



Operational Risk Before the Loss

From Forward-Looking Practice to Pre-Loss Measurement

A RASB White Paper

July 2026

Central thesis

The industry is visibly moving toward forward-looking operational-risk practice. The missing layer is a disciplined way to measure the operational risk already embedded in business activity before losses occur.

Table of Contents

1. Executive Summary	2
2. The Industry Turn Toward Forward-Looking Operational Risk	3
3. What Forward-Looking Currently Means in Practice	4
4. The Measurement Gap.....	5
5. Anticipation Is Not the Same as Measurement.....	7
6. Pre-Loss Risk Measurement	7
7. The Risk Accounting View of Operational Risk.....	8
8. Why This Matters for Current Industry Practice	9
9. From Loss History to Operational Condition	10
10. Implications for Banks	11
11. Implications for Regulators and Standard-Setters	12
12. A Research and Pilot Agenda	13
13. Conclusion	14

1. Executive Summary

Operational risk management is visibly moving beyond its historically backward-looking foundations. Across banking, investment management, insurance, professional associations, data consortia, consultancies, technology providers, and public bank disclosures, there is growing interest in scenario analysis, emerging-risk identification, predictive key risk indicators, operational resilience testing, stress testing, fraud intelligence, cyber-risk monitoring, third-party-risk surveillance, continuous control monitoring, and AI-enabled analytics.

This trend is real, but still incomplete. Much of what is currently described as forward-looking operational risk remains centred on three broad practices: imagining possible future events, monitoring indicators that may signal deteriorating conditions, and preparing the organisation to withstand disruption. These are valuable disciplines. They improve awareness, challenge, escalation, and resilience. But they do not, by themselves, create a consistent measure of the operational risk exposures already accumulated in the business before losses occur.

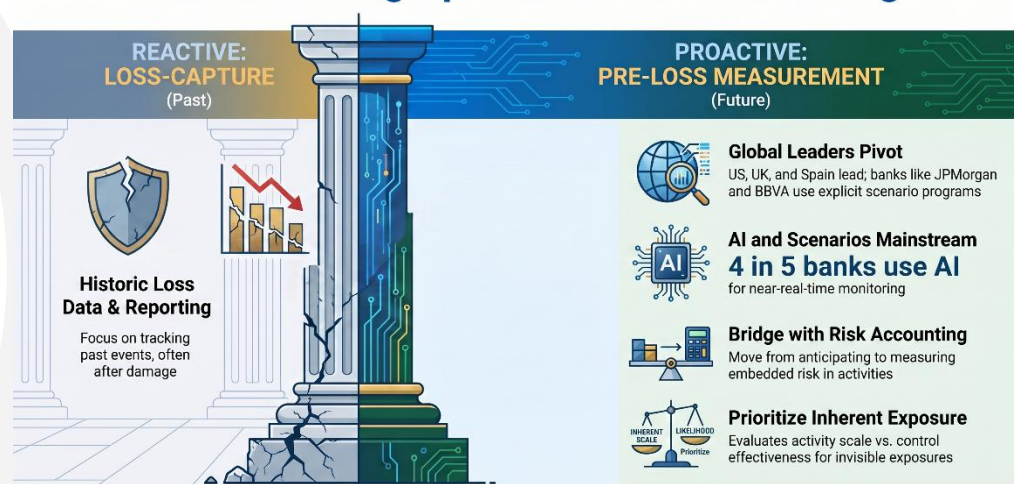
That is the measurement gap this paper addresses. Current forward-looking practices typically ask: What could happen? Which indicators are deteriorating? What severe but plausible scenarios should be tested? How resilient would the institution be under disruption? Risk accounting asks a different question: how much operational risk is being carried now, given the inherent exposure of the business and the effectiveness of the controls and mitigants currently in place?

This distinction matters. A firm may have a scenario-analysis programme, a key-risk-indicator dashboard, a resilience-testing regime, and emerging-risk reporting, yet still lack a coherent, comparable, auditable measure of operational-risk accumulation across products, processes, business units, control points, and mitigation practices.

Risk accounting should not be understood as an attempt to predict specific future loss events. It is a method for measuring present operational conditions that make future losses more or less likely, more or less severe, and more or less preventable. It is forward-looking not because it forecasts named events, but because it measures accumulated risk exposure before it turns into loss.

The industry is already asking the right question: how can operational risk management become less dependent on historical losses and more sensitive to emerging conditions? The next step is to move from forward-looking judgement to pre-loss measurement.

Future-Proofing Operational Risk in Banking



What this paper does not claim

This paper does not argue that scenario analysis, KRIs, RCSA, resilience testing, or regulatory capital frameworks should be abandoned. It argues that these practices need a stronger measurement layer beneath them: a structured view of inherent exposure, mitigation effectiveness, and residual risk before loss occurs.

2. The Industry Turn Toward Forward-Looking Operational Risk

Operational risk has traditionally been difficult to measure in a way that is both quantitative and operationally meaningful. Historical loss data is useful, but it is inherently incomplete. Severe operational losses are often rare, clustered, idiosyncratic, and shaped by changing business models, technologies, legal environments, third-party dependencies, customer behaviours, and control weaknesses. A loss history may tell an institution what has gone wrong, but it may say much less about the risk currently accumulating in business areas that have not yet failed.

This limitation is increasingly visible in industry practice. Banks and other financial institutions are under pressure to manage cyber risk, fraud, data integrity, outsourcing, cloud dependency, artificial intelligence, conduct risk, payments disruption, model risk, operational resilience, and geopolitical supply-chain effects. These risks do not wait for long internal loss histories before becoming material. They often emerge through changing operating conditions, new product configurations, control drift, technology concentration, external threat evolution, or the interaction of business complexity with weak mitigation.

Public industry evidence shows that financial institutions are responding by expanding the forward-looking components of their operational-risk frameworks. ORX, for example, described operational-risk scenario analysis as being at a turning point and reported that nearly 90% of firms in a large scenario-process benchmarking exercise were actively undertaking or planning enhancements to their scenario processes. The same ORX material points to better metrics, digitised assessment tools, integrated databases, workflow automation, and more data-led review and challenge as priorities for scenario programmes. [S1]

The professional-development market reflects the same shift. UK Finance's Operational Risk Series 2024 included dedicated sessions on operational-risk appetite and predictive key risk indicators, risk events, scenario analysis and emerging risks, and the future of the operational-risk discipline. This is a useful signal because it shows that forward-looking operational-risk themes are not restricted to academic papers or vendor marketing; they are part of mainstream practitioner training. [S2]

Bank disclosures also increasingly use forward-looking language. BBVA describes risk-identification processes as forward looking and designed to identify emerging risks, supported by scenario analysis, stress testing, control consideration, and forward projection of Risk Appetite Framework variables under stress scenarios. [S3] Other global bank disclosures similarly refer to operational-risk scenario analysis, tail and emerging risks, business-environment and internal-control metrics, operational-loss forecasting, governed indicators, and operational-resilience scenario testing. [S4-S9]

The trend is also visible in operationally adjacent domains. In Spain, BBVA, Banco Santander, and CaixaBank launched FrauDfense Check, a fraud-prevention service based on secure information exchange between financial institutions, after testing the service in real banking use cases including onboarding, product contracting, transfers, instant payments, Bizum payments, and card transactions. Although fraud prevention is not identical to enterprise-wide operational-risk measurement, initiatives of this kind show appetite for more anticipatory, collaborative, data-driven risk detection. [S10]

The conclusion is not that the industry has converged on one new standard. It has not. The conclusion is narrower but still important: operational-risk practice is visibly broadening from loss capture and periodic control assessment toward a more anticipatory discipline.

3. What Forward-Looking Currently Means in Practice

The phrase forward-looking operational risk is used in several overlapping ways. In practice, it usually refers to one or more of the following disciplines.

3.1 Scenario analysis

Scenario analysis remains the central forward-looking tool in operational risk. Its purpose is to explore severe but plausible events, assess potential impacts, test assumptions, inform capital or resilience planning, and stimulate management discussion. It is especially useful where historical loss data is sparse, backward-looking, or insufficiently representative of future exposures.

The industry is still investing in this discipline. ORX's 2024 scenario-process work emphasised enhancements to the end-to-end scenario process, including better coverage, metrics, tooling, governance, and benchmarking. Deloitte and ORIC International have also treated operational-risk scenario analysis as critical to governance and capital assessment, while noting persistent challenges in integrating internal loss data, external loss data, and expert judgement consistently. [S1, S11]

3.2 Emerging-risk identification

A second meaning of forward-looking practice is the structured identification of emerging risks. These may include AI, cyber, geopolitical disruption, regulatory change, third-party dependency, cloud concentration, payments fraud, climate-related disruption, data integrity, conduct risk, and new business-model risk.

Emerging-risk identification is important because many operational losses are not simply random accidents. They are often the visible outcome of risk conditions that developed over time. A new technology creates new process dependencies. A growing outsourcing model concentrates failure points outside the institution. A control that was adequate for a manual process becomes inadequate after automation. A product expands faster than its control architecture. A vendor becomes operationally critical before exit planning matures. Emerging-risk processes attempt to identify such shifts early.

3.3 Key risk indicators and early-warning metrics

Key risk indicators are intended to provide early warning of rising risk exposure. They may monitor overdue reconciliations, failed transactions, control breaks, cyber vulnerabilities, system availability, customer complaints, manual overrides, unprocessed exceptions, vendor-service failures, fraud attempts, staff turnover, policy breaches, access-control anomalies, or remediation delays.

This is one of the clearest examples of forward-looking aspiration in operational risk. A good indicator does not merely describe past loss. It signals that the environment is becoming more vulnerable. UK Finance's inclusion of predictive key risk indicators in its operational-risk curriculum illustrates the increasing practitioner focus on this area. [S2]

3.4 Operational resilience testing

Operational resilience has become a major forward-looking discipline. It asks whether important business services can continue within defined tolerances under disruption. NatWest, for example, reports regular scenario tests and a broad approach to operational resilience, including third-party disruption, data issues, business interruption, and interconnected operational risks. [S9]

Operational resilience is closely related to operational risk, but not identical to it. It is often service-continuity oriented: can the institution withstand and recover from disruption? Operational-risk measurement asks a broader question: how much risk is accumulating across the business because of exposure and mitigation quality, including but not limited to resilience?

3.5 Stress testing

Stress testing is used to examine how operational losses, controls, capital, or services may behave under adverse conditions. In the United States, large banks commonly link operational-risk stress testing to broader capital stress-testing processes. In Europe, scenario-based and ICAAP-related uses are also common, though public disclosures vary by institution and jurisdiction. [S4-S9]

Stress testing is valuable because it forces the organisation to examine conditions outside normal operating experience. However, it typically remains event- or condition-based. It does not necessarily provide a standing measurement of operational-risk accumulation in ordinary business conditions.

3.6 AI, analytics, and continuous monitoring

Finally, the forward-looking agenda increasingly includes data analytics, workflow automation, AI-enabled monitoring, continuous control monitoring, fraud intelligence, cyber telemetry, and third-party-risk surveillance. These approaches can be powerful, especially where risk signals are frequent, data-rich, and time-sensitive.

But here again, the distinction matters. Detecting anomalous transactions, predicting fraud attempts, monitoring supplier alerts, or identifying cyber vulnerabilities are all valuable operational controls. They are not, by themselves, a general measurement framework for operational risk across the enterprise.

4. The Measurement Gap

The industry trend is therefore genuine, but fragmented. Current forward-looking practices are useful, but they often do not answer the core measurement question.

A scenario workshop may identify a severe plausible event, but it does not necessarily tell management how much operational risk is currently embedded in each business component. A KRI dashboard may show deteriorating signals, but it may not translate those signals into a coherent measure of residual risk. An emerging-risk report may identify AI, cyber, outsourcing, fraud, or data risk as strategic themes, but it may not map those themes to the exact products, processes, control points, best practices, and mitigation deficiencies through which loss potential is already accumulating.

A resilience test may show whether an important service can withstand disruption, but it may not quantify the risk contribution of poor mitigation in related upstream

or downstream processes. An AI model may detect anomalies, but it may not provide an auditable measure of operational-risk exposure across the business.

This is the measurement gap. The problem is not that current forward-looking tools are wrong. The problem is that they are often incomplete as a measurement discipline. They help institutions anticipate, discuss, monitor, and prepare. But they do not necessarily produce a consistent, comparable, repeatable, evidence-based measure of operational risk exposure accumulations before they turn into a loss.

4.1 Probability, severity, and exposure scale

One reason the gap persists is that forward-looking operational-risk practice often gravitates toward likelihood: which event could occur, which indicator is worsening, which scenario is plausible, or which threshold might be breached. These questions matter, but they are incomplete. Operational risk is not only a question of probability. It is also a question of scale.

A control weakness in a low-volume back-office process does not carry the same business meaning as a similar weakness in a high-volume payment flow, customer onboarding process, trading-support process, cloud-hosted critical service, or outsourced process that supports millions of transactions. The same apparent control deficiency may have very different consequences depending on business volume, process criticality, customer impact, legal exposure, transaction value, recoverability, and concentration.

Risk accounting therefore adds an exposure-sensitive view of loss potential, not merely a probability-sensitive view of likelihood. It asks not only whether loss could occur, but how much risk is structurally embedded in the activity given its scale, importance, vulnerability, and mitigation quality.

4.2 When tail events are accumulated invisible exposures

Operational-risk losses are often described as tail events. This language is useful when it highlights low-frequency, high-impact loss potential. But it can also obscure an important possibility: some so-called tail events may be less an unforeseeable bolt from the blue than the late recognition of accumulated exposure.

Control deterioration, process workarounds, unresolved findings, access exceptions, transaction growth, vendor concentration, incident backlogs, technology obsolescence, manual intervention, weak reconciliation, and poor remediation may all accumulate gradually. If the organisation does not measure these changes as changes in residual risk, the eventual loss may appear sudden only because the accumulation was not actually visible to the decision makers.

The risk accounting perspective is particularly relevant here. It treats operational effectiveness as something that can degrade or improve over time and that should therefore be recorded dynamically. If inherent exposure is expanding while mitigation quality is weakening, the residual-risk position is deteriorating even if no loss has yet occurred. The absence of loss is not the same as the absence of risk.

4.3 Compliance is necessary, but not sufficient

The measurement gap also matters because regulatory compliance is not equivalent to operational safety. Banks must satisfy regulatory requirements, and sound regulation is an essential component of financial stability. But an institution can comply with reporting, capital, governance, documentation, and resilience expectations while still lacking sufficient visibility over the operational conditions through which losses are accumulating.

When risk management becomes primarily an exercise in evidencing compliance, it may protect the institution against supervisory criticism or fines without necessarily improving management's ability to prevent loss. The business benefit of risk management lies in better decisions: where to invest, which controls matter most, which processes are becoming vulnerable, which risks are increasing faster than mitigation, and which remediation actions will produce the greatest reduction in residual risk.

5. Anticipation Is Not the Same as Measurement

A useful distinction can be made between three layers of forward-looking operational-risk practice:

1. Anticipation - identifying what might happen.
2. Detection - monitoring signals that conditions may be worsening.
3. Measurement - quantifying how much risk is currently being carried.

Most current forward-looking practice is strongest in the first two layers. Scenario analysis strengthens anticipation. It helps institutions imagine severe but plausible events, challenge assumptions, and assess potential loss or resilience consequences. KRIs and dashboards strengthen detection. They help institutions monitor whether known signals are moving toward tolerance, appetite, or escalation thresholds.

Risk accounting belongs primarily to the third layer. It aims to measure the present accumulation of operational risk by examining inherent exposure, mitigation quality, and residual risk before loss occurs. This does not make anticipation or detection unnecessary. On the contrary, both are essential. But they are not substitutes for measurement.

A medical analogy may help. A patient can be asked about possible future illnesses, monitored for warning symptoms, and stress-tested through a physical examination. But a meaningful diagnosis also requires measurement of the patient's current condition. Similarly, an institution can imagine future operational events, monitor early warning indicators, and test resilience. But it still needs a disciplined way to measure the current operating condition that makes future loss more or less likely.

6. Pre-Loss Risk Measurement

Risk accounting should be understood as a pre-loss measurement discipline. It does not attempt to predict that a specific operational-loss event will occur on a specific date. Operational losses are too complex, path-dependent, and context-sensitive for that kind of claim to be reliable in most areas of non-financial risk.

Instead, risk accounting asks whether the institution is carrying operational risk because of the combination of:

- the inherent risk of the activity;
- the vulnerability of the process;
- the importance, scale, and potential loss size of the product or service;
- the quality of the control environment;
- the degree to which relevant best practices are observed;
- the effectiveness of mitigation at relevant control points;
- the residual risk that remains after mitigation.

This makes risk accounting forward-looking in a structural sense. It measures risk before loss by analysing the present conditions from which future losses may arise.

The phrase pre-loss is important. It avoids a common misunderstanding. A pre-loss measurement framework is not the same as a predictive event model. It does not say: this institution will suffer this loss next quarter. It says: this business component is carrying a measurable level of operational risk because its inherent exposure is high and its mitigation quality is insufficient.

That is a more defensible, useful, and auditable claim.

7. The Risk Accounting View of Operational Risk

At the heart of risk accounting is the distinction between inherent risk, mitigation, and residual risk.

- Inherent risk represents the risk arising from the nature, scale, complexity, and exposure of the activity before mitigation is considered.
- Mitigation represents the extent to which controls, practices, processes, systems, governance, monitoring, and other safeguards reduce the risk.
- Residual risk represents the remaining risk after mitigation is applied.

This is conceptually familiar to operational-risk professionals, but risk accounting seeks to make the relationship more disciplined and measurable. The key point is that operational risk is not measured only by past loss. It is also carried in current operations. A business unit may have avoided major losses so far but still be structurally vulnerable. Conversely, a business area may have experienced historical losses but now operate under much stronger mitigation. Loss history is relevant, but it cannot be the only anchor.

Risk accounting therefore requires a structured decomposition of the business into assessable components. These may include products, processes, business lines, control points, risk categories, mitigation practices, and best-practice requirements. The purpose is not administrative complexity for its own sake. The purpose is to locate and record risk exposures as it accumulates, right where it is actually generated and mitigated.

A generic enterprise score is not enough. Operational risk accumulates through specific combinations of activity, exposure, process design, control weakness, dependency, and mitigation failure. A useful measurement framework must therefore be granular enough to support timely management action, while still being standardised enough to allow comparison, aggregation, and auditability.

Concept	Risk accounting interpretation	Management relevance
Inherent risk	Risk arising from the activity before mitigation.	Shows where the business creates exposure by virtue of what it does and at what scale.
Mitigation effectiveness	The degree to which controls and practices reduce inherent exposure.	Shows whether the operating model is reducing risk or merely documenting control activity.
Residual risk	Risk remaining after mitigation.	Supports prioritisation, board reporting, audit challenge, and investment decisions.
Operational condition	Current state of exposure, control quality, and mitigation maturity.	Turns risk management from a retrospective exercise into a live management discipline.

8. Why This Matters for Current Industry Practice

The risk accounting perspective strengthens existing forward-looking practices rather than replacing them.

8.1 Scenario analysis

Scenario analysis asks what severe events might occur. Risk accounting provides a structured baseline of current exposure and mitigation quality before scenarios are applied.

This can improve scenario selection, calibration, and challenge. Scenarios can be prioritised around areas where inherent risk is high and mitigation is weak. Scenario assumptions can be tested against evidence about actual control quality. Scenario outputs can be linked to remediation priorities rather than remaining as workshop narratives.

8.2 KRIs and dashboards

KRIs often suffer from ambiguity. A red indicator may show that something is deteriorating, but it does not always explain how much residual risk is being carried or what mitigation gap matters most.

Risk accounting can give KRIs a measurement context. Indicators can be mapped to control points, best practices, mitigation requirements, and residual-risk effects. This helps distinguish between signals that are operationally noisy and signals that materially affect risk exposure accumulation.

8.3 RCSA

RCSA is one of the most widely used operational-risk tools, but it often suffers from subjectivity, inconsistency, optimism bias, and weak comparability across business units.

Risk accounting can strengthen RCSA by requiring clearer decomposition of risk, more explicit mitigation criteria, more comparable and, most importantly, auditable

scoring. It can also help move RCSA from a compliance exercise toward a measurement exercise.

8.4 Operational resilience

Operational resilience focuses on the continuity of important business services under disruption. Risk accounting can complement resilience work by measuring the operational-risk conditions that make disruption more likely, more severe, or harder to recover from.

For example, resilience testing may show whether a payment service can remain within impact tolerance. Risk accounting can help identify whether the underlying operational risk is driven by weak access controls, insufficient process redundancy, inadequate vendor governance, poor incident response, incomplete reconciliation, or other mitigation gaps.

8.5 Emerging-risk management

Emerging-risk processes identify new or intensifying threats. Risk accounting helps translate those threats into affected products, processes, controls, and mitigation requirements.

This is especially important for AI, cyber, fraud, cloud dependency, data integrity, and third-party risk. These risks are often discussed at a high thematic level. Risk accounting helps convert the theme into measurable operating conditions.

8.6 Capital and supervisory dialogue

Risk accounting is not a substitute for regulatory capital rules, nor should it be interpreted as a return to complex internal operational-risk capital models.

Its value lies elsewhere. It provides a structured, evidence-based view of operational condition that can support internal capital adequacy discussions, supervisory engagement, board reporting, remediation prioritisation, and benchmarking without attempting to replace standardised capital frameworks.

9. From Loss History to Operational Condition

The central shift implied by risk accounting is a move from reliance on loss history to a focus on operational condition.

Loss history answers the question: what has gone wrong? Operational condition answers a different question: what is vulnerable now?

Both perspectives are necessary. Losses provide empirical grounding. They reveal failure modes, validate risk categories, expose weaknesses, and inform scenario design. However, operational-risk management cannot depend solely on realised events. In complex organisations, waiting for losses to confirm risk may be equivalent to waiting for the control environment to fail.

Operational condition is broader in scope. It encompasses the structure of the business, the quality of the control environment, the maturity of mitigation, adherence to best practices, the strength of governance, the reliability of processes, and the extent to which known risk drivers are effectively controlled.

A bank with strong operational-condition measurement is better positioned to ask and answer critical questions:

- Which business components carry the highest residual risk?
- Which controls or best practices deliver the greatest mitigation effect?
- Which remediation actions would most efficiently reduce residual risk?

- Which products or processes create disproportionate exposure?
- Which emerging risks affect specific control points?
- Which KRIs are truly meaningful because they correspond to high-risk weaknesses?
- Which scenario assumptions are supported by current mitigation evidence?
- Which operational-resilience weaknesses correspond to measurable residual risk?

These are not only modelling questions; they are management and governance questions. Boards need to understand not just that operational risks exist, but where risk is accumulating, whether mitigation is improving, and whether investment in controls is demonstrably reducing risk.

This is also where risk accounting connects to value creation. Risk management creates business value when it improves the allocation of scarce management attention and investment. It can help management decide whether to remediate a control weakness, redesign a process, improve automation, strengthen vendor governance, limit growth in a risky activity, or accept a residual-risk position knowingly.

10. Implications for Banks

For banks, the implication is clear: forward-looking operational-risk management should not end with scenarios, dashboards, or resilience testing. These tools must be integrated into a coherent measurement architecture.

A mature framework would include:

- A clear taxonomy of business components and operational-risk exposures.
- A structured mapping of risks to control points and mitigation practices.
- A disciplined assessment of whether critical best practices are observed.
- A clear distinction between inherent risk, mitigation effectiveness, and residual risk.
- A defined linkage between KRIs and the risk conditions they are intended to signal.
- Integration between scenario analysis and current operational-condition evidence.
- A remediation-prioritisation approach based on measurable reductions in residual risk.
- An evidence trail sufficient for review, challenge, and audit.

This is not primarily a technology challenge. While technology can support implementation, the foundation is methodological discipline. Without a structured measurement approach, data risks becoming noise. Dashboards may proliferate without improving understanding. KRIs may multiply without clarifying priorities. Scenario analysis may become a periodic exercise rather than a decision tool. Resilience testing may remain disconnected from broader risk accumulation. AI tools may detect patterns without producing accountable measurement.

The issue is not a lack of activity. Many institutions already have extensive operational-risk processes. The issue is whether those processes produce a coherent, consistent measure of pre-loss risk.

10.1 Risk management as business value

Risk management should not be treated as a defensive compliance function alone. A broader and more commercially relevant view is that risk management protects and creates value by improving decisions, prioritisation, investment allocation,

operational resilience, and strategic confidence. This view is consistent with established risk-management principles and with broader management thinking that risk functions should help the business make better decisions, not merely evidence compliance. [S12, S13]

Pre-loss measurement is valuable because it makes this practical. It can help a bank compare potential remediation actions in terms of risk reduction, identify where operational effectiveness is degrading, justify control investment to senior management and boards, and avoid treating all control weaknesses as equal. A bank that can measure residual-risk reduction can manage operational risk as a business-performance and resilience discipline, not only as an obligation.

11. Implications for Regulators and Standard-Setters

For regulators and standard-setters, the shift toward forward-looking operational risk raises an important question: if operational-risk capital becomes more standardised, how can institutions demonstrate that they still understand and actively manage their true operational-risk profile?

A standardised capital formula can determine a requirement, but it cannot show whether controls are improving, whether emerging risks are being mitigated, whether operational resilience is strengthening, or whether residual risk is accumulating in specific areas.

Regulators have historically been cautious about internal operational-risk models and with good reason. Such models can be opaque, unstable, difficult to validate, and hard to compare across institutions. However, rejecting complex internal capital models does not require abandoning operational-risk measurement altogether.

A more useful distinction is between:

- internal models used to determine regulatory capital; and
- operational-condition measurement used to manage risk.

Risk accounting belongs firmly in the second category. Its purpose is not to override capital rules, but to provide institutions and supervisors with a structured, transparent view of operational risk before losses occur.

This perspective can enhance supervisory review, internal governance, board reporting, remediation tracking, operational-resilience assessment, thematic analysis, and industry benchmarking.

11.1 Regulatory sufficiency and operational safety

Regulatory compliance is necessary, but it is not equivalent to operational safety. A firm may comply with regulatory expectations while still carrying material residual risk in specific business components. Conversely, a firm may improve its operational condition in ways that are highly valuable to the business even if the capital formula is not immediately affected.

This distinction is essential if operational risk management is to remain useful to boards and senior management. Risk management should not collapse into a narrow compliance exercise. It should help the institution understand and manage the operational conditions from which loss, disruption, customer harm, regulatory breaches, and reputational damage may arise.

Policy relevance: RASB response to the Federal Reserve NPR

RASB has argued in response to recent [US FED proposals](#) on operational-risk capital that the move toward standardised capital treatment should not end the search for better operational-risk evidence. On the contrary, standardised capital approaches increase the need for structured operational-condition indicators that can support supervision, governance, and risk management without reviving opaque internal capital models..

12. A Research and Pilot Agenda

The next phase should be empirical and collaborative. The industry does not need further abstract debate about whether operational risk can be measured; it needs structured pilots to test whether pre-loss measurement can be made reliable, comparable, and decision-useful.

A practical research agenda could include:

12.1 Taxonomy testing

Institutions should assess whether common taxonomies can consistently map products, processes, risks, control points, and mitigation practices across business areas.

12.2 Best-practice calibration

Risk accounting depends on identifying critical mitigation practices. Research should evaluate whether expert judgement, loss analysis, audit findings, and control-performance data can support robust and consistent best-practice hierarchies.

12.3 Cross-bank benchmarking

Anonymous benchmarking exercises could test whether similar business components exhibit comparable inherent-risk and mitigation patterns across institutions.

12.4 Linkage to loss and incident data

Pre-loss measurements should be compared with subsequent incidents, losses, near misses, audit findings, control failures, and remediation outcomes. The objective is not perfect prediction, but evidence that measured weaknesses correspond to increased vulnerability.

12.5 Integration with KRIs

Research should examine whether KRIs become more decision-relevant when explicitly linked to measured residual-risk conditions.

12.6 Integration with scenario analysis

Scenario analysis should be evaluated against operational-condition baselines. Do areas with higher residual risk generate different or more credible scenario assumptions? Does mitigation evidence improve challenge and calibration?

12.7 Governance and auditability

Any measurement framework must be subject to challenge. Pilots should test evidence standards, independence of assessment, review processes, version control, and audit trails.

12.8 Board usefulness

Ultimately, the value of any framework lies in its impact on decision-making. Pilots should assess whether outputs improve board and senior-management

understanding, prioritisation, investment decisions, accountability, and risk reduction.

13. Conclusion

The industry's growing emphasis on forward-looking operational risk is both necessary and constructive. It reflects an understanding that historical losses, while essential, are insufficient to capture the risks embedded in modern financial institutions. Operational risk is shaped by evolving conditions: technology, process design, control quality, third-party dependency, cyber threats, fraud patterns, regulatory change, business complexity, data integrity, and organisational behaviour.

Current forward-looking practices are valuable. Scenario analysis enhances preparedness. KRIs provide early warning signals. Emerging-risk processes broaden awareness. Resilience testing evaluates continuity under stress. Analytics and AI strengthen detection in data-rich environments.

However, these practices do not fully address the measurement challenge. What is missing is a disciplined approach to pre-loss operational-risk measurement: a structured way to quantify the risk embedded in the business before losses occur, and to track how that risk evolves as business activity expands and control effectiveness changes.

Risk accounting provides such an approach. It does not attempt to predict specific operational-loss events. Instead, it measures the conditions that make losses more or less likely, more or less severe, and more or less preventable. It distinguishes inherent risk from mitigation effectiveness and residual risk. It links risk to products, processes, control points, and best practices. It enables comparison, prioritisation, accountability, and evidence-based improvement.

Crucially, it reconnects operational-risk measurement to the scale and dynamics of real business activity. As volumes increase, processes evolve, or controls weaken, risk accounting captures the resulting changes in residual risk - making visible the accumulation of exposure that might otherwise remain hidden until a loss occurs.

The industry has already taken an important step by embracing forward-looking thinking. The next step is to make that thinking measurable, consistent, and actionable.

Operational risk management must evolve from anticipating losses to measuring the conditions that create them. That is the transition from forward-looking practice to pre-loss measurement.

Appendix: Comparative View of Forward-Looking Practice and Risk Accounting

Current practice	Main question	Typical limitation	Risk accounting contribution
Scenario analysis	What could happen?	Episodic, judgement-heavy, and often detached from measured operating condition.	Anchors scenario selection, calibration, and challenge in measured exposure and mitigation quality.
KRIs and dashboards	Which signals are deteriorating?	Indicators may be noisy, indirect, or poorly linked to residual risk.	Maps signals to control points, best practices, and residual-risk effects.
Emerging-risk scanning	What new risks are appearing?	Often thematic and difficult to translate into measurable exposure.	Maps emerging risks to products, processes, controls, and mitigation gaps.
Operational resilience testing	Can important services withstand disruption?	Focused on service continuity and impact tolerance rather than full risk accumulation.	Measures underlying vulnerability and mitigation quality across operational components.
AI and analytics	What patterns can be detected?	Often domain-specific and not an enterprise measurement framework.	Fits analytics into an accountable structure for exposure, mitigation, and residual risk.
Loss data	What went wrong?	Backward-looking and incomplete where losses are rare or conditions have changed.	Complements loss data with current operational-condition measurement.

References and Source Notes

- S1.** ORX, "Scenario analysis in operational risk at a turning point", 21 October 2024. ([link](#))
- S2.** UK Finance, "The Operational Risk Series - 2024". ([link](#))
- S3.** BBVA, "Management and control model" - risk identification, emerging risks, scenario analysis and stress testing. ([link](#))
- S4.** JPMorgan Chase, Management discussion and analysis / operational-risk disclosures, 2025. ([link](#))
- S5.** Citi, Pillar 3 disclosures - operational-risk scenario analysis and emerging risks, Q4 2024. ([link](#))
- S6.** Deutsche Bank, Annual Report 2025 - operational-risk scenario analysis and forward-looking mitigation. ([link](#))
- S7.** ING Bank N.V., Additional Pillar III Report 2025 - non-financial-risk repository, indicators, incidents, control performance, and emerging risks. ([link](#))
- S8.** Lloyds Banking Group, FY 2024 Pillar 3 Report - operational-risk framework, indicators, scenario analysis, loss forecasting, and governed metrics. ([link](#))
- S9.** NatWest Bank, Annual Report - operational resilience and scenario testing. ([link](#))
- S10.** BBVA, Banco Santander and CaixaBank launch FrauDfense Check to strengthen fraud prevention. ([link](#))
- S11.** Deloitte and ORIC International, material on enhancing operational-risk scenario and capital assessments. ([link](#))
- S12.** McKinsey, "The value in digitally transforming credit risk management", 21 July 2016. ([link](#))
- S13.** ISO 31000:2018, Risk management - Guidelines. The standard frames risk management as creating and protecting value. ([link](#))
- S14.** RASB response to recent US operational-risk capital [NPR](#). ([link](#))