Hanyani Mabaso

Associate Director
Insurance

Tel: +27 82 870 7883
Email: hanyani.mabaso@kpmg.co.za

Mohammed Ahmed

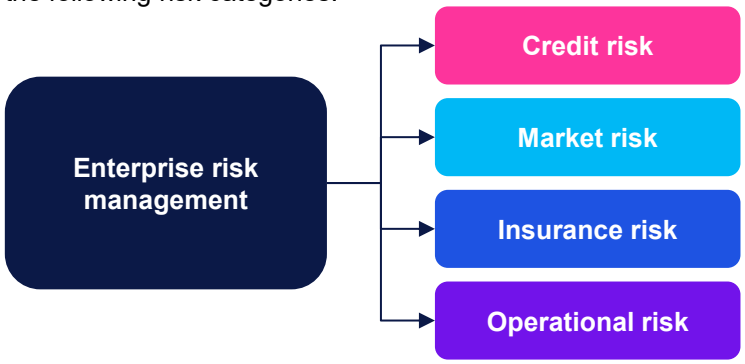
Manager
Financial Risk Management: Actuarial

Tel: +27 66 391 2248
Email: mohammed.ahmed@kpmg.co.za

Enterprise risk management

The insurance industry, like most businesses in South Africa, is exposed to a variety of internal and external forces, ranging from social media scrutiny and cyber-attacks to local and global political developments, amongst others. These internal and external forces, not always within the control of the insurance company, form part of the insurer's enterprise risk management (ERM) universe. Anything that could go wrong for the insurer should be managed under the ERM framework of the entity. ERM is the governance tool employed by an entity to manage these risks. The purpose of an effective ERM framework is to assist insurers with aligning their risk appetite to the strategic objectives of the entity, achieving greater resilience against things that could go wrong.

The ERM framework for an insurer can be categorised into the following risk categories.



Credit risk is the risk that one party to a financial instrument will cause a financial loss to the other party by failing to discharge an obligation. Insurers are exposed to credit risk from balances due from reinsurers, cash and cash equivalents and financial investments. This risk is material due to the significance of reinsurance as a material risk mitigation mechanism for many insurers, and financial investments to manage claims payouts and investment returns.

Market risk refers to the potential for unexpected changes in market conditions, which can result in losses or lower-than-expected market returns. Premiums received from policyholders are typically invested in financial instruments that match the insurer's expected claims payout profile, in order to earn a return. Market risk is therefore a key risk for insurers in that if not managed appropriately, there is a risk that the insurer may not be able to pay out claims obligations as they become due.

Insurance risk is the risk that insurance products are underpriced and that incurred losses are greater than the price that has been charged for said insurance products. It goes without saying that this is a key risk for insurers, underpinning its core operations.

Credit, market and insurance risk exposures are easily measurable through a variety of techniques such as expected credit loss models, balance sheet management and actuarial analysis.

The measurement of **operational risk**, however, is more complex.

Operational risk refers to all remaining risks, after considering credit, market and insurance risk. Anything that could go wrong at an insurer, other than credit, market and insurance risk, would be classified as operational risk. Think of reputational, legal, competition, people and cyber security risks, to name a few.

Operational risks are generally expected to occur less frequently, however the extent of severity or magnitude can be monumental. For example, an insurer that has been subject to a cyber-attack or reputational damage may be forced to close doors. Given the significance of this risk, it is important for insurers to be able to accurately and effectively measure and manage this risk.

So how do we currently measure operational risk in South Africa?

The Prudential Standard FSI 4.4[1] sets out the details for calculating the capital requirement for operational risk for insurers using a Standardised Formula. This calculation is based on a simple linear measure applied to an insurer's earned premiums and technical (insurance) provisions and, for linked insurance obligations, assets under management. The formula calculates operational risk as a percentage of premiums or technical provisions. No rationale has been provided as to why the standard applies those particular percentages.

What is important to note with this standardised formula is that it excludes risks arising from strategic decisions and reputational risk. Our view is that these risks form part of operational risk and should be quantified. What is not clear is what is excluded or included under the banner of strategic decisions – how are risks in respect of product innovation, market relevance, restructuring, strategic partnerships, supplier relationships and hiring of key management considered?

In light of the short comings noted above, it is important for insurers to consider mechanisms to measure and manage the complete suite of operational risk exposures.

In order to compare the enterprise-wide risk exposures disclosed by insurance companies in South Africa, we developed a risk taxonomy based on our industry experience.

[1] https://www.resbank.co.za/en/home/publications/prudential-authority/pa-insurance/pa-post-insurance/Draft_Prudential_Standards_-_9_March_2018

KPMG operational risk taxonomy for South African insurers

Risk	Description
Credit risk ##	The risk that one party to a financial instrument will cause a financial loss for the other party by failing to discharge an obligation.
Market risk ##	The potential for unexpected changes in market conditions, which can result in losses or lower-than-expected market returns.
Liquidity risk ##	The risk of not being able to meet financial obligations as and when they fall due, due to inaccessible and insufficient liquid resources.
Insurance and model risk ##	The risk that an insurance product is underpriced, potentially resulting in operating losses for the insurer.
Operational risk #	All remaining risks after taking into account credit, market and insurance risk.
Reputation risk #	The risk of negative publicity in respect of the insurer, which could potentially hinder the insurer's ability to sell new business or keep existing clients.
Legal and regulatory risk #	The risk of financial or other losses as a result of non-compliance with laws, contracts and regulations.
People risk #	The risk as a result of human error, poor talent management and succession planning, which could result in the insurer not being able to compete successfully in the market.
Technology risk #	The risk of employing redundant technology, which could result in operational inefficiencies and eventually a loss of clients.
Cyber risks #	The risk of financial losses as a result of a cyber-attack.
Compliance risk #	The risk that the insurer will not comply with its own policies, laws and regulations. This also includes risks that the insurer is not treating customers fairly, which could result in fines and penalties and reputational risks.
Fraud (internal and external) #	The risk of financial losses as a result of fraud.
Going concern #	The risk that the insurer will not be able to operate as a going concern in the foreseeable future, resulting in a loss of shareholder value.
Business continuity #	The risk of disruptions to business operations, including exposure to epidemics, pandemics, strikes and riots.
Political risks (local and global) #	The risk of operational disruptions and financial losses as a result of the political environment.
Economic and public infrastructure risks #	The risk that the operating environment, due to economic and public infrastructure factors, does not support adequate and sustainable growth of the business.
Competition and strategy risk #	The risk of being outcompeted in the market due to not being able to execute the strategy effectively, resulting in a loss of shareholder value.
Outsourcing risk #	The risks that third parties will not be able to meet their contractual obligations to service the insurer or its customers.
Process risks #	The risk of process failures, resulting in operational losses, loss of customers and potential fraud.
External risks #	Crime, theft and malicious damage to property.
Financial reporting risks #	The risk of non-compliance with financial reporting standards, leading to inaccurate decision-making.
Project risks #	The risk that strategic projects will not be executed as planned, are delayed or will not meet the desired objectives.
Climate change #	The risk of increased severity and frequency of natural disasters because of climate change.

Non-operational risks
 # Operational risk

Further to the above, we analysed the risks disclosed by certain large listed insurance groups (Sanlam, Discovery, Momentum, Old Mutual, Santam and OUTsurance) based on the frequency of each risk category mentioned in the risk section of the financial statements and integrated reports up to 31 December 2024. While this may not accurately represent the true risk ranking, it provides insight into the risks that insurers are most concerned about. Set out below are the top five risks identified from this exercise:

1 **Competition and strategy**

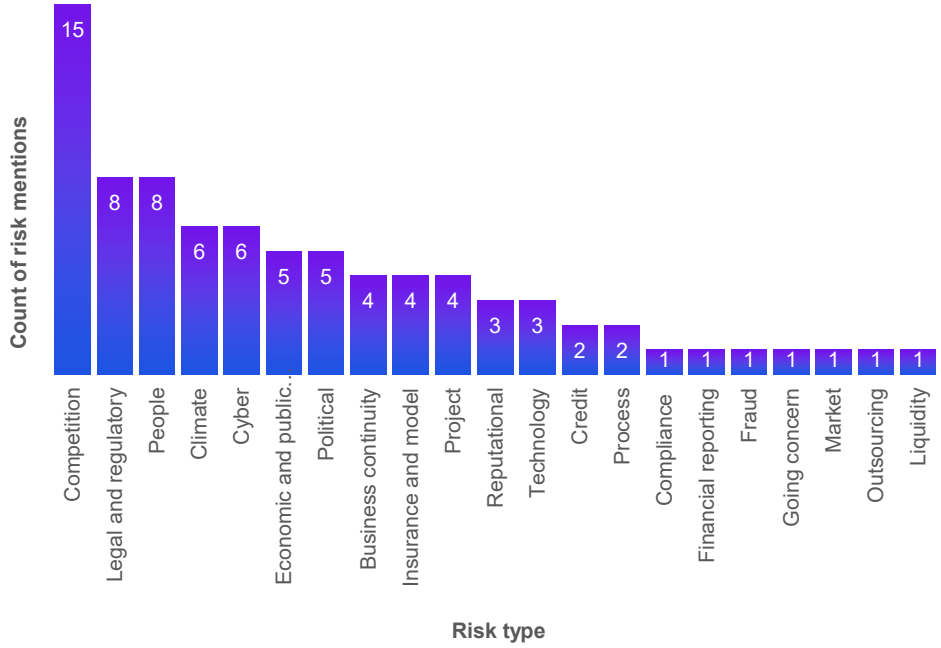
2 **Legal and regulatory**

3 **People**

4 **Climate**

5 **Cyber**

The number of times the risk is mentioned on the insurers' risk register



It is not surprising that credit and market risk do not appear in the top five risks, as these risks can be measured with a higher degree of certainty and therefore risk exposures are well understood and managed. In fact, only Momentum included market risk in their top ten risks, while Old Mutual mentioned credit risk among theirs. Of the three measurable non-operational risks, insurance risk is considered to be the most challenging to measure. This is understandable considering the frequency and severity of natural disasters in South Africa in recent years, along with the occurrence of the COVID-19 pandemic. Insurance risk is also closely connected to climate risk, which is also featured in the top ten risks. This is expected as we have started to observe insurers and reinsurers adjusting their pricing models to take into account increased risks related to climate change.

Competition risk refers to the possibility that a company may struggle to compete effectively in the market. It includes the risk of not being able to achieve sustainable growth and remain competitive. This risk is closely tied to the business strategy, where some insurers refer to it as “strategic risk”. Our analysis reveals that many insurers are concerned about competition risk. For example, Old Mutual identifies growth and strategic execution as the second and third most significant risks respectively, with sovereign risk being the highest, but with a lower likelihood of occurrence. Momentum indicated that the risk related to competition and strategy has increased, placing these risks at position two and four of their top five risks respectively, while Old Mutual’s top two risks relate to competition and strategy.

What is also interesting is that non-life insurers appear to be less worried about competition and strategy risks and are more concerned about risks relating to the operating environment such as political, climate change, legal and economic risks.

The operating environment in South Africa has been challenging, characterised by new market entrants, intense competition from Insurtech companies and the rise of new insurance distribution channels. The competitive landscape is vying for the same customers in a country facing high unemployment rates, low GDP growth and a high cost of living. Considering the rising prominence of competition risk, there is room for consideration in including this risk as part of the determination of operational risk as required by the Prudential Standards.

As it relates to legal and regulatory risk, Discovery is the only insurer that identified the National Health Insurance Act (NHI) Act as a top concern. The NHI Act, which was signed into law on 15 May 2024, has a substantial impact on the Discovery Group. This is due to their ownership of Discovery Health, the largest medical scheme administrator in the country, and their significant contribution to the Group's overall results. Although the NHI Act has not yet been implemented, it has created considerable uncertainty for medical schemes and their administrators. This Act could potentially limit private health coverage. However, the near- to long-term consequences are not yet entirely known, given the extent of uncertainty around how the Act will operate and funding mechanisms.

In their 2024 report, OUTsurance expressed concerns regarding the 2022 Employment Equity (EE) Amendment Act, in that their progress and targets for transformation might not be satisfactory. However, the legal, regulatory and compliance risk with this Act remains uncertain due to questions remaining around the practical implementation of the Act and if further refinements or clarifications will be provided by the Government of National Unity.

All six insurers identified concerns related to people and climate risk. They are particularly worried about succession planning, retaining top talent and replacing senior executives, as well as the relocation of skilled workers to developed countries, a phenomenon often referred to as “brain drain”. We have seen unpredictable weather events in the last five years, which created unpredictable claims patterns, especially for the non-life insurance industry. It is no surprise that climate risk is a concern for the industry.

Conduct risk can be linked to the fair treatment of customers. This is particularly relevant in the South African context, where customer vulnerability is exacerbated by factors such as low literacy levels and limited access to information. Conduct risk is also closely aligned to competition and strategic risk, as the successful execution by an insurer of its strategic objectives relies on the appropriate conduct of its people, with talent risk also of relevance in this scenario.

Cyber risk is a significant concern among insurance companies, appearing prominently in their list of top five risks. Insurers are increasingly worried about cyber breaches that could compromise their data and systems, ultimately leading to both operational, reputational and financial losses. Additionally, the sophistication and innovation of cybercrimes are escalating, heightening insurers’ concerns.

Now that we understand the key risks that insurance companies in South Africa are prioritising, we discuss some best practice approaches that can be employed in measuring operational risks.

Risk testing approaches in an ERM landscape

A robust ERM framework typically involves the following components:

01 **Risk governance and culture**

02 **Risk identification**

03 **Risk measurement and assessment**

04 **Risk monitoring and reporting**

05 **Risk mitigation**

The focus of the rest of this article is to address risk governance and culture and risk measurement and assessment in response to the identified risks noted above.

Risk governance and culture

An effective ERM framework rests on a foundation of rigorous governance structures and a risk-aware culture. Governance structures determine the policies, responsibilities and oversight mechanisms that ensure risk management is embedded across the organisation. Culture ensures that these mechanisms are implemented effectively in day-to-day operations by encouraging transparency, accountability and proactive risk-taking within defined boundaries.

Effective risk governance connects the board, senior management and operational teams through the establishment of distinct committees, reporting lines and escalation protocols. A positive culture reinforces the organisation’s risk appetite, ensures open debate of risks and aligns decision-making with strategic objectives.

Risk measurement

What is risk and how do you measure it?

At its core, risk is the possibility that an unexpected event could occur, something that might disrupt a business's ability to achieve its objectives. This could range from a cyber-attack or power outage, to a sharp drop in the stock market or a failure in internal processes.

In the context of ERM, measuring risk involves assessing both the likelihood of an event occurring and the severity of its potential impact. As outlined earlier, some risks, such as market or credit risk, can often be quantified using models and historical data. Other risks, such as operational or cyber risk, are more difficult to model and often rely on expert judgment, scenario analysis and insights from past events.

As the risk landscape becomes increasingly digital and interconnected, measurement approaches must go beyond financial metrics. Less tangible, but equally critical factors, like system downtime, customer trust, reputational damage and recovery time also need to be considered.

Within this framework, stress testing and scenario analysis play a crucial role, particularly for risks where limited historical data exists, such as emerging or systemic risks. International regulatory frameworks like the Insurance Capital Standard (ICS), Individual Capital Assessment (ICA) and Solvency II recognise these techniques as essential for understanding and managing risk exposures in complex environments.

Risk measurement models – what are they and where do they fit in?

Risk measurement techniques, such as stress and sensitivity testing and scenario analysis, are only as effective as the underlying models used to quantify them. To apply these techniques, a model is required, often a simplified yet representative view of how risks impact a company's financial position. These are typically financial projection models, and they form the cornerstone of any meaningful risk analysis or testing within an ERM framework.

At their core, these models simulate the financial statements of an insurer, projecting key items such as balance sheets, income statements and capital positions under a range of assumptions.

They allow management to assess how specific adverse scenarios (e.g. a market crash, cyberattacks, or catastrophic events) might impact critical business metrics such as solvency, profitability, liquidity and regulatory capital.

More sophisticated models are modular, integrating multiple sub-models that reflect different dimensions of risk. For example:

- an Economic Scenario Generator (ESG) simulates macroeconomic variables like interest rates, inflation and equity returns which influence investment performance and product liabilities.
- a Catastrophe (CAT) model estimates losses from low-probability, high-severity natural disasters (e.g. a 1-in-200-year hurricane), helping insurers quantify their exposure to climate and geographical concentration risks.
- a reinsurance model projects expected recoveries under different treaty structures and stress conditions, accounting for factors like reinsurer creditworthiness and exhaustion of layers.

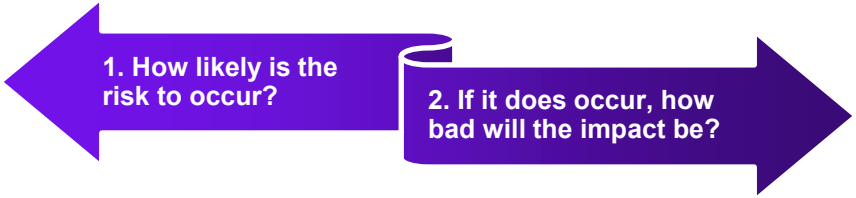
These sub-models must interact dynamically and coherently. Coherence means, for example, that a major natural catastrophe event will likely result in *demand surge inflation,* raising the cost of materials and labor and increasing claim amounts. A robust model would reflect this knock-on effect, as well as the timing and limits of reinsurance recoveries, which may be affected by the financial strain on reinsurers globally after the occurrence of the same catastrophic event.

One example of an integrated approach is the Dynamic Financial Analysis (DFA) model. The DFA model is a forward-looking simulation tool that combines projections of both assets and liabilities under various economic and operational scenarios. It evaluates how different risk drivers evolve over time and interact with each other, such as investment income declining during a market downturn while claims spike due to an operational failure. DFA models typically operate over multi-year time horizons and are used to support strategic decision-making, capital planning, product pricing and Own Risk and Solvency Assessment (ORSA) processes. They can incorporate feedback loops, allow for stochastic (random) inputs and help management understand the full distribution of potential outcomes and not just the expected value. In essence, these models translate abstract risk concepts into quantifiable financial outcomes that decision-makers can act on. They provide the infrastructure upon which stress testing and risk analytics are built.

The remainder of this section will focus on specific risk measurement techniques, such as scenario and sensitivity analysis and reverse stress testing, that rely on such models.

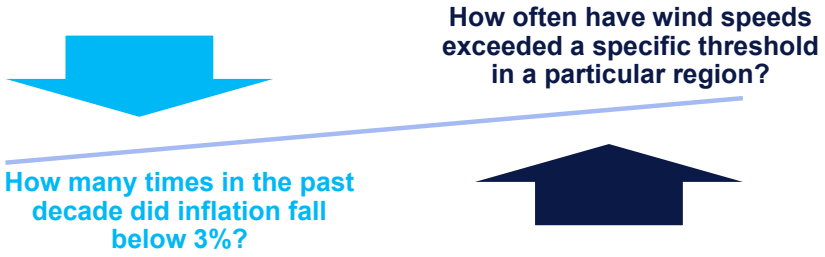
Risk measurement techniques

When measuring any risk, there are two fundamental questions to be answered:



Risk incidence rate (how likely is the risk to occur?)

Some risks lend themselves to historical analysis, where sufficient, relevant data exists. For example:



In these cases, statistical methods like frequency distributions, trend analyses and correlations with macroeconomic drivers (like interest rates, oil prices or central bank policy) are used to estimate likelihoods. These methods can be enhanced through tools like ESGs, which simulate a wide range of future market conditions using a combination of historical calibration and forward-looking views.

However, for emerging risks (such as new regulatory frameworks, climate or nature and biodiversity risks) and company-specific risks (like internal fraud, cyber breaches or operational process failures), reliable data or relevant precedents are often not available to the same extent as for traditional risks. These risks require creative and qualitative approaches.

In these cases, organisations typically:

- conduct structured workshops or expert elicitation involving frontline staff, risk managers, actuaries, IT and compliance representatives, as well as experts in a specific field;
- use scenario mapping to identify triggers and early warning indicators; and
- convert these qualitative inputs into incident rates or probability assumptions that can be used in quantitative models.

For example, if a claims fraud detection system is temporarily weakened due to a technology outage, an internal workshop may estimate that undetected fraud could increase the claims ratio by 2–5% based on management experience. This range can then be stress tested in the financial model.

Risk quantification (if the risk occurs, how bad will the impact be?)

Once we have a sense of the likelihood of a risk occurring, we turn our attention to impact. This is where the risk becomes “real” in financial or operational terms. The goal is to answer: *if this event occurs, what happens to us?*

The severity of impact can be measured using:

- financial outcomes: losses in profit, erosion of capital buffers, cash flow strain, asset write-downs or increased liabilities.
- regulatory metrics: solvency coverage ratios, liquidity ratios and capital adequacy.
- operational metrics: system downtime, claims processing delays, customer churn and reputational damage.

Risk practitioners rely on a suite of risk testing techniques, each suited to different use cases:

- sensitivity testing: focuses on changing a single input at a time (e.g. changing interest rates by ±200bps) to see how sensitive key outputs are to that variable.
- scenario testing: involves simulating multi-variable shocks to reflect complex real-world events. Scenarios can be:

historical (e.g. the 2008 global financial crisis),	*hypothetical (e.g. a major cyber-attack on a cloud provider), and*	*stylised (e.g. an abrupt 30% drop in equity markets).*

- reverse stress testing: starts from the point of failure (e.g. breach of solvency capital requirement) and works backward to identify the combination of shocks that would cause it. This technique is especially useful in surfacing hidden vulnerabilities and preparing contingency plans.

These testing methods are applied on top of the organisation's financial or capital models to simulate outcomes and assess resilience.

For operational or emerging risks where models are less mature or data is sparse, expert-led scenario analysis remains the most practical and flexible tool. For example, one might simulate the financial effects of a ransomware attack causing a 10-day system outage, a surge in call center costs, delayed premium collections and increased reputational fallout.

Whether we are using historical data, expert judgment, or simulation models, the two halves of the equation, likelihood and impact, must be tied together into a coherent narrative and quantifiable output. This combination forms the foundation of effective risk testing and supports key decisions around capital planning, mitigation strategies and risk appetite calibration.

The following sections explore these techniques in more detail, along with how they interact with broader risk governance and business strategy.

Risk-type specific approaches

Enterprise-wide stress testing works best when each risk class is analysed with methods that are tailored to how that risk actually shows up in the organisation. For that reason, we separate the risk universe into four categories:

A Financial risk (insurance, market, credit, liquidity)

These risks move quickly, have deep data histories and translate directly into capital or liquidity shortfalls. Statistically driven engines such as value-at-risk (VaR), Expected Shortfall (ES) and market-shock scenarios effectively capture these risk dynamics, with treasury and asset-liability matching (ALM) teams already owning the data and managing limits. Managing these risks first establishes the organisation's baseline balance-sheet resilience.

Financial risk sits at the heart of every balance-sheet conversation, so the measurement toolbox is long-established and data-rich. Day-to-day exposures are captured with VaR or where regulators require a more tail-sensitive Expected Shortfall view. Both metrics translate market moves, credit-spread shifts and funding stresses into a single "loss-at-confidence-level" number that portfolio managers and boards can understand.

Model credibility can be maintained through back-testing: each day's profit or loss is compared with the previous day's VaR or ES estimate, with parameters tightened whenever realised losses exceed the model's predictions.

However, even well-behaved VaR models can downplay extreme events and risk teams should layer on a suite of stress tests:

- historical scenarios that replay past shocks (some examples can include the 1998 Asian crisis, the 2008 credit crunch and the 2020 COVID-19 liquidity squeeze) using the firm's current positions.
- hypothetical scenarios that impose bespoke curve twists or credit-spread spikes inspired by today's macro fears (for example, a sudden 300-basis-point jump in short-end rates).
- stylised shocks that knock a single risk factor, for example, equities down 30% or oil up 50% to gauge linear sensitivities.

Collectively, these methods reveal the routine volatility a trading desk must shoulder and the extraordinary shocks that would test solvency or drain liquidity lines, enabling boards to set market-risk limits with clear sight of both ends of the distribution.

Insurance risk is also a core component of financial risk, which includes:

- underwriting risk: deviations from expected claims pay-outs due to mispricing, portfolio shifts or unexpected frequency/severity experience.
- catastrophe risk: exposure to low-frequency, high-severity events such as natural disasters.
- reserving risk: deterioration of claims provisions compared to expectations.
- reinsurance risk: inability to recover from reinsurers due to disputes, counterparty default or exhaustion of limits.

B Operational risk

Losses here stem from people, processes, systems and third parties and are often low-frequency and high-severity in nature. Since historical data is sparse, the approach shifts to hybrid methods: loss-distribution modelling where data exists, driver-based regressions where indicators explain losses and expert scenario workshops where imagination must fill the gaps. The Association for Savings and Investment South Africa (ASISA) guidelines in respect of taxonomy and near-miss reporting reinforce the need for a quantitative-qualitative blend.

Operational risk is far-reaching: fraud, data errors, process breakdowns, system outages and third-party mishaps seldom follow neat distributions. Where loss data is plentiful, firms will deploy a Loss Distribution Approach (LDA), fitting frequency and severity curves and then shifting them under stress to estimate capital for a 1-in-200-year loss.

When data is thin, risk teams build driver-based regressions linking losses to causal indicators: transaction volumes, staff turnover, change-request counts and macro variables. Due to the wide-spread nature of these risks, blind spots are prevalent. Organisations therefore convene scenario-analysis workshops whereby underwriters, actuaries, IT architects and compliance officers craft “extreme-but-plausible” narratives: a rogue-trader incident that evades controls; a supply-chain collapse that idles claims servicing; a cloud lock-out that freezes policy administration for ten days. Expected incident frequencies and loss severities from those workshops feed directly into capital models.

Continuous-control monitoring closes the feedback loop. Real-time risk indicators such as failed logins, access-override counts, batch-process errors and vendor breaches trigger escalation long before financial losses appear. This blend of data, expert judgement and live key risk indictors (KRI) mirrors the ASISA operational-risk guideline, which emphasises near-miss reporting, root-cause analysis and thresholds that scale to firm complexity.

C Cyber/Information and Communication Technology (ICT) risk (a focused subset of operational risk)

Technically a subset of operational risk, cyber risk merits stand-alone treatment. The European Insurance and Occupational Pensions Authority’s (EIOPA) cyber stress-testing principles highlight how a single ransomware wave or cloud-provider outage can propagate system-wide, creating downtime, restoration costs and regulatory fines that dwarf ordinary operational risk events. Dedicated scenarios, metrics and governance, often led by the chief information security officer (CISO), can prevent cyber exposures from being lost in generic operational averages.

Cyber risk has become material and substantially different in propagation speed and systemic reach. We, therefore, assess this risk separately even though it sits within the broader operational risk taxonomy.

EIOPA’s cyber-stress-testing principles frame the risk on two fronts:

- cyber resilience: the firm as a direct target. Stress tests model ransomware waves, cloud-provider outages, data-exfiltration or large-scale denial-of-service attacks. Impact metrics extend beyond cash payouts to system downtime, recovery and forensics spend, regulatory fines and softer hits to reputation and customer trust.
- cyber underwriting exposure: for insurers that sell cyber cover. Here, accumulation scenarios test a single software vulnerability exploited across thousands of policyholders, checking that gross and net (post-reinsurance) losses fit within risk appetite and capital.

Because cyber events leap across borders and vendors, scenarios must reflect service-provider concentration and “demand-surge” effects.

D Business continuity, resilience and third-party risk

Finally, we test whether the firm can keep delivering its services under systemic stress such as pandemic surges, grid failures or a critical vendor collapse. Reverse stress testing pinpoints single points of failure while continuity planning assesses how quickly alternate sites, staff or suppliers can restore operations. This cross-cutting lens forces the organisation to stitch together insights from the other three buckets into a coherent crisis playbook.

Business continuity risk turns the lens outward to question whether the organisation can keep delivering critical services when systemic shocks hit. Modern continuity programmes now assume pandemics, grid failures, geopolitical sanctions or major dependencies on third parties.

Risk teams first run forward scenarios: how long can policy servicing run on generator power? Can claims triage shift to an alternate site? Then apply reverse stress testing, asking: “What combination of data-center outages, supplier defaults and staff unavailability will breach our capital or liquidity buffers?”

Mapping those dependency chains from the scenarios pinpoints where additional redundancy, vendor diversification or contingency funding is needed. The results feed straight into funding-plan triggers, vendor-resilience clauses and board-approved crisis playbooks.

Grouping risks in this manner achieves the following goals:

It pairs the right measurement method with the relevant risk behavior: statistical engines for market shocks, scenario workshops for operational surprises, specialised tests for cyber contagion and reverse stress tests for end-to-end service failure.

It aligns risks management with organisational ownership: chief financial officer and/or treasury function for financial risk, chief operating office and/or risk function for operational risk, CISO for cyber/ICT risk and the enterprise resilience team for continuity.

It avoids both double counting and blind spots, because boundary events (for example, an operational failure triggering a financial loss) are explicitly tagged and measured in only one place.

It mirrors international regulatory expectations, from Solvency II's separation of market and operational modules, to EIOPA's dedicated cyber guidance and ASISA's operational-risk taxonomy, ensuring that stress tests speak the same language as supervisors and rating agencies.

Where stress testing sits in ERM

Stress testing is the bridge between model-heavy risk analysis and board-level decision-making. Results flow straight into risk appetite statements, capital and liquidity limits, contingency-funding triggers and recovery/resolution playbooks.

Regulators formalise this link: insurers must evidence capital resilience through the ORSA. By embedding the outputs of multi-risk stress tests into those supervisory processes, insurers will be able to demonstrate that the capital they hold for day-to-day volatility is also sufficient for the "1-in-200-year" shock.

Implementation roadmap: seven practical steps

Global guidance from Moody's converges on a common cycle that can be applied to any stress testing exercise[2]:

01 **Define scope and objectives: identify entities, risk types and appetite thresholds the test must address.**

02 **Select scenario types: blend historical, hypothetical, stylised and reverse stress testing scenarios to capture both known and emerging threats.**

03 **Select modelling methods: deploy LDA, Monte-Carlo engines, regression models or expert judgement according to the data at hand.**

04 **Validate, calibrate and quantify: benchmark assumptions, reconcile to recent events and translate shocks into capital, liquidity, profit or loss, downtime, fines and reputational impacts.**

05 **Report and act: present findings and mitigation options to senior management and/or the board; update limits or controls as required.**

06 **Monitor and refresh: feed near-misses, key-risk-indicator trends and horizon-scanning insights into the next testing cycle.**

07 **Document and evidence: maintain clear audit trails for supervisors and internal assurance.**

[2] https://www.moodys.com/web/en/us/insights/banking/stress-testing-best-practices-a-seven-steps-model.html?

KPMG

These steps turn stress testing from a one-off modelling exercise into a living governance tool, one that continuously aligns capital, appetite and strategy with a rapidly evolving risk landscape.

Set out below is our view on additional forward-looking considerations that can be incorporated by insurers:

Embed insurance risk metrics directly alongside market and credit risk in the capital model, so that volatility from claims, catastrophe events or technical reserves is assessed with equal rigour.

Expand stress testing to integrate underwriting, reserving and reinsurance shocks with market, credit and liquidity stresses to produce a single capital impact view.

Maintain continuous feedback loops from near-miss analysis, claims experience and reinsurance recoveries into model calibration.

Strengthen governance oversight so that the board understands tail dependencies. For example, how a catastrophe event could affect both underwriting losses and market asset values simultaneously.

Use scenario narratives that combine financial, operational and reputational dimensions to test resilience in ways models alone cannot.

KPMG

Comparative summary table

Set out below is a summary of the four risk categories discussed under “Risk-type specific approaches”. It reflects:

(i) the preferred testing methods for each class; and

(ii) the metrics leaders most often track when judging whether risks remains within appetite.

Risk category	Core testing techniques	Primary metrics and outputs
Financial (insurance/ market/ credit/ liquidity)	• VaR/Expected Shortfall models • Sensitivity runs • Historical and hypothetical stress scenarios	• Potential loss distribution • Capital and liquidity coverage • Limit breaches • Funding gap under stress
Operational	• Loss-Distribution Approach • Driver-based regressions • Scenario workshops (“extreme-but-plausible”) • Continuous KRI monitoring	• Tail loss (99.5% level) • Frequency-severity curves • Control-gap diagnostics • Near-miss frequencies
Cyber/ICT	• Cyber-specific scenario analysis (ransomware, cloud outage, data breach, denial-of-service attack) • Accumulation tests for insurers (portfolio clustering)	• Direct cash loss • System-downtime hours • Restoration and forensics spend • Regulatory fines • Reputational impact narrative
Business continuity/ third-party resilience	• Systemic or external shock scenarios (pandemic, grid failure, geopolitical sanctions) • Reverse stress testing to locate single-points-of-failure	• Service interruption cost • Recovery-time objectives • Vendor dependency heat-map • Contingency-plan readiness

Conclusion

We discussed the current ERM landscape for South African insurers, detailing key risk categories, risk measurement techniques and how major insurers perceive and rank these risks. It also emphasises the increasing complexity and importance of non-financial and operational risks.

We recommend that Risk Committees develop a risk appetite framework to communicate and monitor the amount and type of risks it is willing to accept to achieve its strategic objectives. Our view is that to achieve this, the risk appetite framework needs to be underpinned by appropriate risk measurement models that are suitable for the insurer’s unique circumstances and strategic objectives.

As the industry navigates an increasingly complex and dynamic risk landscape, it is important for insurers to evolve their enterprise risk management frameworks beyond traditional financial metrics. With the increased frequency and severity of operational risks, a more holistic, data-informed and scenario-driven approach is required to ensure that insurers are risk resilient.

Through uniting governance and culture with robust quantitative and qualitative techniques, and explicitly integrating insurance risks into measurement frameworks, insurers will be better positioned to withstand shocks, meet regulatory expectations and protect stakeholder value.

KPMG