Deloitte.

Three Lines of Defense

Time to rethink and reframe the model

Luxembourg

Executive Summary

The world has changed. Exponential advancements in technology, combined with unpredictable economic and geopolitical events have created an environment of relentless volatility, uncertainty, complexity, and ambiguity (VUCA). In today's environment, fortunes are created and lost even more quickly.

Financial services organisations can no longer afford to operate as if the world is static. And the role of Risk Management can no longer act as a separate and reactive function.

Risk Management must be dynamic and capable of anticipating and adapting to VUCA events. But it must do so within a strict and tightening regulatory framework to promote and enable a trusted, safe, sound and resilient organisation that meets the demands of its customers, shareholders and regulators. No small task.

Given the speed, complexity and severity of risks, for organisations to achieve a fair share of profits, they must be more focused, clearly defining and acting on a strategic intent of where to play and how to win.

They must create an ecosystem where taking on risk is seen as an opportunity. The Risk function must extend its capabilities to cut through all lines of defense, and any silos within the firm's organisational structure, and develop risk sensing and shaping capabilities that cut across the organisation in a risk intelligent manner.

Today's risk function must be:

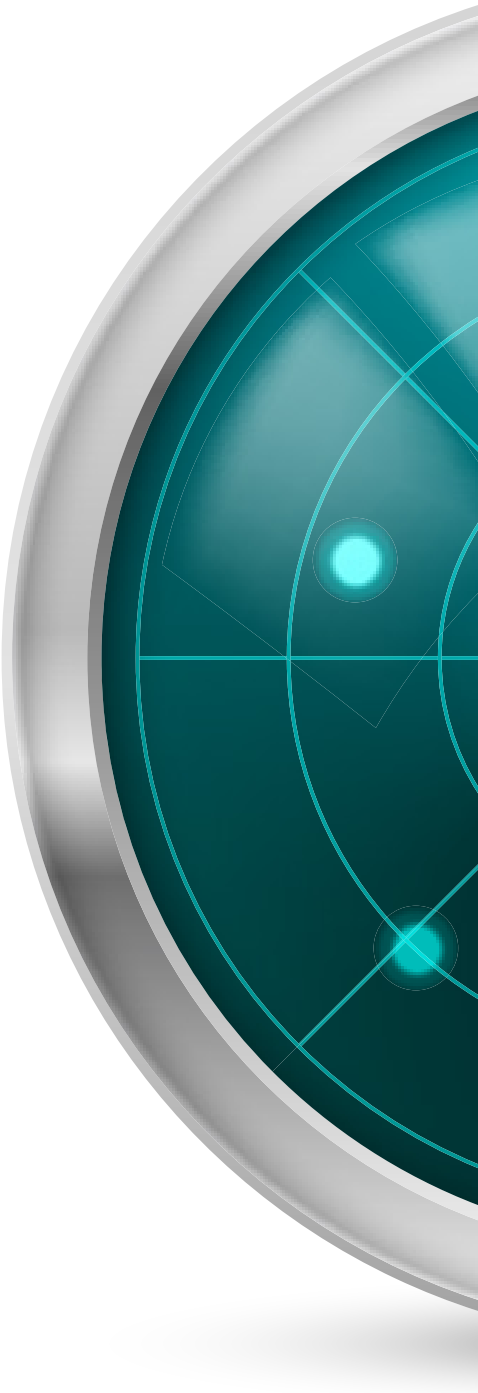
- **People enabled:** In order to avoid just another tilt of the risk model, the organisation should map out the desired end state and identify the right people, the right capabilities, the right tools and the information and incentives necessary.
- **Tech enabled:** The risk function must explore and engage in technology and innovation which are on the verge of enabling the improvement of business performance through accessing better data to make decisions and increase productivity. It must utilise RegTech powered by robotics, machine learning, cognitive and predictive analytics, artificial intelligence, and other new supporting technologies.

In addition to these demands is the need to reshape business models, to rethink how best to care for customers, protect them and increase the speed to serve them, as well as be streamlined, agile and flexible, and reduce human error.

By any measures of cost, of efficiency and effectiveness in reducing risk, and the twin impacts on customer experience and empowered responsible staff members, there are strong incentives for financial services organisations to rethink and reframe how they approach risk management.

The 'Three Lines of Defence' model is central to how most organisations currently approach risk management.

Across the world we believe this 1990s model is failing to live up to its promise.



Our own research identified that across all sectors, the growth in compliance workers had largely offset the productivity gain created by the reduction in back-office workers.

The technology dividend was being spent on increased compliance related staff. As ambiguity takes hold, coupled with increased community expectations and regulation across the global banking industry, the current risk operating models that were built around divisional organisational structure or risk disciplines, are being challenged to deliver the outcomes expected in the market.

"The growth in compliance workers largely offset the productivity gain created by the reduction in back-office workers."

The reality is that communication between silos has created layers of bureaucracy that slow the process.

A truly collaborative, connected, 'risk-aware' organisation, is yet to be hardwired into organisational design.

It is not that the fundamental principles underlying the 'Three Lines of Defence' are not sound – they absolutely are.

But the evolution of complex risk methodologies, frameworks and systems, has meant that responsibility for risk management activities are in danger of being diluted across multiple parties.

We believe this means that the Three Lines of Defence model requires a rethink and 'reframe'.

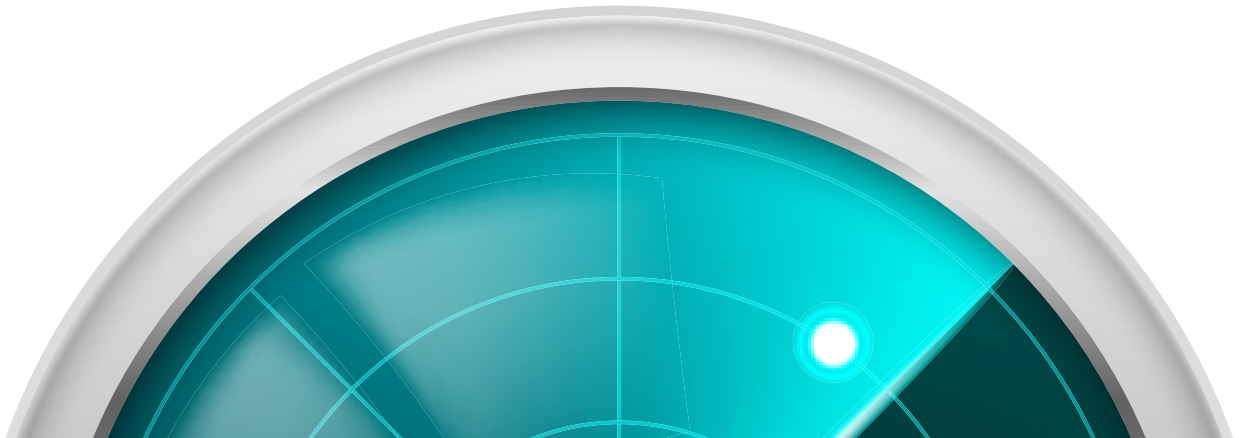
The increasingly difficult issue of ownership of conduct and managing conduct risk that organisations are also grappling with, and the need for risk and control to be adaptive and nimble right across the end-to-end value chain, adds to our thinking.

In this paper we put forward an approach to refresh the current model, particularly pertinent should your answer to the simple questions below be 'no'.

- Do Line 1 risk staff members have sufficient understanding of business processes to adequately understand the business impact of issues and incidents?
- Do business managers really take accountability for risk? Or does having a multitude of people in named Line 1 'risk' roles – people disassociated from day to day management of the business – allow business management to pass on responsibility for risk management?
- Does the business understand how key risks are being managed and where these key controls are located across the value chain?
- Does the business have an effective and integrated assurance plan across all three lines? There is often repetitive and inefficient review duplication, and a perception among business stakeholders that we have 'checkers checking the checkers'.

By reframing the approach from focussing on what 'could go wrong' to what 'needs to go right' we believe organisations will be able to go a long way towards reducing the inefficiency brought about by complexity and ambiguity, and be better able to meet the contemporary and increasingly demanding needs of customer, regulator and shareholder.

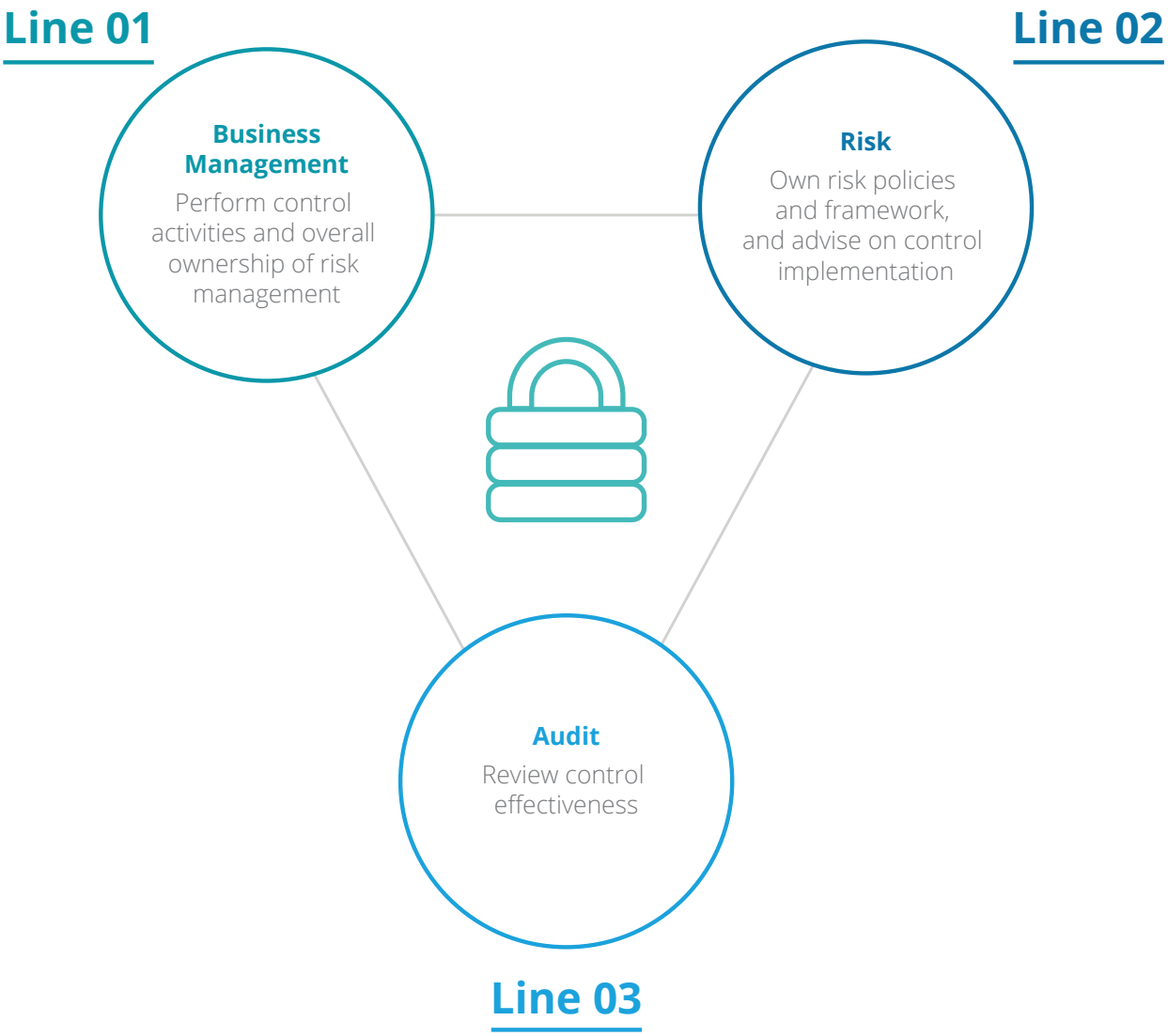
"By focusing on what must go right rather than everything that can go wrong, will ensure controls will be better designed to meet key business objectives."



How has the Three Lines of Defence model evolved?

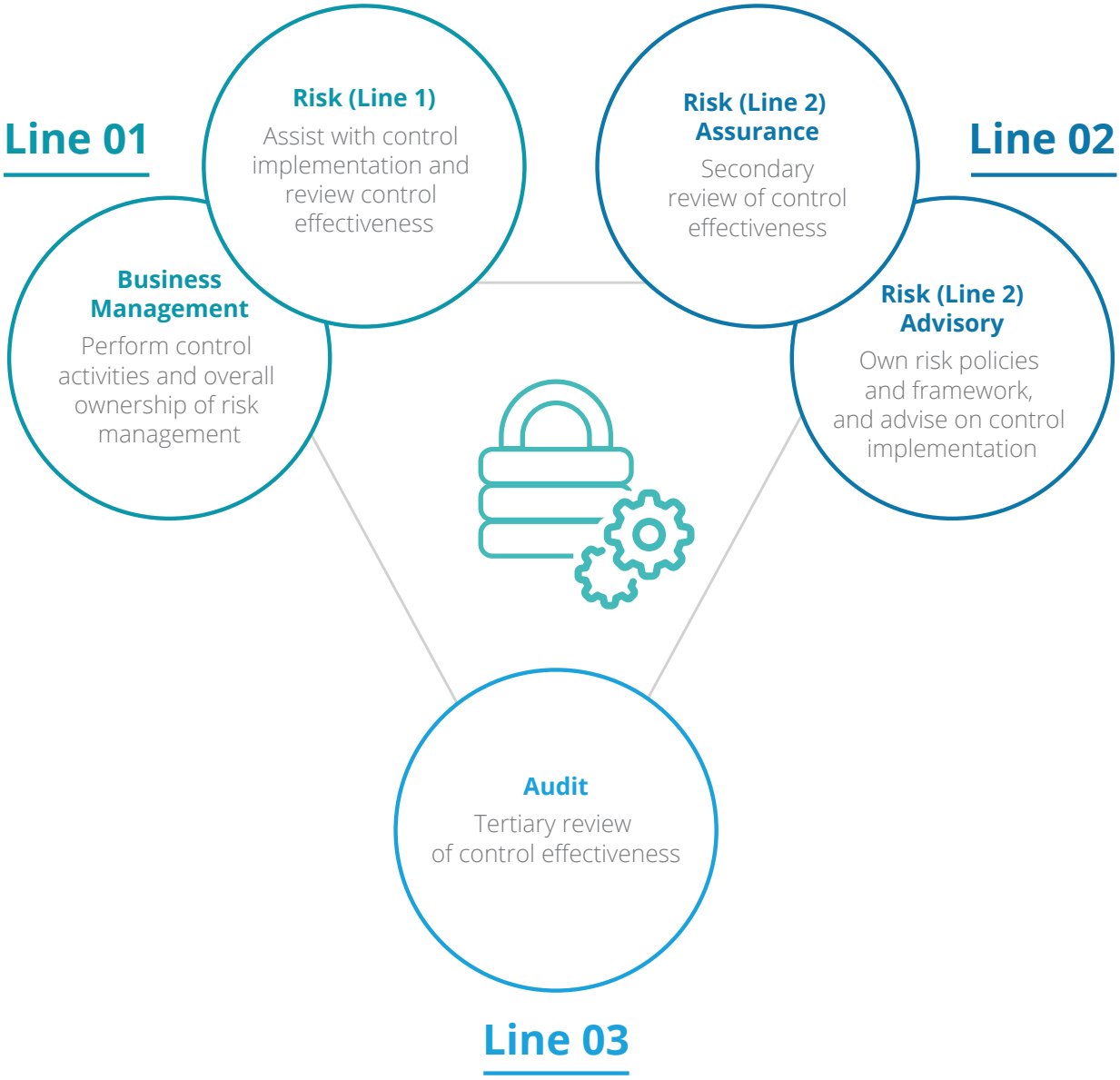
The original model was built on the principle of separating responsibilities for executing, advising and reviewing control activities.

This model usually looked like this:



This has changed over time. Responsibility for risk management activities in a typical bank is now distributed across multiple roles and functions.

The model which has evolved often looks more like this (simplified for clarity):



In this model the risk function has been split into Line 1 and Line 2 elements, and the Line 2 Risk function has been divided into Assurance and Advisory arms. In addition, some firms employ Line 1 assurance functions.

Our research across banks indicates there is no universal model and many X-trends. For each bank integrating risk and compliance functions to take advantage of operational synergies, there is another bank separating risk and compliance to give each a distinct voice at the executive and Board tables.

For each bank moving staff from the 2nd line into the 1st line there is another bank which is re-thinking the role of risk professionals in the 1st line.

The one common sentiment is frustration that the banks' current investment in risk and compliance is not delivering the intended results. In many banks the effectiveness of risk has weakened, even as the resources devoted to it have increased.

In this environment we think the time is right for a re-think.

Is the current model effective?

If the answer to the questions in the Executive Summary was 'no', despite the evolution of the three lines, we may conclude that it has failed to deliver an appropriate return on the significant investment. This is also reflected in risk outcomes. If risk is managed well most issues should be detected immediately by the 1st line.

How can we improve?

Banks need to reduce the complexity of risk management by revisiting the original Three Lines of Defence model.

We suggest a realignment of the business (Line 1) around (i) identifying and assessing the multi-risk exposure it creates, and (ii) the design and effectiveness of controls against the end-to-end value chain and processes, rather than against risk functions e.g. Operational Risk or Credit Risk.

A number of global financial services organisations have created 1st line control owners connected to their key processes – i.e. aligned to what must go right.

These control owners are senior appointees and are peers of the business leaders. Their focus on controls mean they are oriented toward operational management rather than the risk team, and they often report through to the business unit Chief Operating Officer.

This cohort of senior control owners has a detailed understanding of the workings of the business and hold an end-to-end view of process and controls rather than one which is limited by the bank's organisational design.

Their operational rather than risk orientation helps them speak the language of the business unit and make the decisions critical to the successful management of risk in the 1st line.

1. **Clear ownership of key controls** is critical to business understanding and ownership of risk.

   If the ownership is agnostic to organisational structure and aligned instead to critical end-to-end processes, then it will be resilient to the ongoing changes to organisational structure which are a feature of most large financial services organisations.

   In addition to the cultural impact, clear ownership establishes the conditions under which control simplification and rationalisation can occur as a precursor to control automation.

   This sequence of ownership, rationalisation, simplification and then automation, offers the opportunity to improve the effectiveness of management and business units. It will also assist to streamline the underlying processes and increase the risk control awareness of the business.

2. **The second point of re-alignment** in our view is assisting with the effectiveness of control testing and other assurance activity across 1st, 2nd and 3rd lines, and the opportunity for these activities to become far more integrated and effective across the organisation.

   The business unit's responsibility is to own the risk they create and their associated controls, and as such requires primary responsibility for testing them.

   However in many banks the pool of control assurance experience and capability sitting in the 3rd line is insufficiently accessed by those carrying out related tasks in the 1st and 2nd line. In preserving the independence of the lines many organisations have lost the opportunity to leverage 3rd line skills and experience across related activities.

   This means that professional training and development of assurance related staff is not evenly distributed through the organisation.

   It also means that control testing in the 1st, 2nd and 3rd lines are not planned and executed to the same degree and rigour, or in an integrated manner.

   The distribution of control testing activities results in unproductive duplication and no clear line of sight of risk gaps and control weakness.

3. **The third point of re-alignment** addresses the need for the 2nd line to play its rightful role in airing issues. For the 2nd line to move from a reactive role to a proactive role, there needs to be better and more sophisticated use of both detective and predictive analytics, as well as enhanced advisory and challenge capability to draw out the key insights and trends.

   This strengthened 2nd line role will then clearly articulate all the potential impacts of the underlying causes on desired business outcomes and the volatility of earnings.

> "A number of global financial services organisations have created 1st line control owners connected to their key processes – i.e. what must go right."

Less bureaucracy, clearer responsibilities

We propose a simpler risk organisational structure based on the original purpose of each line i.e.:

- Shift primary responsibility for risk management back to business management and recognise that risk ownership is not necessarily achieved by building large separate 1st line risk teams. This can only be achieved with far greater embeddedness of risk culture in business management[1].
- To do this, create business unit senior owners of end-end controls for all key processes. These owners must have responsibility for control effectiveness and control efficiency and be aligned with the business Chief Operating Officers.

  The control owners don't need to be risk or audit people but need to deeply understand how things work – what needs to go right. They will have the responsibility to call on control testing experts to provide the confidence that their controls are designed and operating effectively.
- Accordingly, business unit teams will look very different in terms of capability across the organisation depending upon the complexity of the business processes and associated risks and controls that they own.
- Re-design controls to reduce overlapping controls, simplify where possible, and automate where practical.
- This control restructuring is also aligned with the imperative to simplify and de-risk business by rationalising products and services – a clear priority as many organisations seek to manage conduct and produce better customer outcomes more consistently.
- Consolidate risk advisory functions into a Risk Management function which is responsible for owning the risk and control operating model and challenging the business.

1 Risk Culture – reflects the behaviours and mindsets that are critical to the functioning of an effective risk management framework. Given the emphasis on 3LoD, this article does not explore Risk Culture in detail.

- Create more integrated control testing and assurance capabilities across all three lines that provides technical training and support to enhance quality and consistency, avoids effort duplication and gaps and preserves the independence of Internal Audit.

Underpinning all of this is a need to clearly define roles and responsibilities in relation to risk management right across the organisation.

To achieve this state, Line 2 capabilities will need to improve across two dimensions:

i. **Collaboration** – between Line 2 risk functions and Line 2 BU risk teams to identify cross silo risks, control gaps and opportunities for process improvement

ii. **Capability** – shifting from capture and record to advise and challenge while leveraging analytic insight in a more proactive way.

"In its essence the three lines of defense model is an aggregated roles and responsibilities construct."

Indeed, in a perfect world in which all people had full clarity of their individual risk responsibilities then the three lines of defense is arguably redundant.

Increase the strategic focus of the risk function

The risk function owns the risk management framework, owns the risk operating model (for the whole organisation, not just the 2nd line), advises and challenges the business, and give risk training and guidance to business management.

An enhanced '2nd line' function should also be focused on being involved in or driving major risk mitigation initiatives. These should include risk/controls rationalisation exercises, large-scale process automation initiatives and strategic risk reviews.

Not only do these initiatives reduce operational risk, but they often have customer and efficiency benefits which improve the perceived contribution of risk to the business.

Focus on attitudes towards risk and behaviour in business management

Central to the change proposed in this article is the idea that the business must take back accountability for risk management.

This can only be effective if coupled with a shift away from a reactive and compliance-oriented risk mindset to that of a strong and proactive risk culture.

Risk practitioners across all three lines need to work closer with HR to drive cultural changes which encourage constructive challenge, ethical decision making, appropriate incentives, openness and transparency.

Once again, Line 1 need to own risk culture and Line 2 will play a challenge and advisory role.

A separate voice for Compliance and achieving synergies with Operational Risk

Many banks around the world have grappled with the need to ensure that the compliance function has a seat at the senior executive table and a voice at the Board. There are divergent structures and trends in this regard with three broad types of operating model.

1. Compliance as part of Operational Risk
2. Compliance as a separate discipline within the Risk function
3. Compliance as an independent function to Risk.

Whilst the number of banks pursuing the approach of Compliance as part of Operational Risk is declining there is no clear trend between how best to position Compliance, as a separate discipline with the Risk function or as an independent function to Risk.

Two key drivers at play here are:

i. The need to attract and retain individuals with skill and experiences which are often quite distinct from the Risk function. As the regulatory environment becomes ever more complex, specialist skills to understand and advise are becoming more critical.

ii. Many of the processes on which an effective compliance function must rely are native to the Operational Risk function and in part to the Assurance function. For example, Risk and Control Self Assessments require the detailed engagement of compliance professionals but the process is best managed in our view through the Operational Risk team.

Similarly Incident and Issue management requires Compliance engagement, but is best managed through Operational Risk. The holistic mapping of risks (including Compliance Risk) also fits more easily within the Operational Risk team.

In our view the organisations which are likely to maximise their return on investment in compliance will allow compliance specialists to specialise and then to integrate their capabilities into other core processes, for example:

1. Compliance plan monitoring (integrated with other assurance activities)
2. Risk and Control Self Assessments (executed by 1st line Control Owners)
3. Incident and Issue management and Risk mapping (executed by 2nd line Risk).

The key is to encourage this integration at a process level whilst retaining an independent identity and voice of Compliance.

Conclusion

Financial services firms globally are failing to realise the hoped for returns on investment in Risk and Compliance and meet the needs of their customers and the regulators. To do so we believe there is a critical need to rethink and reframe the value of the risk functions within the organisation.

Financial services organisations can no longer afford to operate as if it were a static world and the role of Risk can no longer act as a reactive function.

To build a truly Risk Intelligent organisation it is important to use data and analytics to generate insights and to build knowledge as well as critically re-thinking the way Three Lines of Defence is deployed so that:

1. Senior 1st line controls owners with real influence and clarity of responsibilities can create the conditions for control rationalisation, simplification and automation they require.
2. 1st line business leaders can take real ownership of risk and control by knowing what needs to go right.
3. Advisory oriented risk professionals are consolidated into the 2nd line, and supported by detective and predictive analytics that play their part in identifying key risk issues for the organisation.
4. Process and control simplification, rationalisation and automation delivers the much needed return on investment in risk and compliance.
5. Compliance has rather an independent voice and integrates operationally with Risk as the owner of the Operational Risk Management Framework and Audit as the leaders of the audit and assurance function.
6. The Internal Audit function while retaining its independence, plays the stronger leadership role of an integrated audit and assurance capability across the three lines.

"If all the above outcomes from rethinking the three lines of defense approach are achieved, then it will be possible to create a 'risk intelligent' organisation that makes strategic decisions with full risk understanding and awareness."

Less bureaucracy,
clearer responsibilities

Increase the strategic
focus of the risk function

Focus on attitudes
towards risk and behaviour
in business management

Focus on what needs
to go right

Contacts

Jean-Philippe Peters
Partner - Risk Advisory
jppeters@deloitte.lu
+352 451 452 276

Martin Flaunet
Partner - Banking & Securities Leader
mflaunet@deloitte.lu
+352 451 452 334

Bertrand Parfait Partner
- Risk Advisory
bparfait@deloitte.lu
+352 451 452 940

Deloitte Luxembourg
560, rue de Neudorf
L-2220 Luxembourg
Grand Duchy of
Luxembourg

Tel.: +352 451 451
Fax: +352 451 452 401
www.deloitte.lu

Deloitte.

Designed and produced by MarCom at Deloitte Luxembourg.