spreads. Losses may also arise from basis or correlation risks.	• Trading • Non-trading
Credit risk	The risk of loss resulting from a decline in credit quality or the failure of a borrower, counterparty, third party or issuer to meet contractual obligations.	• Wholesale • Retail
Liquidity risk	The risk that a firm is unable to meet current and future cash flow and collateral requirements without adversely affecting its operations or financial condition. This risk may be exacerbated by constrained access to funding sources, inability to monetise assets, or the composition of liabilities and liquid assets.	• Funding profile
Investment risk	The risk of loss arising from adverse performance of assets managed on behalf of clients or the firm, including the risk of failing to meet a portfolio's stated investment objectives, benchmark or risk profile.	• Asset allocation risk • Concentration risk • Valuation risk • Mandate/ benchmark risk

Non-financial risks

Risk Type	Definition	Sub-categories
Operational risk	The risk of loss resulting from inadequate or failed internal processes, people and systems, or from external events. Excludes strategic and reputational risk.	• Business disruption • Fraud • Human capital • Model • Processing
Conduct risk	The risk of harm to clients, counterparties, markets, employees or the firm arising from inappropriate behaviour, decisions or practices that fail to meet expected standards of integrity, fair dealing and market conduct.	• Customer/client protection risk • Market practices risk
Compliance risk	The risk to current or projected financial condition and resilience arising from violations of laws, rules or regulations, or from non-conformance with prescribed practices, internal policies, procedures or ethical standards. Includes legal risk (risk of loss, including litigation costs, settlements and regulatory fines, arising from failure to comply with laws, regulations, ethical standards or contractual obligations) and regulatory risk.	• Bribery risk; Money laundering risk • Prudential and regulatory risk • Sanctions
Reputational risk	The risk to current or projected financial condition and resilience resulting from adverse perceptions held by key stakeholders. This risk may affect a firm's ability to establish new relationships, provide services or maintain existing business. Effective management includes early identification, escalation and active management of issues, as well as consideration of reputational implications in new activities, products, third-party relationships and market expansion.	-
Technology risk	The risk of loss or disruption arising from the failure, inadequacy or misuse of technology systems, infrastructure or data.	• Cyber risk • Data risk • IT/systems availability

Third-party risk	The risk arising from a firm's reliance on external providers or outsourced arrangements to deliver critical services, including risks of concentration, resilience and reduced direct oversight and control.	• Outsourcing • Concentration risk • Fourth-party/supply chain risk • Third-party reporting
Strategic risk	(a) The risk of a sustained impact (not episodic impact) to the firm's core strategic objectives as measured by impacts on anticipated earnings, market capitalisation, or capital, arising from external factors affecting the firm's operating environment; and (b) the risks associated with defining and executing strategy.	-

Bibliography

Australian Prudential Regulation Authority (2023), *Prudential Standard CPS 230: Operational Risk Management*, July 2023.

Basel Committee on Banking Supervision (2021), *Revisions to the Principles for the Sound Management of Operational Risk*, March 2021.

European Central Bank (2024), *Draft Guide on Governance and Risk Culture*, July 2024.

Financial Conduct Authority (2024), *Culture and Non-Financial Misconduct Survey: Findings*, 25 October 2024 (updated 24 March 2026).

Financial Stability Board (2026), *Sound Practices for Responsible Adoption of Artificial Intelligence (AI): Consultation Report*, 10 June 2026.

Group of Thirty (2018), *Banking Conduct and Culture: A Permanent Mindset Change*, 2018.

KPMG (2026), *A New Frontier for Risk Culture: How AI Could Change How We Think About Banking Risk Culture*, May 2026.

Oxford Character Project (2023), *Character in UK Finance*, October 2023.

Prudential Regulation Authority (2026), *UK Deposit Takers Supervision: 2026 Priorities*, 15 January 2026.

Starling Insights (2025), *Deeper Dive: Supervisors on Supervision*, November 2025.