aim
AFRICA INSURANCE MAGAZINE

irmic
INSURANCE & RISK MANAGEMENT INFORMATION CENTRE

Chief Risk Officers Convention 2026

Theme: *Future-proofing: Strategic Risk Management for Resilience*

REPORT

Email: andrew@irmic.co.zw
Call/WhatsApp: +263 78 316 3516 | +263 71 679 2708
Website: www.irmic.co.zw

Editor's Note

AIM Publications, an arm of the Insurance & Risk Management Information Centre successfully hosted the 2nd Annual Chief Risk Officers Convention at the prestigious Troutbeck Resort in Nyanga from 3 – 6 June, 2026.

Themed future-proofing: strategic risk management for resilience, the convention brought together over 100 senior risk executives across Zimbabwe. This convention was a landmark gathering, a testament to the growing recognition that strategic risk management is not merely a corporate function, but a cornerstone of national transformation. In an era defined by rapid technological disruption, climate uncertainty, geopolitical volatility, and the expanding frontier of Artificial Intelligence, the imperative to future-proof our institutions has never been more urgent.

Zimbabwe stands at a pivotal moment in its economic journey; pursuing the national 2030 Agenda of building an upper middle class economy and strategic risk management is a critical pillar. By embedding robust, forward-looking risk frameworks across public and private institutions, we lay the foundations for a sustainable, resilient economy, one capable of withstanding shocks, seizing emerging opportunities, and delivering lasting prosperity for every Zimbabwean. The conversations, insights, and commitments forged at this years' edition of the convention were not the end of a dialogue; they are the beginning of a transformation.

We humbly extend our sincere gratitude to the organizations, government ministries, departments and agencies for partnering and actively participating at the convention and we look forward to hosting you at the National Conference on Risk Management this September.

Enjoy reading!

Andrew Chinoperekwei
Programs Director
andrew@irmic.co.zw, +263 78 316 3516

The 2026 CROs Convention Strategic Resolutions

Following extensive deliberation by delegates representing all sectors of Zimbabwe's economy and governance landscape, the 2026 Annual Chief Risk Officers Convention adopted the following four resolutions. These resolutions were made unanimously:

Resolution 1: National Risk Management Report

The Convention resolved to spearhead the development and publication of a National Risk Management Report, led by dedicated committees drawn from the risk management community. This report will serve as a critical national reference document, capturing the current state of risk management practice across Zimbabwe's public and private sectors, identifying gaps and opportunities, and providing the evidence base for risk-informed policy development. The Report will be made available to all government ministries, regulatory bodies, and institutional stakeholders.

Resolution 2: Transformation of the Risk Management Function

The Convention commits to driving the transformation of risk management in Zimbabwe from a compliance exercise to a strategic enabler, integrating risk thinking into every decision-making process at all levels, from national policy formulation to organisational operations. This resolution affirms that effective governance is inseparable from effective risk management, and that Zimbabwe's long-term development agenda depends on institutions that make decisions with full awareness of the risks and opportunities they face.

Resolution 3: Sectoral Symposiums and Training Programmes

The Convention resolved to roll out sectoral symposiums and targeted training programmes across Zimbabwe, commencing with a Public Sector Risk Management Symposium to be held in partnership with the Ministry of Finance, Economic Development and Investment Promotion. This Symposium will build sector-specific risk management capacity within government institutions, equipping public servants, from senior officials to operational staff, with the knowledge, tools, and frameworks to manage risk effectively in the public sector context.

Resolution 4: National Conference on Risk Management

While the Chief Risk Officers Convention serves risk executives and senior practitioners, the Convention recognised the need for an inclusive, country-wide platform open to every risk professional in Zimbabwe regardless of seniority, sector, or specialisation. The Convention resolved to establish a National Conference on Risk Management as a flagship annual event, bringing together practitioners, academics, regulators, and policymakers under one roof to advance the national risk management agenda.

The National Conference on Risk Management is proposed to be launched in September 2026 in Kariba, with the formal support and co-hosting of the Ministry of Finance, Economic Development and Investment Promotion.

CROs Convention Chairperson Welcome Remarks Reflections

In her opening address, the Chairperson of the convention, Ms. Margaret Mukurazhizha welcomed delegates to the Chief Risk Officers Convention 2026, hosted by AIM Publications, an arm of the Insurance Risk Management Information Centre (IRMIC) at Troutbeck Resort, Nyanga, under the theme "Future Proofing: Strategic Risk Management for Resilience."

She reflected on the symbolism of Nyanga's mountains, rivers, and landscapes as a fitting backdrop for a convention centred on resilience and renewal, drawing a parallel between Zimbabwe's own journey through adversity and the role of risk leaders in building institutions that can withstand disruption. She likened the resilience required of chief risk officers to the endurance of the baobab tree and the granite mountains of Nyanga, noting that Zimbabwe's economy had demonstrated similar reinvention across agriculture, mining, tourism, and technology.

She described future proofing as requiring the courage to anticipate risk, the wisdom to adapt, and the vision to transform uncertainty into progress. She called on delegates, as custodians of resilience and modern-day architects of Zimbabwe's future, to embody the strategic foresight and to craft strategies that would safeguard their organisations and inspire future generations while paving the way to achieve NDS2 (positioning Zimbabwe to be an upper middle class economy by 2030) and Agenda 2063 (focusing on transforming Africa into a global powerhouse).

She closed her remarks by thanking the Ministry of Finance, Economic Development and Investment Promotion for supporting the convention, the organising committee, sponsors, partners, and all participants for making the gathering possible, expressing hope that the convention's deliberations would ignite bold ideas and resilient strategies.

The central argument is clear: the world has entered an age of intelligence where risks are faster, more interconnected, and more disruptive than ever before. Traditional risk management frameworks are no longer adequate. The region faces a historic opportunity to leapfrog legacy systems, embrace intelligent technologies, and reposition African institutions from being passive recipients of global risk trends to becoming proactive, resilient leaders in the new digital era.

Public sector risk management & ESG framework: building resilient, transparent, and accountable public institutions

Sanguita Popatlal, Chief Director, Corporate Governance Unit in the Office of the President Cabinet

Across the public sector, the convergence of fiscal pressure, technological vulnerability, and growing demands for transparent governance has elevated risk management from a compliance function to a strategic imperative. These insights were shared by Ms. Sanguita Popatlal who was the Guest of Honour at the convention representing the Mr. Allen Choruma. Her presentation outlined the current risk landscape, the

governance structures best placed to address it, and the concrete actions institutions can take to embed resilience into their operations.

At its core, the framework rests on four interlocking themes: integrated Enterprise Risk Management (ERM), Environmental, Social, and Governance (ESG) accountability, compliance with International Public Sector Accounting Standards (IPSAS), and a governance model that distributes responsibility clearly across all organisational lines.

Why risk management matters

The public sector operates under a unique mandate: it cannot exit difficult environments, must serve every citizen equitably, and is held to standards of accountability that far exceed those applied to private enterprises. Against this backdrop, robust risk management is not optional, it is the mechanism through which governments protect resources, sustain services, and maintain public trust.

- ✓ Protects public resources and reduces financial waste,
- ✓ Improves continuity of essential service delivery,
- ✓ Strengthens governance structures and ministerial oversight,
- ✓ Builds and maintains public trust and institutional accountability.

Enterprise risk management (ERM) framework

The framework adopts a full-cycle ERM methodology: Identify ◎ Assess ◎ Manage ◎ Monitor. This continuous loop is aligned to the strategic objectives of each public entity, embedded across Ministries, Departments, and Agencies (MDAs), and supported by ongoing monitoring and reporting mechanisms.

ESG risk framework: public sector context

Ms. Sanguita highlighted that, ESG considerations are no longer the exclusive domain of the private sector. For public institutions, Environmental, Social, and Governance risks carry a distinct character shaped by a mandate to serve society, manage multi-generational assets, and act as the regulator and rule-setter simultaneously.

Implementation progress: CIAU annual report 2025

The Central Internal Audit Unit (CIAU) 2025 Annual Report demonstrates tangible momentum in rolling out the ERM framework across government:

- ✓ 23 MDAs trained, with a focus on ministries,
- ✓ 580 senior executives trained in risk management principles and application,
- ✓ 800+ risk champions deployed across institutions to embed a risk-aware culture,
- ✓ Ongoing institutional rollout to extend coverage to all remaining public entities.

Future state vision

The presentation charts a clear target state for public sector risk management, one that moves beyond compliance and towards genuine organisational resilience:

- ✓ Fully integrated governance, ERM, ESG, and IPSAS frameworks operating as a cohesive system,
- ✓ Real-time risk dashboards across all MDAs providing dynamic, actionable intelligence,
- ✓ A shift from reactive compliance to proactive, risk-based decision-making at all levels,
- ✓ Public institutions that are resilient, transparent, and worthy of citizen trust.

Key recommendations

Drawing on the analysis and implementation evidence presented at the annual chief risk officers convention by the Guest of Honour, Ms. Sanguita Popatlal, the following recommendations are offered to public sector leaders and risk practitioners:

Embed ERM across all institutions

Continuously roll out the full ERM lifecycle: identify, assess, manage, and monitor to all MDAs. Use the Three Lines Model to assign clear accountability at management, oversight, and assurance levels. Extend the risk champion network beyond the current 800+ to ensure every operational unit has an embedded advocate

for risk awareness.

Strengthen cybersecurity and digital governance

Given the elevated risk of cyberattacks and data breaches, institutions should invest in dedicated ICT risk frameworks, conduct regular penetration testing, and establish incident response protocols. Cybersecurity maturity assessments should be incorporated into the annual internal audit plan.

Integrate ESG into strategic planning

Public institutions should formally incorporate ESG risk factors: climate resilience, equity of service delivery, workforce well-being, and governance transparency into their annual strategic and operational risk registers. Every identified high-risk ESG item must be assigned to a named departmental owner with measurable mitigation targets.

Public institutions should formally incorporate ESG risk factors: climate resilience, equity of service delivery, workforce well-being, and governance transparency into their annual strategic and operational risk registers. Every identified high-risk ESG item must be assigned to a named departmental owner with measurable mitigation targets.

Invest in real-time risk intelligence

The presentation made one thing clear, progress towards real-time risk dashboards across all MDAs should be a strategic technology priority. Dynamic dashboards reduce the lag between risk materialisation and management response, enabling proactive rather than reactive governance.

Build a culture of risk awareness

Sustained investment in training is critical. The 580 executives and 23 MDAs already trained represent a strong foundation, but risk literacy must cascade to all levels of the public service. Annual risk management forums, peer learning networks, and mandatory refresher training will ensure the culture endures beyond individual champions.

Effective risk management = resilience, sustainable governance

The public sector operates at the intersection of fiscal constraint, citizen expectation, and systemic risk exposure. The Guest of Honour speech by Ms. Sanguita Popatlal demonstrates that effective risk management is not a bureaucratic overhead, it is the engine of effective governance and a strong pillar for achieving the NDS2 rooted in Zimbabwe attaining an upper middle class economy by 2030.

When ERM, ESG, and IPSAS are integrated and embedded across institutions, the result is not merely compliance, it is a public sector capable of delivering on its mandate with transparency, accountability, and resilience. The implementation progress documented in the CIAU 2025 Annual Report is encouraging; the path forward is clear.

Risk leadership transformation: leading Zimbabwe, SADC and the world through the age of artificial intelligence

Dr. Eng. Martin Manuhwa, Managing Consultant, ZAIDG Consulting Engineers

In this keynote address at the annual CROs convention, Dr. Eng. Martin Manuhwa delivered a compelling call for a fundamental transformation in how risk leaders in Zimbabwe, SADC, and Africa approach their profession in the era of Artificial Intelligence and the Fourth Industrial Revolution (4IR).

The central argument is clear: the world has entered an age of intelligence where risks are faster, more interconnected, and more disruptive than ever before. Traditional risk management frameworks are no longer adequate. The region faces a historic opportunity to leapfrog legacy systems, embrace intelligent technologies, and reposition African institutions from being passive recipients of global risk trends to becoming proactive, resilient leaders in the new digital era.

The evolving risk landscape

Dr. Manuhwa opened with a stark assessment of today's risk environment. Risks are no longer isolated events; they cascade across interconnected systems. A cyberattack can trigger a power failure, which leads to telecommunications outages, banking disruption, economic loss, and ultimately social instability. The presentation cited the World Economic Forum's 2026 outlook, which identifies uncertainty as the defining theme of the global risk horizon.

The top risks facing organisations and nations today include cybersecurity threats, climate change, geopolitical conflict, supply chain disruption, AI-generated risks, economic volatility, infrastructure failure, and disinformation. Traditional approaches; quarterly reporting, historical analysis, reactive response, and siloed functions are being replaced by the demands of continuous monitoring, predictive analytics, proactive prevention, and integrated intelligence.

Artificial intelligence in risk management

AI is already transforming risk management across multiple domains. The presentation outlined an AI-powered Risk Command Centre model capable of simultaneously monitoring cyber threats, operational risks, financial risks, climate risks, supply chains, and critical infrastructure.

Sector applications

- ✓ Banking and financial services: AI-powered fraud detection, AML monitoring, liquidity forecasting, behavioural analytics, and risk scoring
- ✓ Energy: smart transformer monitoring, predictive maintenance, remote diagnostics, and grid resilience
- ✓ Healthcare: telemedicine, disease surveillance, predictive analytics, and population health intelligence
- ✓ Generative AI: emerging use in AI risk advisors, board decision support, regulatory monitoring, and automated reporting
- ✓ Digital twins: virtual replicas of physical systems are highlighted as a particularly powerful tool, enabling organisations to predict failures, simulate emergencies, reduce costs, and improve planning.

Human-centred risk leadership

Despite the transformative power of AI, the presentation was unambiguous: AI cannot replace the essentially human qualities that define great risk leadership. These include judgment, ethical reasoning, contextual understanding, empathy, curiosity, wisdom, and personal responsibility.

The future risk practitioner is envisioned as more than a technical domain expert. They must be a big-picture thinker, an innovator, and an ethical leader skilled at defining the right problems, navigating complexity and uncertainty, and leading collaborative responses to systemic challenges.

The evolution of the risk function was mapped from risk officer through risk manager, risk executive, and chief risk officer, towards the emerging roles of strategic risk leader and enterprise intelligence leader.

Recommendations and key takeaways

For risk leaders and organisations

- ✓ Transition from reactive risk management to AI-enabled predictive risk intelligence, integrating continuous monitoring and scenario simulation
- ✓ Invest in cyber resilience as a boardroom priority, not just an IT function, covering critical infrastructure, financial systems, and supply chains
- ✓ Embed climate and ESG risk formally into enterprise risk frameworks, treating climate exposure as a core business risk
- ✓ Adopt the five leadership priorities for future boards: AI-enabled risk intelligence, cyber resilience, climate risk management, digital leadership skills, and strategic risk transformation.

For professional development

- ✓ Future risk practitioners must build competency across digital literacy and data analytics, AI and cybersecurity, data science, sustainability, human behaviour, and strategic thinking
- ✓ Continuous professional development and stronger collaboration between academia and industry are essential for closing the skills gap
- ✓ Professional bodies should update codes of conduct to embed AI ethics, data governance, and responsible technology use as core obligations

For governments and regulators

- ✓ Invest in local data centres and computing infrastructure to close the AI computing power gap
- ✓ Fund AI training datasets that represent African languages, cultures, and contexts.
- ✓ Develop consistent national and regional AI policies with strong oversight and cross-border institutional coordination
- ✓ Institutionalise Quality-Based Selection (QBS) in public procurement legislation for complex infrastructure projects, moving beyond lowest-cost contracting to merit-based selection

For the region (Zimbabwe and SADC)

- ✓ Build a regional resilience network through cross-border data sharing, regional early warning systems, shared cyber defence, integrated infrastructure planning, and collective risk intelligence
- ✓ Leverage Africa's demographic advantage, the youngest and fastest-growing population globally to leapfrog legacy systems and build digital-native infrastructure
- ✓ Pursue Zimbabwe's intelligent nation vision across smart energy, healthcare, agriculture, digital finance, e-government, and smart infrastructure

Conclusion

"The future will not be built by those who fear uncertainty. The future will be built by those who learn to lead through it."

The keynote closed with a call to action grounded in both urgency and optimism. Zimbabwe has the talent. SADC has the potential. Africa has the opportunity. The question is not whether transformation is coming, it is whether the region's risk leaders will be the architects of that transformation or its subjects.

The path is clear: Risk ◎ Insight ◎ Strategy ◎ Resilience ◎ Prosperity. AI will generate answers, but humanity must still determine the values, purpose, direction, and meaning that guide those answers.

Fundamentals of riskmanagement: designing a risk framework from policy to practice

Prof. Stanley Mutenga, CEO, Starz Risk Solutions

This article summarises a practical presentation delivered at the CRO Convention 2026 by Prof. Stanley Mutenga, CEO of Starz Risk Solutions. The presentation offers step-by-step guidance for designing an Enterprise Risk Management (ERM) framework applicable to both private institutions such as insurance companies and public sector entities including State-Owned Enterprises (SOEs), government ministries, utilities, regulatory authorities, and local authorities.

The central argument is that a risk framework should not begin with a generic risk register. Instead, it must be anchored in a deep understanding of how the institution creates value, delivers its mandate, and remains sustainable. Only from that foundation should risk owners, appetite, controls, Key Risk Indicators (KRIs), and reporting structures be derived.

Core principle

Before any risk categories or registers are created, organisations must answer one fundamental question:

"How does this institution create value, deliver its mandate, and remain sustainable?"

The risk universe, risk owners, appetite, controls, KRIs, and reporting structure should all flow from the answer to that question.

The 12-step risk framework

Define the institutional mandate and strategic objectives

The starting point is clarity on what the institution is trying to achieve. For a private insurer, objectives include growing profitable underwriting income, maintaining solvency, and strengthening reinsurance protection. For a public utility, objectives include reliable service delivery, reducing losses, and maintaining financial sustainability. The practical output of this step is a Strategic Objective–Risk Linkage Table mapping each objective to what could prevent its achievement and who owns that risk.

Map the business model

The organisation must document how it creates and protects value through its value chain. For an insurer, this runs from Strategy through Product Design, Underwriting, Claims, Reinsurance, and Investment to Regulatory Reporting. For an SOE, the value chain moves from National Mandate through Service Delivery, Revenue Management, and Asset Management to Governance and Accountability. This value chain becomes the foundation of the risk universe.

Derive the risk universe from the business model

Rather than using generic risk categories, risks are derived from each point in the value chain. For most SOEs, regulators, and public institutions, the recommended Level 1 Risk Universe comprises four domains:

- ✓ Strategic mandate delivery: risks to achieving constitutional, statutory, and policy objectives
- ✓ Service delivery & operations: risks to efficient, reliable, and safe service provision
- ✓ Corporate services: risks arising from finance, ICT, HR, procurement, and supporting functions
- ✓ Governance, oversight & transformation: risks to governance, leadership, and institutional resilience

Within each domain, risks are further classified as financial risks (affecting revenue, funding, liquidity, capital), conduct risks (affecting ethics, compliance, and stakeholder trust), and operational risks (affecting processes, people, systems, assets, and service delivery).

Assign clear risk ownership

A common failure is treating risk as everyone's responsibility, which in practice means nobody owns it. Each risk must be assigned an Executive Owner, an Operational Owner, and an Oversight Function. For example, investment risk is owned by the CFO at the executive level, managed by the Investment Manager at the operational level, and overseen by the Risk Committee.

Define risk appetite and tolerance

Without defined risk appetite, risk management becomes opinion-based. Each risk domain should carry an explicit appetite statement and measurable tolerance thresholds using a Green-Amber-Red framework. For instance, an SOE in the Governance domain should carry zero tolerance for fraud, corruption, regulatory breaches, and misreporting. For Service Delivery, a low appetite is recommended with tolerance thresholds such as critical service downtime below four hours and infrastructure availability above 95%.

Build the risk register from the risk universe

The risk universe is the full map of all possible exposures. The risk register is the active management tool that identifies which specific risks require immediate attention. Each registered risk should include an exposure assessment, a list of risk drivers, and linkage back to the relevant domain and appetite threshold.

Develop KRIs for each material risk

KRIs are the early warning system that signals when a risk is worsening before it becomes a crisis. Each KRI should have defined Green, Amber, and Red thresholds. For example, for Service Continuity Risk in an electricity utility, the KRI of Grid Availability is Green above 98%, Amber between 95–98%, and Red below 95%.

Link risks to controls

Controls must be mapped to each risk exposure across three categories: Preventive Controls (stopping the risk from materialising), Detective Controls (identifying when the risk is increasing), and CorrectiveControls(responding when the risk materialises). This structure should reflect the Three Lines of Defence model, with management owning preventive controls, risk and compliance functions owning detective monitoring, and internal audit providing independent assurance.

Integrate risk into decisions

Risk management has no value unless it changes decisions. Every major decision paper presented to the Executive Committee or the Board must include a documented assessment covering key risks, risk appetite implications, financial impact, stress scenarios, and management actions. This applies to strategy approvals, capital projects, procurement decisions, and budget allocations.

Design practical reporting

Reporting must be designed for the audience and their decision-making needs. The Board should receive quarterly reports on top risks, appetite breaches, and strategy risks. The Board Risk Committee should receive quarterly reports on KRIs and emerging risks. The Executive Committee needs monthly updates on risk actions, incidents, and controls. Risk owners require detailed monthly reports on risk and control performance.

Test the framework

A risk framework must be stress-tested using realistic scenarios. For a public utility, a scenario such as a major supplier failure during peak demand should test procurement continuity, alternative supplier arrangements, service delivery impact, financial exposure, and stakeholder response. Scenario testing reveals weaknesses before they become crises.

Move from framework to behaviour

The framework is only effective if it changes how people behave. Risk ownership must shift from the CRO to the business. Bad news must be escalated early rather than concealed. Risk appetite must drive limits and management actions rather than remaining a generic statement. Controls must be tested rather than assumed effective.

The mature ERM line of sight

The hallmark of a mature public-sector ERM framework is a clear, unbroken line of sight connecting every element of the organisation's risk management to its mandate and performance:

National Development Objectives ⚜ Institutional Mandate ⚜ Business Model ⚜ Risk Universe ⚜ Risk Appetite ⚜ Risk Ownership ⚜ Controls ⚜ KRIs ⚜ Reporting ⚜ Decisions ⚜ Performance

This approach aligns with the principles of ISO 31000, COSO ERM, and modern results-based management systems. It ensures that risk management ceases to be a compliance exercise and becomes an operating system for better decisions.

Closing note

A practical risk framework is not a policy document. It is a living system that must mirror how the institution is managed, speak the language of its executives, and influence every significant decision. The test of its effectiveness is not whether risks are reported, it is whether risk information changes strategic choices, project approvals, procurement decisions, budget allocations, and service delivery priorities.

From risk expert to strategic leader: the architecture of influence

A playbook for the modern CRO, head of risk, and risk manager

Socrates Mhlanga, CEO, Signal Radar Group

Risk is everywhere. Every business decision, every strategic choice, every moment of inaction carries uncertainty and that uncertainty, managed well, is the engine of growth. Managed poorly, it is the source of decline. Yet most organisations remain fundamentally poor at managing risk. Not because they lack frameworks or tools, but because the risk function has not made the leap from technical expertise to strategic influence.

This article draws on the keynote at the chief risk officers' convention 2026 delivered by Socrates Mhlanga: From Risk Expert to Strategic Leader: The Architecture of Influence to chart the practical playbook for modern risk leaders. It covers the universal barriers to effective risk management, the three foundations of a sound risk function, the invisible architecture of organisational decisions, the RADAR intelligence methodology, the 4C narrative structure, and ten recommendations for risk leaders ready to make the transition from expert to strategic influencer.

Risk is everywhere and most organisations handle it poorly

Risks are uncertain events that could affect the achievement of goals. That definition is deceptively simple. In practice, it means that every strategic priority, every investment decision, every operational process exists within a field of uncertainty. There is more change and complexity in the operating environment today than at any previous point and that trajectory is not reversing.

Risk appetite sits at the heart of this reality. Too much risk leads to disaster. Too little leads to gradual decline a quieter failure, but a failure nonetheless. Businesses that refuse to take calculated risks in pursuit of growth and competitive positioning do not stay still; they fall behind.

The three foundations: culture, process, and governance

Getting risk management right is not a matter of deploying the most sophisticated tools. It requires getting three foundations right: culture, process, and governance. Of the three, culture is by far the hardest and by far the most important.

"The measure of a risk function is not the quality of its risk register or processes. It is how problems are solved and the quality of the decisions made in its presence."

Recommendations for the modern risk leader

The following recommendations are grounded in the keynote's frameworks and are designed for CROs, Heads of Risk, and risk managers who are ready to make the transition from technical expert to strategic leader:

Start with an honest influence audit

Ask the question the keynote poses directly: how influential are you? Map the last ten significant organisational decisions and determine honestly whether risk intelligence was decisive, marginal, or absent. The answer defines the starting point for the transition ahead. Without this diagnosis, any improvement effort is directionally blind.

Fix the culture before the processes

Do not invest in process sophistication while the underlying culture prevents the right risks from reaching the table. Begin with the hardest work: creating an environment where challenging the status quo is safe, risk flows horizontally as well as vertically, and data overrides seniority in risk conversations. Without this foundation, the best process produces the most polished wrong answers.

Keep the risk process deliberately simple

Resist the temptation to sophisticate the risk management cycle beyond what the organisation can consistently sustain. The Identify ◎ Assess ◎ Treat ◎ Monitor cycle, applied consistently and aligned to business goals, delivers more value than an elaborate methodology applied inconsistently. Complexity that limits adoption is itself a risk management failure.

Structure every communication around the 4Cs

Retire risk report templates that are built for completeness. Replace them with the 4C structure: Context (the live decision), Connection (the specific risk linkage), Consequence (quantified impact), and Call to Action (a recommendation that reframes the decision). Every risk communication should end with a position, not a summary of considerations.

Build the system, not just the effort

The leverage principle demands that you invest in building systems recurring intelligence-gathering cadences, stakeholder relationship rhythms, pre-meeting engagement protocols rather than working harder within the existing model. Map the moments in the organisation's decision cycle where risk intelligence can be introduced most effectively, and build repeatable processes for each of them.

Measure influence, not activity

Replace or supplement internal activity metrics: reports produced, risks logged, audits completed with outcome-based measures of decision quality. Track specific instances where a decision was made differently because of risk intelligence. Build a library of these moments. Present them to the Board as evidence of value. The function that cannot demonstrate this will always be the first candidate for de-prioritisation.

Transition from risk expert to strategic leader

"Success is not a better risk report. Success is a decision made differently because of your risk intelligence."

The transition from risk expert to strategic leader is not a career stage, it is a fundamental choice about what the risk function is for. The expert produces analysis. The strategic leader shapes decisions. Both require deep technical competence, but only one creates the kind of value that makes the risk function indispensable rather than merely necessary.

The architecture of influence presented in this keynote, built on cultural foundations, navigating the invisible decision landscape, filtered through RADAR, and delivered via the 4C structure is a practical, adoptable playbook. It does not require a new title or a larger budget. It requires a shift in mindset: from reporting the past to shaping the future.

The risk leaders who make this shift will not just survive the next five years of transformation in the profession, they will define what the profession becomes.

From policy to practice: bridging the gap between risk frameworks and organisational performance

Professor Stanley Mutenga, Chief Executive Officer, Starz Risk Solutions

This article summarises the keynote presentation delivered by Prof. Stanley Mutenga, CEO of Starz Risk Solutions. The presentation challenges conventional thinking about risk management in both private and public sector institutions, arguing that the most dangerous gap in modern organisations is not between risk identification and risk assessment, but between risk knowledge and risk-informed action.

The central provocation of the presentation is captured in a single question posed to every risk professional in the room:

"If risk management disappeared from your organisation tomorrow, would decision-making change?"

Organisations today have more risk infrastructure than at any point in history: comprehensive policies, dedicated risk committees, extensive audit programmes, detailed risk registers, and layers of compliance review. Yet corporate failures, governance crises, strategic collapses, fraud scandals, and cyber incidents continue at an alarming pace.

If the honest answer is no, then what exists is risk documentation, not risk management. The presentation builds from this premise to offer a diagnostic of why risk management so often fails, and what leadership must do differently to embed it as a genuine performance tool.

The great paradox of modern risk management

Organisations today have more risk infrastructure than at any point in history: comprehensive policies, dedicated risk committees, extensive audit programmes, detailed risk registers, and layers of compliance review. Yet corporate failures, governance crises, strategic collapses, fraud scandals, and cyber incidents continue at an alarming pace.

Professor Mutenga identified this as the central paradox of modern risk management. The problem is not a shortage of frameworks. The problem is the gap between what policies state and what practice delivers.

The conclusion is direct: risk management failure is rarely a methodology problem. It is most often a leadership problem, a governance problem, and a culture problem.

The strategic purpose of risk management

The presentation argues that most organisations define risk management incorrectly. They treat it as a compliance function, a control mechanism, or a reporting obligation. This framing fundamentally limits its value.

Risk management exists for one purpose: to improve the quality of strategic decisions made under uncertainty. It should answer the questions that matter most to leaders:

- ✓ Which strategy should we pursue, and what assumptions does it rest on?
- ✓ What could destroy our business model or threaten our mandate?
- ✓ What could undermine long-term sustainability or public value delivery?
- ✓ How resilient is our organisation if our assumptions prove wrong?

Crucially, the presentation notes that while public and private institutions have different objectives, they share the same risk drivers. Economic volatility, technology disruption, climate risk, cyber threats, talent shortages, and reputational erosion threaten both sectors equally.

From risk registers to risk intelligence

One of the most important transitions called on by Prof. Mutenga is the shift from a compliance-oriented risk register to a decision-support risk intelligence system. The traditional approach produces a risk register that feeds into a risk report, which is reviewed by a risk committee, which produces a board report that is ultimately archived. Information flows but decisions do not change.

The modern approach treats risk data as raw material for analysis, which generates insights, which inform

decisions, which drive actions, which produce measurable performance improvement. The difference is not technological. It is a question of intent and leadership.

Emerging risks and operational resilience

He also draws attention to the risks not yet on most risk registers, grouping them across four domains:

- ✓ Technology risks: artificial intelligence disruption, deepfake fraud, and escalating cyber warfare,
- ✓ Economic risks: sovereign debt stress, inflation shocks, and currency instability,
- ✓ Environmental risks: climate change, water insecurity, and the challenges of energy transition,
- ✓ Societal risks: trust erosion, critical skills shortages, and political instability.

Alongside emerging risks, the presentation introduces the concept of operational resilience as the new frontier of risk management. The question is no longer only what could go wrong, but whether the organisation can survive when it does go wrong. This requires honest answers to questions about system failure continuity, leadership succession, cyber-attack recovery, and supply chain collapse.

Recommendations

Prof. Mutenga closed his session with a set of concrete recommendations for leaders and risk professionals seeking to move from policy to genuine practice:

- **Redefine the purpose:** position risk management as strategic decision support, not a compliance function. Every risk activity should be traceable to a better decision. Diagnose the culture Before investing in new frameworks or technology, assess honestly whether the organisation rewards or punishes transparency and escalation.
- **Operationalise risk appetite:** translate risk appetite statements into measurable thresholds, limits, and escalation triggers that are embedded in planning, budgeting, and approvals.
- **Close the governance gap:** boards must move beyond receiving risk reports to actively challenging executive assumptions, monitoring early warning signals, and demanding evidence that risk information changes decisions.
- **Build risk intelligence:** replace compliance-driven risk registers with analytical systems that generate actionable insights connected directly to strategic and operational decisions.
- **Address emerging risks early:** establish mechanisms to identify and assess risks not yet on the risk register, particularly those driven by technology disruption, climate, and societal change.
- **Measure what matters:** evaluate the risk function on the quality of decisions it influences and the surprises it prevents, not on the volume of documentation it produces.
- **Embed risk in every decision:** no major strategic, capital, procurement, or operational decision should proceed without a documented assessment of risk exposure, appetite alignment, and contingency planning.
-

Closing message

The presentation ends with a challenge that encapsulates its entire argument:

"The ultimate test of risk management is not whether risks are identified. It is whether the organisation changes its behaviour because of what it knows. Institutions fail not because they cannot see risk, but because they fail to act on it."

If every risk policy, framework, committee charter, and risk register disappeared tomorrow and decision-making would not change, the challenge is not the framework. The challenge is the culture. Transforming risk management from a documentation exercise into a genuine performance discipline requires leadership commitment, governance accountability, and a cultural environment in which transparency is valued and escalation is safe.

Building an ethics culture

Dr. Tawanda Collins Muzamwese, Chief Executive Officer, Toxiconsol Consultancy t/a African Sustainability Consultants

Corruption, bribery, and fraud remain among the most pressing threats to sustainable development and organisational integrity across the globe. In this presentation delivered at the convention, Dr. Tawanda Collins Muzamwese of African Sustainability Consultants examined the nature of ethics, the root causes and manifestations of unethical conduct in business, and outlined practical strategies for building a culture of integrity within institutions.

The presentation drew on global frameworks, including the Transparency International Corruption Perceptions Index and the ISO 37001 Anti-Bribery Management Systems standard, while contextualising the discussion within the Zimbabwean business environment.

Understanding ethics and ethical dilemmas

Ethics is defined as the integrity measure that evaluates values, norms, and rules forming the basis of individual and social relationships from a moral perspective (Smith and Smith, 2002). At its core, ethics distinguishes good from bad and right from wrong, prescribing what ought to be done and what must be avoided.

The presentation highlighted that ethical dilemmas are commonplace in business environments. Real-world scenarios from receiving erroneous bank payments and accepting high-value personal gifts to cross-board memberships and the misuse of client data illustrate just how frequently professionals are confronted with choices that test their integrity.

The global and local context of corruption

Corruption is one of the leading global problems affecting the development and progress of nations. It undermines economic productivity, causes significant financial losses, accelerates environmental degradation, and increases workplace safety incidents. Transparency International defines corruption as the use of public office for private gain.

The situation is particularly acute in developing countries, where corruption can be deep-rooted and institutionalised. In the Zimbabwean context, professionals and institutions continue to face significant ethics pressures across all sectors of the economy.

High-risk areas and common unethical practices

The presentation identified

several categories of unethical behaviour in banking and business, ranging from insider trading and bribery to discrimination and environmental harm. Key high-risk areas include:

- ✓ Recruitment and selection: where financial inducements are exchanged for favourable hiring outcomes,
- ✓ Procurement and contracting: prone to bribery in the awarding of contracts for goods and services,
- ✓ Regulation, permits, and inspections: where officials and companies may manipulate processes for personal gain,
- ✓ Conflict of interest: including undisclosed business interests, shareholding, personal relationships, and dual roles,
- ✓ Loan disbursement: where bank staff may be bribed to ease lending requirements,
- ✓ Shell and fictitious companies: used to siphon payments for services never rendered,
- ✓ Degree and certificate mills: fraudulent institutions issuing qualifications in exchange for money,
- ✓ Compensation fraud: employees falsely claiming workplace injuries that occurred elsewhere.

The impact of corruption on organisations includes loss of markets and credibility, financial losses, recruitment of incompetent practitioners, poor safety performance, environmental violations, and the worsening of climate change outcomes.

Recommendations and strategies

Dr. Muzamwese offered a comprehensive set of recommendations for organisations, regulators, and professional bodies:

Policy and regulatory frameworks

- ✓ Mainstreaming anti-corruption and anti-bribery provisions into national laws and sector-specific policies,
- ✓ Strengthening whistleblower protection systems and anonymous tip-off mechanisms,
- ✓ Ensuring merit-based recruitment of practitioners and inspectors, prioritising those with demonstrable integrity,
- ✓ Adopting open-contracting practices and strengthening internal procurement controls,

Institutional Governance

- ✓ Establishing and enforcing codes of conduct and anti-fraud policies within institutions
- ✓ Considering appropriate sanctions following investigations including criminal prosecution, civil action, disciplinary measures, and civil recovery of financial losses
- ✓ Strengthening internal audit functions and financial controls,
- ✓ Building internal capacity to reduce over-reliance on external contractors, which presents elevated corruption risk

ISO 37001 anti-bribery management system

A key recommendation was the adoption of ISO 37001, the international standard for Anti-Bribery Management Systems. This standard requires organisations to implement anti-bribery policies, conduct risk assessments, deliver training, assign responsibilities, establish financial controls, and create investigation mechanisms. It applies to bribery across public, private, and not-for-profit sectors, and covers both direct and indirect bribery. ISO 37001 can be implemented as a standalone system or integrated into an organisation's broader management framework.

Conclusion

As organisations grow and navigate increasingly complex environments, they will inevitably face more sophisticated corruption and bribery challenges. The responsibility for confronting these challenges does not rest with any single actor, it falls on regulators, companies, professionals, and individuals alike.

While global progress on corruption has been limited, the presentation concluded on a note of cautious optimism: with committed effort and coordinated action, it is possible to build a business environment in Zimbabwe and across Africa that is defined by ethics, transparency, and integrity.

Terence Murasiki, Director, ABMI Research Institute, South Africa

Strategic combined assurance: integrating governance, risk and compliance for organisational resilience

Organisations today face a risk environment shaped by constant change, compounding uncertainties, and the cascading effects of decisions across operations, service delivery, customer experience, and long-term sustainability. In this environment, a siloed, audit-centric view of assurance is no longer adequate. Strategic combined assurance as presented by at the convention by Terence Murasiki offers a structured, integrated response: one that draws on the full breadth of an organisation's assurance providers, coordinates their efforts, and delivers a consolidated picture of governance health to the governing authority.

This thought piece distils the key concepts, models, and implementation guidance from the ABMI strategic combined assurance course presented at the CRO Convention in Zimbabwe. It covers the foundational principles of combined assurance, the governance models, the three pillars of strategic assurance, implementation roles and lifecycle, and the maturity framework that measures an organisation's progress.

The interconnected nature of risk

Risk does not exist in isolation. Change generates uncertainty; uncertainty influences decisions; decisions shape operations; operations determine service quality; service quality drives customer outcomes; and customer outcomes ultimately define organisational performance, reputation, and sustainability. This interconnected chain means that a risk materialising at any one link can ripple across the entire organisation. Managing risk effectively therefore demands an equally integrated assurance response.

What is combined assurance?

The traditional view of assurance positioned auditors, internal and external, as the primary or sole providers of assurance to management and the board. Combined assurance challenges and expands this view. It recognises that organisations already have a wide variety of assurance providers embedded across their operations, and that the task is to coordinate, optimise, and integrate these efforts rather than duplicate them.

A key insight from the ABMI framework is that assurance is not exclusively positive. Negative findings confirming that something does not or will not work are equally valid and valuable forms of assurance. The purpose is to give decision-makers an accurate picture of organisational reality, whether favourable or not.

The practical case for combined assurance becomes most visible when the governing authority begins receiving different, misaligned reports containing redundant or conflicting information from various parts of the organisation. This fragmentation is a clear signal that assurance coordination is needed.

In summary, combined assurance:

- ✓ Considers a wider pool of assurance providers beyond traditionally recognised sources,
- ✓ Provides a means of integrating and optimising assurance efforts across the organisation,
- ✓ Enhances integration and enriches risk conversations at all levels,
- ✓ Gives the Governing Authority a consolidated view of how assurance is achieved across key strategic considerations and risks.

The King report simulated approach

The King Report model structures assurance across five levels, ascending from operational risk ownership to board-level oversight:

Line functions: risk owners' primary duty is to manage and report on risks in their operational areas,

Specialist functions: risk contributors are responsible for oversight, policy-setting, and specialist guidance (risk management, compliance, legal),

Internal assurance: these are independent internal assurance, e.g. internal audit,

External assurance: these are independent external assurance, e.g. external auditors,

Board & committees: responsible for oversight and stakeholder assurance, including the audit & risk committee.

Primary, secondary, and oversight lines

According to Terence, the ABMI framework further refines the assurance landscape into three practical categories:

Primary lines

Risk sponsors, risk owners, and line management who own and bear the first duty to manage risks in their areas. While not independent in the formal assurance sense, they provide highly reliable assurance because of their daily proximity to the risks involved.

Secondary lines

Operational and oversight committees, advisors, specialists, and both internal and external independent assurance providers. These actors are not directly responsible for managing risks but oversee their management. A clear delineation between these providers is recommended, as the type and extent of assurance they provide though related differs in important ways.

Oversight lines

The governing authority, its subcommittees, and independent committees. This layer plays both a leadership and a summative role, using the results of all combined assurance sources to provide relevant onward assurance to external stakeholders, most critically the shareholder.

Strategic combined assurance: the three pillars

Strategic combined assurance goes further than conventional risk-register-based assurance. It establishes a framework for responding to and providing assurance on any organisational matter regardless of when it is identified under three strategic pillars: governance, risk, and compliance.

Governance

The governance pillar encompasses five domains:

- ✓ Leadership, ethics & corporate citizenship: ethical leadership, values and culture, responsible corporate citizenship, and fit-and-proper requirements.
- ✓ Strategy, performance & performance reporting: strategic planning, implementation, performance management, and reporting,
- ✓ Governance structures, effectiveness & delegations: governing structure, governance calendar, board and committee effectiveness, and delegations' framework,
- ✓ Functional and effective control systems: risk and opportunity management,

technology and cyber, ESG and sustainability, projects, supply chain, and legislative compliance.
- ✓ Stakeholder management: planning, stakeholder interface, communications, reporting, and integrated disclosures.

Risk

The risk pillar covers:

- ✓ Strategic risks: risks to the achievement of long-term organisational objectives,
- ✓ Operational risks: day-to-day risks affecting service delivery and performance,
- ✓ Thematic risks: risks that are not yet formally specified in the risk register but carry organisational significance,
- ✓ Business continuity management: readiness to maintain critical operations under disruption,
- ✓ Specialised risks: sector- or context-specific risks requiring dedicated expertise.

Compliance

The compliance pillar addresses:

- ✓ Founding legislation: the primary statutes under which the organisation is established and governed,
- ✓ Sector regulations: regulatory requirements specific to the industry or sector,
- ✓ Technical standards and guidance material: applicable professional and technical standards,
- ✓ Compliance universe: the full inventory of applicable obligations, systematically managed and monitored.

Key recommendations

Drawing on the ABMI strategic combined assurance framework, the following recommendations are offered to governing authorities, chief risk officers, and assurance practitioners:

Broaden the definition of assurance

Move beyond the audit-centric view of assurance. Map all existing assurance providers across the organisation from operational management, specialist functions, committees, internal audit, and external audit and formally recognise their contributions within a combined assurance framework. Both positive confirmations and negative findings are valuable.

Formalise the combined assurance framework and plan

The absence of a formal framework is the most common barrier to effective combined assurance. Organisations should establish a board-approved combined assurance framework and an annually reviewed combined assurance plan. These documents should describe the assurance universe, assign assurance providers to each area, and define the extent and reliability required.

Adopt the three pillars approach

Structure combined assurance plans around the three strategic pillars of Governance, Risk, and Compliance rather than solely around the risk register. This broader scope ensures that thematic risks, governance indicators, and compliance obligations receive appropriate assurance coverage, even when they have not yet been formally documented.

Reposition internal audit as the assurance of assurance

Internal audit should shift from being the primary assurance provider to being the function that assures the effectiveness of the combined assurance model itself. Audit planning should encompass the entire combined assurance universe, with coordination extending to all other assurance providers.

Conclusion

The interconnected nature of risk demands an integrated response. Combined assurance is that response.

Strategic combined assurance represents a maturation of organisational governance from reactive, audit-focused compliance to a proactive, integrated system that listens to all its assurance voices and presents a coherent, credible picture of organisational health to its governing authority.

The ABMI framework, as presented by Terence Murasiki, offers a practical and deeply considered architecture for this journey. It acknowledges the diversity of assurance sources that already exist within organisations, provides the structural tools to coordinate and optimise them, and gives boards and audit committees the consolidated intelligence they need to discharge their oversight responsibilities with confidence.

The death of the reporter: exceptional risk leadership in 2031

What the next five years demand from risk leaders who want to matter

Socrates Mhlanga, CEO, Signal Radar Group

In a keynote address titled: the death of the reporter, Socrates Mhlanga issues a sharp challenge to the risk management profession: technical competence is no longer the differentiator. By 2031, risk analysis will be a commodity available to anyone with the right tools and data. The real battleground for value will be decision architecture: the ability to shape consequential outcomes before they ever reach the formal agenda.

This post-convention article distils the key frameworks and insights from that address covering the compliance trap, the invisible architecture of influence, the SIGNAL and RADAR systems, the evolution toward the strategic intelligence officer, and recommendations for risk leaders who want to remain relevant and impactful in the years ahead.

The 2031 horizon: strategic redefinition

The five-year horizon to 2031 is not a story of incremental evolution, it is a structural redefinition of where value is created in the risk profession. Artificial intelligence, automation, and an explosion of organisational data are rapidly commoditising what was once a differentiating capability. Any well-resourced team can now produce technically sophisticated risk outputs.

The consequence is stark: the organisations that benefit most from risk management by 2031 will not be those with the best models. They will be those with risk leaders who understand that the war is not won in the data it is won in the decision room. The capability gap ahead is not technical competence. It is decision architecture.

"Exceptional leadership will be defined by the ability to shape important outcomes before they reach the formal agenda."

The compliance trap: floor, not ceiling

One of the address's most important distinctions is between the floor and the ceiling of risk management. Regulatory compliance is the floor, the minimum standard required to operate. It is not, and must never be treated as, the ceiling of ambition. A risk function that optimises for compliance has, by definition, defined its ambition downward.

The label the function earns in the boardroom: the "No Department" or the "Compliance Monitor" is a natural consequence of this identity. Exceptional risk leadership, by contrast, uses compliance as a baseline from which strategic influence is built. The shift in question is not: Are we compliant? It is: What decisions can we shape from here?

From CRO to strategic intelligence officer

One of the address's most provocative arguments is that the title Chief Risk Officer is becoming a misnomer. It carries the institutional baggage of the "No Department" a label that, whether fairly earned or not, limits the function's ability to lead. Mhlanga proposes a fundamental identity evolution: from CRO to strategic intelligence officer (SIO).

This is not a cosmetic rebrand. It is a repositioning of what the risk function is for, who it serves, and how it creates value. The SIO operates across three pillars.

The behavioural architect (SIGNAL)

According to Socrates the SIO understands the human and political physics of the boardroom not as a peripheral skill, but as a primary one. The ability to read power, navigate influence, and time interventions precisely is what separates the risk leader who shapes strategy from the one who merely reports on it after the fact.

The narrative engineer (RADAR)

The SIO is a master of translation. Raw data and technical analysis do not move decision-makers, stories that connect risk to what decision-makers care about do. The narrative engineer uses the RADAR architecture to ensure every output is designed to activate rather than merely inform.

The strategic peer

Socrates also emphasized that, the SIO does not sit in the corner of the boardroom waiting for the "Risk Item" on the agenda. The SIO is present throughout the strategic conversation as a peer contributor, adding value to every item, not only those formally labelled as risk. This demands that the risk leader develops strategic relationships, business fluency, and the credibility that flows from consistently connecting risk insight to real business outcomes.

Redefining the measure of a risk function

The keynot address issues a fundamental challenge to how risk functions evaluate their own performance. Conventional metrics: quality of the risk register, completeness of processes, audit ratings measure the wrong thing. They reward internal activity rather than external impact.

"The measure of a risk function is not the quality of its risk register or processes. It is about how well problems are solved and the quality of the decisions made in its presence."

This reframing has profound implications. It means the risk function's success metric is observable in the boardroom and the strategy room, not in the risk department's own documentation. Did decisions improve? Were problems solved more effectively? Was the organisation better navigated because of risk's presence? These are the questions that matter.

The keynote address by Socrates delivers its central diagnosis with equal sharpness: most organisations do not have a risk problem. They have a decision problem. The risk function that recognises this and repositions itself accordingly becomes genuinely indispensable.

Recommendations for risk leaders

The following recommendations are drawn directly from the address's frameworks. They are intended for CROs, risk leaders, and governing authorities who want to build the risk function that will matter in 2031:

Diagnose your decision influence

Socrates submitted that, before anything else, conduct an honest audit of how much genuine influence the risk function currently exerts on strategic decisions. Not on risk registers or compliance ratings but on actual organisational decisions. Map the last ten significant decisions and ask: was risk's input decisive, marginal, or absent? The answer will reveal the real gap.

Escape the compliance ceiling

According to Socrates it is time to reposition the risk function's stated purpose; explicitly, in conversation with the governing authority and executive leadership from compliance monitoring to strategic intelligence. Without this reframing at the top, the function will remain confined to its compliance floor regardless of the talent it possesses.

Build all six SIGNAL competencies

Invest in developing shadow drivers' awareness, influence pathway mapping, governing constraints analysis, now or never timing, alignment narrative fluency, and lock-in signal detection. These are learnable skills. Embed them in the professional development framework for every member of the risk team, not only the most senior.

Transition from mechanic to architect

It is crucial to make a deliberate, explicit choice about the professional identity the risk function embodies. Mechanics will increasingly be replaced by technology. Architects who design decision landscapes and map hidden drivers will be irreplaceable. Make the transition visible in job descriptions, performance frameworks, hiring criteria, and team culture.

Master the timing of influence

Developing the situational awareness needed to sense when decision windows open is foundational for risk executives. The risk leader who brings the right insight to meetings too late has delivered no value. Build processes for continuous intelligence gathering informal conversations, pre-meeting engagement, and horizon scanning to ensure risk intelligence reaches decision-makers while it can still change outcomes.

Become fluent in executive language

Risk leaders who communicate exclusively in risk management vocabulary will be filtered out. Develop fluency in the language of the executive agenda: strategic objectives, competitive positioning, capital allocation, stakeholder value, and organisational purpose. Translate every risk insight into this language before it reaches the boardroom.

Embrace the strategic intelligence officer identity

Whether or not the title changes, the risk leader who operates simultaneously as a behavioural architect, narrative engineer, and strategic peer will be the one whose function is valued, resourced, and genuinely heard. Begin the transition now, five years ahead of the horizon rather than scrambling to catch up when the profession has already moved on.

Conclusion

"If you don't filter for strategic relevance, the executive will filter you out entirely."

Socrates Mhlanga's address is not a comfortable one for the risk profession. It does not celebrate how far the discipline has come. It challenges practitioners to acknowledge that the ground is shifting and that the skills and identities that earned credibility in the past will not be sufficient to create value in 2031.

The death of the reporter is not a threat; it is an invitation. An invitation to become the architect, the narrative engineer, the strategic peer, and ultimately the strategic intelligence officer that organisations will desperately need as the complexity of their decision environments continues to compound.

The risk leaders who answer that invitation, who invest in decision intelligence, master the RADAR output architecture, escape the compliance ceiling, and build genuine strategic influence will define what exceptional risk leadership looks like in the next five years.

Efficient risk-based capital allocation: optimising product and business unit performance

A deep dive into synthetic actuarial models and enterprise risk management

Tafadzwa Chiduza, Managing Director, Claxon Actuaries

Capital allocation, deciding how much resource to deploy across each business unit, product line, or line of business is one of the most consequential decisions a board and executive team make. Yet most organisations allocate capital on the basis of revenue, assets, or historical precedent, with little regard for the risk actually consumed in generating returns.

Presented by Tafadzwa Chiduza at the convention, this paper makes the case for risk-based capital allocation: a disciplined, methodologically rigorous approach that measures each unit's contribution to enterprise risk and prices capital accordingly. It covers the performance measurement paradox, five capital allocation methodologies, two detailed case studies, a synthetic ERM model architecture, and a practical four-stage implementation roadmap.

The performance measurement paradox

EBITDA and net profit tell you what you earned. Risk-adjusted metrics tell you what you earned relative to what you risked to earn it. Only the latter can drive genuinely optimal capital allocation yet most Boards still govern by the former.

Capital allocation methodologies

Five methodologies are

available, ranging from operationally simple to theoretically rigorous. The right choice depends on an organisation's data maturity, modelling capability, and strategic ambition:

The synthetic actuarial ERM model

The presentation introduces a five-module stochastic ERM architecture that enables full enterprise risk intelligence for both capital allocation and strategic decision-making:

- ✓ Economic scenario generator (ESG): stochastic scenarios for inflation, FX rates, equity returns, and proxy risk-free rates across 1–10 year horizons,
- ✓ Asset model: projects market value of the investment portfolio under each ESG scenario, calibrated to ZICARP market risk shocks,
- ✓ Liability model: projects best estimate liabilities and risk margins across life and non-life blocks under economic scenarios,
- ✓ Dependency / copula model: captures cross-risk correlation, with t-copula (fat tails) preferred over Gaussian copula to reflect tail dependence in stress scenarios,
- ✓ Capital aggregation & performance engine: computes aggregate balance sheet, ZICARP SCR, RORAC, EVA, and CSM coverage by business unit across all simulated scenarios.

For Zimbabwe specifically, the model requires calibration adaptations: bayesian credibility blending of sparse local data with SA/regional benchmarks; a jump-diffusion process for currency risk; and a scenario library including hyperinflationary episodes and USD liquidity crises.

Recommendations

The presentation closes with concrete recommendations for insurers, conglomerates, and their boards:

Audit current performance metrics: initiate a phased transition from EBITDA-only reporting to RORAC-based decision-making at Board and executive level. Ask: for every dollar of capital deployed, how much risk-adjusted return did we earn?

Build on ZICARP: use the SCR by risk module and the inter-risk correlation matrices (TS 6.1, 6.2, 6.3) as ready-made tools for a Stage 2 capital allocation framework. The regulatory infrastructure already exists use it,

Integrate IFRS 17 and ZICARP: use IFRS 17 risk adjustments as proxies for ZICARP risk margins and develop a unified CSM by product group alongside allocated SCR. The two frameworks are structurally complementary,

Implement risk-adjusted incentives: link at least a portion of senior management compensation to RORAC or EVA. This is the single most powerful lever for embedding capital efficiency into daily underwriting decisions,

Plan now for internal model development: begin the groundwork for a synthetic ERM model even if regulatory recognition of internal models is years away. The economic capital framework built today will become the regulatory framework of tomorrow.

Conclusion

"The insurance industry exists to provide certainty to the uncertain. It is time it applied the same rigour to its own capital allocation that it applies to the risks of its policyholders."

Risk-based capital allocation is not an academic exercise, it is the difference between an organisation that grows strategically and one that accumulates risk in ways that are invisible until a tail event exposes the true cost of years of suboptimal deployment.

The frameworks presented are available to Zimbabwean institutions today. The tools exist. The regulatory scaffolding, through ZICARP, is in place. What remains is the commitment to build the capability and governance structures that make capital allocation a living strategic discipline rather than an annual compliance task.


aim
irmic
INSURANCE &RISK MANAGEMENT INFORMATION CENTRE
Chief Risk Officers Convention


©GOLDENLIFEVISUALS


Diagnose your decision
Influence


irmic
INSURANCE &RISK MANAGEMENT INFORMATION CENTRE

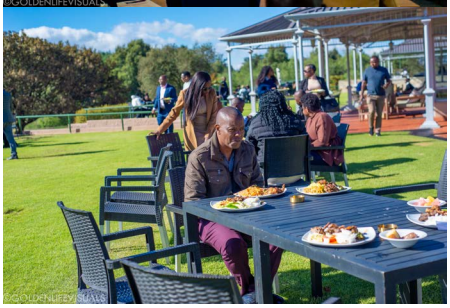

©GOLDENLIFEVISUALS


©GOLDENLIFEVISUALS


©GOLDENLIFEVISUALS


©GOLDENLIFEVISUALS


©GOLDENLIFEVISUALS


©GOLDENLIFEVISUALS


©GOLDENLIFEVISUALS



aim
irmic
Chief Risk Officers Convention

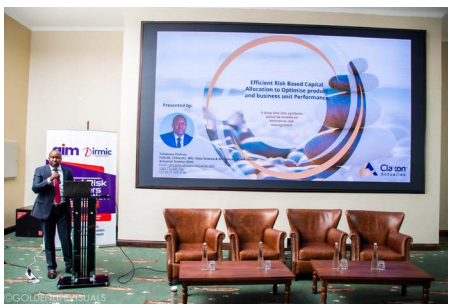

aim
irmic









aim
AFRICA INSURANCE MAGAZINE

Efficient Risk Based Capital Allocation to Optimize product and business unit Performance
aim
irmic



Ready to Transitio