Deloitte.

Modernising the three lines of defence model

An internal audit perspective

Introduction

Businesses are continuing to evolve out of necessity, responding to an onslaught of disruption, new business models, and technology. This continuous change affects business operations at all levels, with customers demanding real-time interactions, regulators applying increasing levels of scrutiny, and governance stakeholders requiring assurance in this complex and dynamic risk environment. The result has exposed weaknesses in the traditional three lines of defence (3LOD) framework.

In its current form, is the 3LOD framework still relevant and efficient? According to a Gartner Corporate Executive Board survey released in November 2018, 66 percent of the CEOs surveyed said that business models will continue to change dramatically in the next three years, and business leaders are focused on aggressively seeking out opportunities to innovate within the rapidly changing and increasing landscape of risks. As the risk landscape becomes more complex and fast-moving, it is critical for organisations to identify and respond to emerging risk events quickly and effectively. We believe that internal audit (IA) should play a key role in this evolution.

3LOD: Current-state challenges

Different groups within organisations play a distinct role within the 3LOD, from business units to compliance, audit, and other risk management personnel. Management (process owners) is the first line, with primary responsibility to own and manage risks associated with day-to-day operational activities. Other accountabilities assumed by the first line include design, operation, and implementation of controls. While the first line is considered to be at the forefront of identifying emerging risks in the daily operation of the business, the second-line function enables this by providing compliance and oversight in the form of frameworks, policies, tools, and techniques to support risk and compliance management.

Finally, the third-line function provides objective and independent assurance for internal and external stakeholders. While one of the third line's key responsibilities is to assess whether the first- and second-line functions are operating effectively, it is charged with the duty of reporting to management, the board, and audit committee in addition to providing assurance to regulators and external auditors that the control culture across the organisation is effective in its design and operation. While the 3LOD framework is widely acknowledged and understood by a range of industries as the governance model for risk, its implementation varies in form and maturity across the spectrum. Traditionally, one of the roles of the IA function is to provide assurance while maintaining objectivity and independence; however, its mandate should continue to evolve as the need to adapt to a business-focused, technology- driven, advisory mindset is amplified (figure 1).

Having originated in the financial services sector in the late 1990s and early 2000s, 3LOD has been widely adopted across all industries, albeit to varying degrees, since the Institute of Internal Auditors (IIA) formally adopted the model in 2013 and revisited in 2023, being now called the Three Lines Model. The level of adoption broadly correlates to the strength of regulatory pressure. In most industries, smaller or emerging organisations typically lack the three defined and distinct lines, with overlapping first- and second-line roles or overlapping second- and third line functions, whereas heavily regulated industries, such as financial services or pharmaceuticals, have established formalised clear lines of defence. Regardless of how mature and integrated the 3LOD model is within organisations, there are a number of challenges that limit its effectiveness.

Figure 1: The changing face of assurance and compliance monitoring

- **Early-stage adoption** – In the early stages of the 3LOD framework, management does not have a strong awareness or ownership of risk and controls. There may be a risk function in place, but often its role is to facilitate the identification and monitoring of risks without insight or challenge by IA. Depending on the industry and sector, regulatory compliance risks are absorbed into both risk and IA functions, with specialist teams existing in pockets or one-off "silos" not seen as assurance functions (for example, health and safety in construction firms or clinical governance in the health care industry) nor well integrated within a broader risk management program. In smaller firms, given the similar risk and control skill sets, the IA and risk functions are seen crossing the boundaries between the second and third lines, causing inefficiencies and duplication.

- **Established lines of defence** – As the 3LOD becomes established, the focus on stakeholder management, developing internal capabilities, and delivering the assurance activities in the second-line functions often creates a silo mentality, leading to a lack of coordination, duplication of risk areas, gaps, and misaligned or conflicting assurance opinions. Where these positions become entrenched, the third line is often perceived as combative, reactionary, and retrospective in its approach. This combination has led to an ineffective 3LOD model, where the board are receiving conflicting and disjointed points of view of its key risks. This challenge was highlighted in Deloitte's 2018 CAE Global survey, where respondents cited improvements in coordination within the 3LOD as an important business imperative.

- **Maturing lines of defence** – In the face of increasing regulatory pressure, as well as businesses recognising the opportunity to become more efficient and effective, we are seeing the strengthening of all three lines of defence, being driven from the board focus on emerging risks and core control disciplines. An example of this is in Malta, where financial services regulators are increasing the personal accountability of senior managers (including executive and nonexecutive directors) over the control environment. The result has been felt across all 3LOD:

  – The first line taking an active role in the management of risk for its area; some are starting to embed first-line monitoring of controls (in larger institutions, this has led to first-line assurance teams – "Line 1b").

  – Risk functions are increasingly forward-looking in their assessments of emerging risks, scanning the horizon, using key risk indicators to highlight potential control failures and working with management to improve the design of controls.

  – In addition to advising management on new regulatory risks and designing corresponding policies, compliance functions are undertaking increased regulatory monitoring reviews, which include regulatory controls testing. This is aligned with Deloitte's point of view, where the first and second lines take on greater ownership of their responsibilities as part of "assurance by design" and "automated core assurance."

  – This has left IA functions undertaking risk-based assurance reviews over the same risk areas as the second line, increasingly with a very similar assurance skill set, leading to a duplication of assurance activities between the 3LOD.

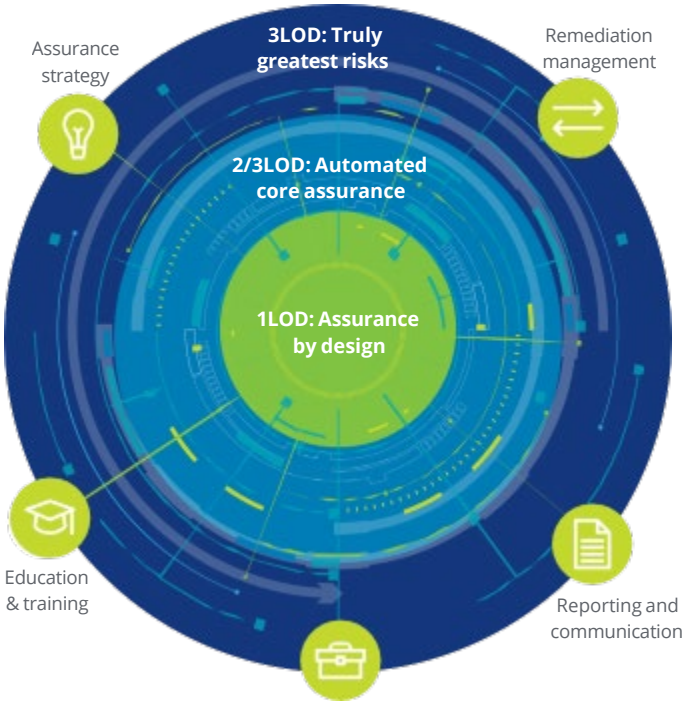
While these actionable and strategic steps are oriented towards an evolution in the 3LOD, there have been several negative side effects for more mature 3LOD models. The first line can have audit fatigue due to duplicative testing from both second and third lines, resulting in less time to focus on the business at hand. There are also cases where the over-fitting or over-strengthening of the second line has resulted in issues because the first line stops performing activities, believing they have responsibility of the second line. In times of crisis, many organisations fall into the trap of overreaction, whereby additional activities are added to the portfolio for the second and third lines. In such situations, the third line is best positioned to help their organisations avoid knee-jerk reactions and help draft a measured response that is risk-focused, pragmatic, and practical.

3LOD: Future state and opportunities

IA functions with the strongest impact in their organisations are those which are adapting to change; collaborating; and making investments in digital assets, analytics, and automation. New technologies have created an opportunity to enable a variety of techniques to improve efficiency and insight from assurance activities, including 100 percent assurance coverage (rather than sampling), automation of assurance tasks, and real-time insight into emerging risks via data-led, continuous monitoring. This creates an opportunity for IA and its future role.

To take advantage of these changes and disruptions, auditors need to rethink their role by adapting to and embracing change, enabling the IA function to become more agile, nimble, and forward-looking, thus driving change through the 3LOD (figure 2).

Figure 2: Tomorrow's three lines of defence



Due to its stature in an organisation, IA is in a great position to assist with integrating assurance activities, particularly in helping the first line take greater ownership of controls and embedding means of self-assurance. Combined with enhanced technology, this would enable modernisation by the second line to allow for real-time monitoring. Although IA cannot place full reliance on the work performed by the first and second lines, it can leverage the monitoring results, perform agile testing of controls, and provide assurance and advice on the "truly greatest risks." To do this, IA will elevate itself to become a more strategic and holistic assurance provider, and risk advisor, collaborating with the other lines and having a seat at the table, a clear line of sight earlier in the process.

For IA to be perceived as protecting, building, and preserving value, it needs to truly assure, advise, and anticipate and accelerate. The IA of the future will play an active role in educating stakeholders and sharing tools, insights, and knowledge. Effective IA functions with a dynamic and forward-looking mindset are likely to be viewed positively by key stakeholders. While the maturity of IA groups within individual organisations will vary, the key is to start identifying current inefficiencies in an organisation's 3LOD model and to encourage innovation with meaningful, strategic steps. Innovation should extend beyond technology, including coordination, communication, audit and risk assessment methodology, and elevating engagement connection with first- and second-line stakeholders. With a renewed vision, IA would be in a better position to strengthen its impact and mobilise itself for future challenges and opportunities.

The road ahead: What can CAEs and their organisations do in response to these challenges?

There are many ways the CAEs and their functions can respond to these challenges. Let's explore some considerations to jump-start the thinking around these challenges.

There are many possibilities that CAEs can consider in looking at the 3LOD model. Since IA commonly focuses on providing assurance on core processes, financial reporting controls, and the most relevant organisational risks, the ability to do more and provide additional coverage required in the future is limited. IA should focus its efforts on shifting ownership of certain elements of risk management to the first and second lines through education and awareness-building, highlighting the value and efficiencies that can be achieved. This can only help, and assurance, coverage, and clarity will increase. By leveraging digital assets and innovative methods, IA and risk management could automate processes previously covered manually, or not covered at all by the IA plan. IA should increase its participation in coordinating and designing processes that could help management and the second line take ownership of these activities, while addressing business risks and minimising the audit fatigue due to the efforts of second and third line.

This model is centred on common methodologies and tools, education, and training, as well as integrated reporting and communications. Of course, this can be achieved through the use of technology. In this optimised model, we see the opportunity for real-time assurance, a lower cost structure, and a better span of control across the organisation. IA can take a leading role in this effort. IA could create opportunities to help implement assurance activities into controls as they are designed. This approach is called "assurance by design." There is a distinct possibility to automate and create workflows that many of the typical second-line activities and some first-line compliance activities can leverage ("automated core assurance"). This would allow IA (third line) to focus on the greatest risks while creating much-needed capacity.

Looking specifically at IA, this framework represents a traditional view of not only fulfilling IA's core assurance responsibilities, but also the need to advise on key risks and help the business anticipate and measure risk. These are the critical elements of the internal audit of the future. There are a number of enablers and accelerators that can be used to achieve these objectives, including:

- Talent; building the workforce of the future; and considering what type of work needs to get done, who is going to do the work, and where the work is going to be performed
- Developing new, dynamic, and innovative approaches for assessing risk, how audits are performed and delivered, and reporting results
- Utilising and integrating digital assets into business as usual

Figure 3: Internal Audit of the future | Inside an innovative mindset

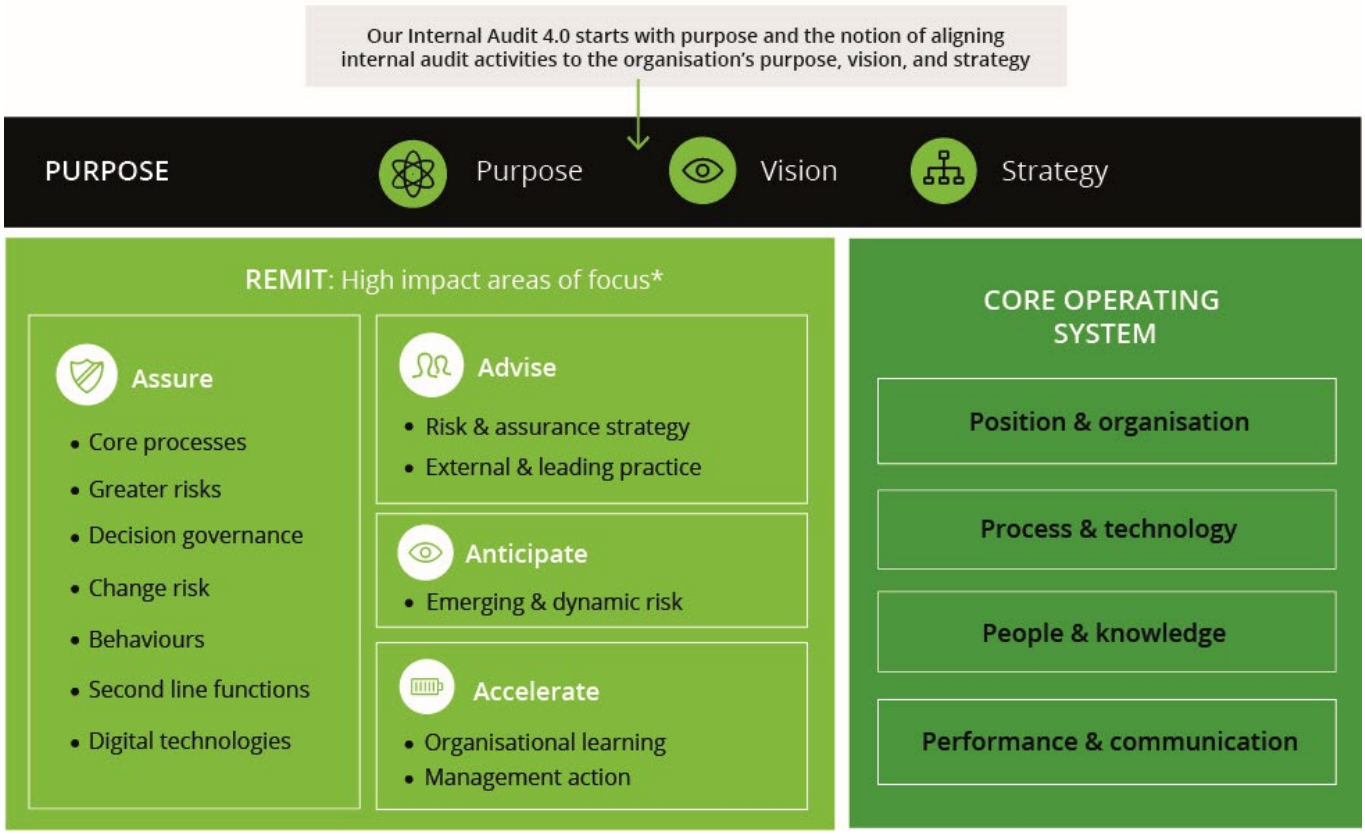
In addition, the CAE should focus on the IA function in considering the importance of developing an innovative mindset. This is critical for organisations as they look to the future and develop forward- looking approaches for managing risk. The CAE should think about and define the skills and attributes that drive innovative behaviour. It is interesting that the skills and characteristics in many ways are the same for what an innovative risk and control professional will need to be impactful in the future (figure 3).

The future is now

As we see, IA is at the cusp of innumerable possibilities to collaborate with the other lines, develop roadmaps, and help lead improvement to optimise governance across the organisation. This is a great opportunity for the profession to redefine itself and cement its position as not only a provider of assurance, but also a function that assures, advises, and anticipates. Our point of view represents fulfilling assurance responsibilities with combined core assurance spread throughout the lines of defence, rather than just through IA, but also includes the imminent need for IA to advise the business with anticipation and measurement of risk. These are critical elements of the IA of the future (figure 4 and Internal Audit 4.0), which will create capacity for IA to focus on the truly most relevant and impactful risks to the organisation.

Figure 4. The future—Internal Audit 4.0

Assure. Advise. Anticipate. Accelerate. The Internal Audit 4.0 framework is designed to help internal audit departments lead in providing core assurance, advising the business, and helping the business anticipate risk and accelerate organisational learning.



*The "Four A's" are the heart of our AI methodology. They will support the organisation to accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes.

Contacts

Ian Coppini
Risk Advisory Leader
Deloitte Malta
icoppini@deloitte.com.mt

Rafael Moreira
Senior Manager - Rislk Advisory
Deloitte Malta
ramoreira@deloitte.com.mt

Deloitte Place,
Triq L-Intornjatur, Zone 3,
Central Business District,
Birkirkara CBD 3050,
Malta

Tel: +356 2343 2000
info@deloitte.com.mt
www.deloitte.com/mt