Armstrong Wolfe

The Power of Collective Ambition

Industry Papers 2022 - 2024

Investigations into the 3LoD

Defining the mandate of 1 & 2LoD

Global Economics GROUP

ARMSTRONG WOLFE™

Investigations into the 3LoD

Contents

Executive Summary

The 10th Anniversary of the Chief Control Officer's Forum

In 2014 Armstrong Wolfe ('AW') hosted a COO Markets roundtable discussion and dinner, the subject of debate an article written by AW's CEO, Maurice Evlyn-Bufton:

» Defining the indefinable the evolution of the front office control officer

At this early stage of market evolution, the concept of a CCO was very limited, the acronym being better known to be the Chief Compliance Officer, as opposed to the Chief Control Officer.

The responsibility of first line operational risk, however, was well established, embedded in front office business management and the product COOs.

The arrival of the concept of the 3 lines of defence, developed in 2008-10 by the Federation of European Risk Management Associations (FERMA) and the European Confederation of Institutes of Internal Auditing (ECIIA), had initiated a corralling of resources into a non-prescriptive model of a 1st, 2nd, and 3rd line.

This triggered an awareness of a distinction in responsibility and accountability, which was accelerated when the FCA launched its 5 Conduct Questions Programme in 2015, initially as a Supervisory tool for the Wholesale Banking sector to help firms improve their conduct risk management and, ultimately, drive cultural change.

The FCA has consistently emphasised the importance of these Rules, which it sees as establishing a baseline level of conduct and good behaviour for everyone doing financial services work, with the aim of reinforcing positive working cultures across the sector.

Into this space of interpretation, AW offered a platform for discussion and debate, the sharing of perspectives and challenges.

By 2016 the title Chief Control Officer had become common place and AW split the forum into COO to CCO forums, managing the 2 communities in parallel but addressing different challenges.

Throughout its evolution AW has been steadfast in keeping to the founding principles of the CCO forums:

» The CCO Forum is for the industry, hosted by the industry, for the benefit of the industry

» Its purpose is to provide a trusted environment for the regional and global Control Officer community to discuss market-wide non-proprietary challenges, to exchange thought and innovation and to develop solutions to meet these challenges

» It is inclusive not exclusive, all banks however large or small, face the same challenges, and if any bank is able to elevate its controls and conduct by participation all members will benefit

AW's CEO states:

> *"Whilst we remain the intellectual hub for the managing directorate of CCO community, I applaud the industry's efforts to seek to address the issues arising through poor controls, culture, and leadership, that manifest themselves in poor conduct.*
>
> *Whilst we have our own in-house expertise of former global and regional professionals, COOs and CCOs, that support the debate from a seat of objectivity, we have also been privileged to work with and continue to engage with the world's leading authorities on this subject, be they academics, advisory and consulting, technologists, industry bodies or regulators.*
>
> *The conference circuit has done wonders in raising the awareness of this challenge to the many, whilst we focus our energy on the voice of the few. Our community is the global and regional COOs and CCOs we serve through the International COO Community (iCOOC), charged and responsible for daily controls and conduct"*

By 2020 the CCO forum met quarterly in 5 financial services centres globally. With the advent of the pandemic the strength of this community and the trust it had in AW's platform manifested itself with AW running 65 virtual regional and global forums in March – April, in support of the COO and CCO communities. This communication bridge enabled peers to meet to discuss how best to meet and navigate the unique portfolio of changes presented by WFH.

In 2020 both the CCO and COO forums were rolled into the International COO Community (iCOOC), and in 2021 its 1st Line Business Controls Working Group presented its year end industry paper to the FCA and has been requested to do the same with its 2022 paper. The 2022 paper will further be presented upon request to regulators in the US, Canada, Hong Kong, and Singapore.

The 2022 paper revisited the principles and recommendations outlined in the 2021 report, seeking to understand what progress has been made in adopting them by the participating iCOOC membership. Its findings will be discussed at the 2023 COO Summit, the session being titled: 3LoD is a journey not a destination.

Recognition and endorsement on the work undertaken by AW group is not short in supply:

> *"The Chief Operating Officer plays a pivotal role in the organisation and is increasingly positioned to advise on and oversee and directly address the operational health and integrity of business models. In a world of continuing and sometimes unexpected change, the community of COO's has become an essential layer of the financial services industry.*
>
> *Armstrong Wolfe provides pure oxygen to this layer by channelling and focusing the energy of the members on key topics in a manner that leads to tangible action for follow-up. It is an honour to be able to assist"* **Ted MacDonald,** Financial Markets Standards Board

In 2024 AW will take its CCO Forum forward with a renewed debate, leveraging the themes coming from the summit's debate on the same:

- 3LoD is a journey not a destination: developing fresh perspectives

Long and short-term participants and advocates were asked the question, **"What differentiates AW's CCO forum and how do you define ROI on participation?**

- "It is the trusted platform for the global 1st Line Control Officer community. Armstrong Wolfe understands the true value is in the peer-to-peer exchange, excellently facilitated and moderated by Maurice and his team".
- "Armstrong Wolfe's Control Officer community has a true sense of camaraderie, that enables effective collaboration".
- "Developing a fully inclusive community within the banking sector is no easy task, this is what Armstrong Wolfe has achieved. I am delighted to be part of it".
- "It is not just the execution of the forums, but the thought leadership Maurice and his advisory team brings to the community. The ability to translate our collective thought into a seamless stream of thought is differentiating".

AW's CEO added:

> *"We remain committed to supporting the members of iCOOC. We remain committed to providing a haven for debate and innovation.*
>
> *We remain committed to helping those charged with making the industry a safer place for investment, a better place for employment and to serve clients and society worldwide.*
>
> *We are exceptionally proud of what we have achieved working with the global COO and CCO communities over the last 9 years and look forward a second decade at the helm. More so we feel our trusted platform will be play a key role as the multi-faceted implications of non-financial risk unfold in a geopolitically unstable world"*

"The Chief Operating Officer plays a pivotal role in the organisation and is increasingly positioned to advise on and oversee and directly address the operational health and integrity of business models."

What our clients say...

"More than a decade ago Armstrong Wolfe were the pioneers of bringing the global banking COO/ CCO community together to discuss topical and emerging issues. As a result, they and their network are at the forefront of thought leadership in this space."
Jason Hope

"Armstrong Wolfe demonstrates a deep understanding of the roles that COOs play within Banking. It leverages this understanding to bring together the COO community, where we can benefit through interaction on shared priority topics."
Chris Dickins

"Armstrong Wolfe continues to deliver high-value and provide deep insights, covering our current environment and providing a future-focused outlook on tomorrow's opportunities. Our membership has been a powerful benefit that has enriched our entire team."
Summer Hinton

"Armstrong Wolfe has uniquely positioned itself as an effective conduit for the COO community to agree, discuss and take proactive measures to address the key themes and challenges facing the financial sector, both planned and unforeseen. By combining peer knowledge and perspectives with deep SMEs and solution providers, AW forums and events provide invaluable support to sell and buy side COOs."
Gary Simpson

"Congratulations on your continued success and progressive evolution. For many years you have added value to the FS COO community,and I have witnessed your transition into a purpose-focused enterprise. The COO community benefits from the support, innovation and thought leadership Armstrong Wolfe brings to it, with the 2022 COO Compendium being another example of demonstrating your deep rooted understanding of this largely misunderstood function. Well done!"
David Sharratt

Global Economics GROUP

Developing fresh perspectives in the 3LoD

Maurice Evlyn-Bufton
CEO
Armstrong Wolfe

Chris Rigg
AW Alliance Partner
Global Economics Group

Background & Introduction

Since it was first articulated, the Three Lines of Defence model has developed to be almost universally accepted by financial institutions and regulatory bodies across the globe as the standard foundation for risk management frameworks.

Yet despite its widespread acceptance, difficulties in defining and implementing the model in practice continue to exist.

Regulators, academics, and industry executives have all highlighted challenges in the application of the Three Lines of Defence model and suggested ways in which some of the inherent structural tensions can be managed.

The work of Armstrong Wolfe's international COO Community (iCOOC) in 2021, summarised in the report titled 'The 3 Lines of Defence: A view from the First Line', pooled the candid views of 29 senior first line of defence representatives from a broad cross-section of international financial institutions.

iCOOC was clear that the guidance it produced represented a series of useful first steps, but that more would need to be done to ensure that lasting change is embedded within the Community.

A universally generalisable solution to these challenges does not exist, but iCOOC has sought to take the next step in promoting change by assessing how well the principles and recommended actions from 2021 are embedded in institutions' operating models. It has done so through a self-assessment survey in which members of iCOOC were asked to assess how far the principles and recommended actions articulated in the 2021 Report had been embedded in their organisations.

32 members replied, providing a truly global snapshot of views from senior leaders within the First Line. Armstrong Wolfe and Interpath Advisory analysed the qualitative and quantitative data in these responses and combined it with personal reflections gained from respondents through Working Group meetings as well as one-to-one conversations to synthesise perspectives and articulate the underlying narrative.

The insights from this exercise, summarised in this paper, are invaluable in highlighting the challenges commonly faced across the Community and accordingly guiding the future direction of iCOOC's work. iCOOC's aim in this work was to promote sharing of working practices, both in the First and Second line, suggest principles, recommend actions and provide benchmarks.

What have we learnt?

iCOOC's responses show that institutions continue to experience difficulties in the alignment of their First and Second line functions, ultimately reflecting potential inefficient working practices, and in turn, cost inefficiencies. To some extent this is unsurprising; these challenges are long standing and if relatively simple solutions were available, they would likely have already been exploited.

Broadly, the trend does appear to be in a positive direction. Respondents have shown progress in articulating what they are working towards in the implementation of the Three Lines of Defence model (measured by assessing how far the 2021 principles have been embedded), even if progress against the recommended actions and how to get there has been more limited.

Challenges related to the balance of resources across the lines seem particularly entrenched, with progress against the recommended actions in these areas being particularly difficult. Respondents commonly perceived an imbalance in resources allocated to the First and Second Lines commensurate to their respective responsibilities remains a source of tension.

Why? How iCOOC can lead change in 2025.

iCOOC members pinpointed a range of factors that may have contributed to the challenges in effecting change against the recommended actions. The consensus was that change is hindered by the issues being:

- fundamentally structural to the Three Lines of Defence model;
- arising from a lack of clarity about what good looks like across stakeholders; and/or
- there is simply insufficient bandwidth for COOs to address them as a result of the wider change agenda.

What does this mean for iCOOC's direction? Sadly, socio-economic conditions look to be as challenging in 2025 as they were in 2024, meaning the demands upon the COO community are likely to be just as intense. Similarly, individual institutions are likely to be best placed to navigate a path through the structural challenges they face.

Therefore, as a community, iCOOC will continue to devote its efforts to finding consensus about the operation of the Three Lines of Defence model and providing leadership in challenging the status quo.

1B or not 1B this is the question

Maurice Evlyn-Bufton
CEO
Armstrong Wolfe

The 2023 1st Line Business Controls Working Group set itself the target to produce an industry paper to define the future target operating model of the 3LoD, thereby seeking to uncover and promote fresh perspectives

Minutes

iCOOC 1st Line Business Controls Working Group

Debate: Developing fresh perspectives on the 3LoD: **1B or not 1B** *this is the question*.

Utilising the AW Q4 2021 report (A view from the 1st line), the group is seeking to answer the questions:

- What progress have we made since the prior report?
- Do we still feel that the issues highlighted in that report are valid?

To answer these questions, in Q3 2022 AW conducted a survey, focused on the principles and recommendations found in the first report. Initial findings strongly indicate whilst adherence to the principles remains strong, little or no progress has been made in implementing the recommendations aligned to these principles. Something that will be investigated in Q4 2022.

As one Control Officer pointed out 'the fundamental issue with the 3LoD model is that there is no definitive model, no golden source to reference when building or fine-tuning your 3LoD, and that without this reference point companies are left to interpret and frame their (best) approach'. This leaves them open to regulatory scrutiny and recommendations (drawn from practices at competitors and embedded elsewhere in the industry).

This does not allow (banks) to be on the front foot and have confidence to take a proactive approach in fine-tuning or reshaping tasks and responsibilities within the 3LoD, fearing the consequences of stepping outside the well-trodden path. The industry mostly remains steadfast as to the model in place, rarely leaping across the divide to incorporate, embed and allow for lessons learnt or for inevitable technological advancements, many of which could help deliver an enhanced control environment, efficiencies and cost savings whilst adhering to the 3LoD principles of independence.

We also understand the attempt to provide a 'harmonised view on a 3LOD TOM' could be received less than enthusiastically by some participants, or run the risk of not having the impact we would like. During conversations, it emerged quite clearly that different organisations have different structures, cultures, politics and a variety of other features which mean a single, definitive model is unlikely to work for all but this does not mean for the purpose of debate such a model cannot be presented. This is what some believe drives the divide on 1B (which is one of semantics only because all agree on the need for control, but have views as to whether it should be called out as being separate or not).

In attempting to come up with a single model, we might run the risk of it being loved or loathed in the same way that the concept of 1B or 1.5 is. On the other hand, if we shift the focus to roles, mandates, 1LOD : 2LOD ratios, barriers to implementation etc, we might receive a more positive response and greater engagement with the group's year-end paper.

If we remain committed to testing the status quo, the best approach would appear to do both. Our conclusion is we need to be brave in this context or otherwise we could find ourselves merely reaffirming the status quo as opposed to challenging it, bettering it, prompting a call to action.

For the avoidance of doubt, when we say 'harmonise' we should state, as we have done so above, that we recognise every firm is different, but remain loyal to our stated aim to deliver a TOM for 3LoD based upon lessons learnt, what is working/what is not, what common issues exist and how to address them etc. In this context, and as an example, we conclude the term 1B/1.5 as an unnecessary addition to the TOM, unless we conversely accept it and thus, we are in all but name shifting to 4LoD.

The year-end paper is not to be a 3LoD bible, but an informed piece of industry research that should enable internal debate within iCOOC's membership, based upon the paper's content being a representation of the views and expertise of 33 of the world's leading banks and their Control Officers.

The forum came in the wake of a 33 iCOOC member bank participation in AW's Q3 2022 1st Line Business Controls survey. This survey revisited the concluding principles and recommendations of the same group's Q4 2021 report, A view from the 1st Line, presented to the FCA. The Working Group will produce a follow-on white paper in January 2023; a consensus and harmonised view on the 3LoD target operating model (see below the 2022 programme of work and timetable).

Drawn from an initial review of the survey results, two points of deliberation were chosen, both presenting a split view which pose a potential challenge to the consensus being sought:

- Terminology, definition, and the use of the term 1B and/or Line 1.5
- The report line and positioning of the 1st Line Control Officer

A Contentious Point

iCOOC member debate suggests the use of the term 1B is a distraction to some, ignored by others, is questioned by those that do not use it, and is accepted as the norm by the minority. There is no consensus, although a majority (across the 33 iCOOC global member banks) question its validity and benefit. 'Each bank is different, has different business models, challenges' is the common refrain to justify having 1B or to put one side a need to question it.

The argument would appear somewhat simpler, however, as its definition and existence create a 4th line of defence, which is not so much ensuring independence as to abdicating responsibility from 1A (if this exists) to 1B, and additionally drives a cultural divide through the 1st line.

The 1st line should see itself as one, not two halves, the controls team being an extension and attached limb of trading and sales, not a function across the divide, a line drawn through the 1st line, defining the territory between 1A and a 1B.

This point is supported by many, the opinion of three Control Officers summarised below:

> *"Before I took over the 1st Line Risk and Control function, the prior regime portrayed itself as LoD 1.5, i.e., 1B. I can say with direct experience this term created more confusion than clarity. Unfortunately, it was also used to shift responsibility away from the group while still 'allowing' the group to mandate responsibilities on to others.*
>
> *To address these issues, I did away with the term and made clear that we were in the 1st LoD along with Trading, Sales, etc. This helped to make our mandate much clearer i.e., our role was to assist in the execution of 1st Line supervision and remediation, rather than to be a check and challenge upon it, namely the 2nd LoD."*
>
> *"The industry still does not have a consensus of the mandate of 1B (controls and even the COO). This needs to be resolved not just within individual firms but across the industry, such consistency will benefit all."*

This persisted lack of consensus and clarity can have adverse results:

- Management fear to relieve the 1A of any risk and control responsibilities through either formal or informal delegations to 1B, or general over-reliance on 1B
- Inconsistent expectations of the 1B from groups external to the bus unit such as regional management, head office, risk, other teams, etc.
- Dividing line within 1st line can lead to lack of buy-in from production teams
- Budget constraints - lack of visibility on the value-added"

> *"My own experience in building a 1B line of defence (a term imposed by headquarters) was to align it as close as possible to the business as possible and help identify real-time and true risks that the business is facing, and consequently (re) design controls that address the risks, providing controls that are executable, effective, and trackable. When you included surveillance into the 1B construct there exists a level of delegated authority to leverage the managers.*
>
> *The problem with this setup was driven by head office that 1B was too close to the business and lacked independence. In my opinion this is a symptom of lack of understanding and fear (of regulatory push back)."*

When this point of view was put before an informed industry expert, one with considerable experience having worked previously for the regulator, with a focus on the 3LoD operating model, feedback was perhaps not surprisingly more contemplative in nature, although the concluding comment seemed to endorse the direction of travel:

> *"I wonder if there is a particular circumstance and/or approach to in-business risk management and business model where a 1B or 1.5 would make more sense, provided it was well run? There may be, but it does not stand out today and therefore you are poised to make quite a big call on 3 LoD organisational design, which I am inclined to support."*

If the objective is to set a 3 LoD target operating model that enhances control, resilience, and shares responsibility within a common objective, then the term 1B arguably becomes dormant if not extinct. If you apply a taxonomy and have detailed role specifications and tasking, focused on the output of each task, then where each task and its owner sits can migrate between the lines, whilst the 1st line retains accountability. If this view is taken, embedded as a principle (iCOOC's membership supported in its Q4 2021 report, A view from the 1st Line), then the term 1B needs to be removed from the narrative.

A Different Perspective

Rather than answer the question on whether 1B should exist (1B or not 1B), perhaps we should take it back to first principles and look at what exactly we are looking to achieve when we say non-financial risk management in the 1st line. Many summarise this in five pillars:

1. **Risk Identification** – this could be via an external/internal event, first, second or third line internal reviews, regulatory reviews, audits. It could also be done via establishing intelligent KRIs. This is also identifying horizon risks such as the impact of future regulation.
2. **Risk Assessment** – quantification of the risk level from the identified gaps.
3. **Risk Governance** – we need to put in place frameworks that ensure we are following policies, standards, and risk management processes. We ensure we can evidence effective risk management in line with the Senior Manager statement of responsibilities shared with the FCA. This is typically documented through non-financial risk committees.
4. **Risk Remediation** – the solutioning of the risk and gaps, from scoping requirements and funding to delivering the remediation.
5. **Risk Monitoring** – ensuring the controls are working as they are supposed to. This could be done via control sample testing and/or key control Indicators.

Looking at the above, the main considerations are:

- How do we ensure the Senior Manager (typically business CEO) commitments to the FCA are met?
- How do we ensure no conflict of interest (poacher and gamekeeper)?
- Where does the competency to perform the role, most effectively reside?
- What is the most cost-effective way of delivering the above?

To ensure the CEO's interest are served and there is no conflict of interest, risk identification, assessment and governance (1, 2 and 3) should sit directly under the Business CEO and not within the COO function **for the following reasons**:

- The COO function run many of the control processes and failures found would typically reside in this world, hence if risk identification and assessment were to sit within COO there is a potential conflict to disclose and reasonably assess impact.
- The COO function may also prioritise the generation of revenue over risk identification and therefore not give the focus required
- The COO function, Business Risk Managers, may have the competency around business processes and risk, however, often lack competency to implement and run effective risk identification, assessment, and governance

Three Further Assumptions

- Risk remediation (4) should sit with process owners of the controls, and this is typically managed by the COO function hence why remediation should be aligned to COO. Governance/assurance of the remediation being done independently by 1st line risk sitting under the CEO
- Risk monitoring is simply another form or risk identification and should also sit within 1st line risk under the CEO
- Lines are not totally black and, in some areas, grey i.e. when it comes to risk identification, we would still expect business COOs to identify risk, the difference being this would be in day to day running of the business vs performing investigations. The business COOs would be involved in risk assessment however not have the final say on the level of risk, ensuring independence maintained

The Control Officer within the 3LoD TOM

The previous lends itself to further defining the role and mandate of the 1st Line Control Officer:

- The role of the control officer is to specifically manage the statutory obligations of SMR on behalf of the CEO. This is to ensure effective risk identification, assessment, remediation, governance, and control effectiveness
- The role should be viewed as being responsible for key component parts of the risk management chain: identification, assessment, governance, and control effectiveness, but not remediation which resides with the respective process/ control owners.
- The role of the Control Officer is to provide informed, independent, and objective counsel to the CEO routinely and/or upon request, to enable the CEO to make informed decisions to stop, restrict or continue business; what to escalate; where to prioritise funding
- The evolutionary role of the Control Officer is to be responsible for the aggregation and translation of the taxonomy of non-financial risks, providing the CEO a reliable horizon scanning capability to make informed and/or anticipatory decisions to mitigate the impact of an unforeseen event e.g., geo-political, conduct, human capital, climate, reputational, cyber, in order to answer the 'so what' when these risks are centralised for translation

"The industry still does not have a consensus of the mandate of 1B (controls and even the COO). This needs to be resolved..."

Notedly on the final bullet point, a former Global COO commented:

> *"The concept of calling something NFR is interesting and has been challenged by certain business heads. What is non-financial risk? Some would say such risks occur from inappropriate processes, controls, or supervision but it is far broader than this. Its management is differentiated from financial risk, be this market, credit, or liquidity, by the distinct skills required to translate NFRs, but to say that 1A can be less focused on NFR, relying on a 1B, is a mistake.*
>
> *We are all aware of the broadening spectrum of threat management and the increasing complexity and interconnectedness of processes, flows, markets, and so on and that the consequence of operational losses, legal fees and remediation are significant and can and do stack up to market or credit risk events. This level of risk needs to be managed by the 1st line, which requires a new and more forward, outward looking approach if a CEO is to be able to manage NFR (of which 1st line controls and governance are a part) effectively in the new paradigm."*

This evolution has led to the market reviewing and some interpreting and positioning the 1st Line Control Officer differently, which leads to further debate as to which model serves the interests of the CEO and business best:

- Control Officer reports into the COO, in business control resources report directly to the Control Officer
- Control Officer reports into the COO, in business control resources report directly into the business line, dotted line to the Control Officer
- Control Officer reports into the CEO, in business control resources report directly to the Control Officer
- Control Officer reports into the CEO, in business control resources report directly into the business line, dotted line to the Control Officer

These battle lines of debate are not as clear on this matter as to the embedded industry-wide perspectives and views on 1B or not 1B. The debate on the correct positioning of the Control Officer (evolutionary NRF Head) is less advanced:

> *"The COO function can be considered 1B by some firms, or 1A for the truly aligned CEO/COO model (see previous AW POVs). When you think about tech dev, AI, new partners - initiatives that the COO can lead, these activities are far from traditional 1B controls/NFR responsibilities.*
>
> *Practically speaking most COOs straddle across 1A and 1B which leads to the same definitional challenge as with the Controls function. Do COOs/BMs just help, or can they affirmatively execute controls/supervision? Is the COO accountable to assess the risk and develop solutions, or do they present what they think and then the business designs the appropriate risk management? Does the COO sign risk-acceptance docs?"*

Another adds:

> *"My conclusion is that 1B must be part of the business and embedded within it, as 1LoD, reporting to the CEO, not through the COO and thus the CEO directly owns and is accountable 1LoD (ref: SMR). The term 1B should be discounted as a confusion. The 2nd line can then focus on standards, frameworks, and effective challenge with which the business operates within - setting the 'rules of the road' and overall governance."*

More a majority verdict than a consensus

Evidenced by the on-going discussions with the ICOOC 1st Line Business Controls community and Working Group, and if pushed at this stage of the 2022 programme and debate, the following conclusions will feed further debate if a consensus is to be secured:

- 1B as a definitive term within the market wide 3LoD narrative serves no purpose in the design of the future 3LoD TOM
- Control Officer reporting into the CEO, with the in business control resources reporting directly to the Control Officer, delivers the independence to avoid the use of the term 1B and raises the importance of 1st line controls and non-financial risk to an appropriate elevated position to the executive

"Is the COO accountable to assess the risk and develop solutions, or do they present what they think and then the business designs the appropriate risk management?"

A view from the 1st Line

1. Introduction

The Markets' Chief Control Officer (CCO) Community was first convened in London by Armstrong Wolfe in 2015, and over the next 6 years it evolved to include 30 banks participating in a quarterly forum in Toronto, New York, London, Singapore and Hong Kong. Running in parallel with forums for the Chief Operating Officer (COO) community, it led to the establishment of the International COO Community (COOC) in 2020.

iCOOC's purpose is to provide a platform for peer-to-peer exchange, debate and the development of potential solutions to meet market wide, non-proprietary challenges in support of the CCO and COO communities. Controls, conduct, culture, and purpose are at the heart of this collective examination.

In the interim years, whatever debate was run, in which ever location, each, and every discussion would find its way at some point to the issue that had become embedded in the 3LOD: how best to make the first and second line work together efficiently and cost effectively.

From 2021 to 2024, representatives from across iCOOC came together to develop this review. Their aim was not to migrate, dilute responsibility or seek to reduce the accountability of the first line, but to share the challenges that they have seen institutions try to work through, and to consider ways to achieve a more effective, workable solution so that they can deliver on their 3LOD obligations and in their objective to protect the franchise of the firms they represent.

This report represents the collective voice of the community that has been engaged in the process.

2. Executive Summary

The concept of the three lines of defence has existed in one form or another since around or just before 2010

It was first comprehensively described in a paper by the Institute of Internal Auditors (IIA) in 2013 which this has served as a loose albeit frequently evolving reference ever since. Numerous papers, both industry and academic have addressed the topic, introducing additional variations and nuances to the model; and financial regulators across the globe have indicated their expectation that the model will be built into the risk and control arrangements made by financial institutions.

The widespread adoption of the Three Lines model means that this report's findings have relevance to a broad range of industry practitioners. As many of our recommendations might require some level of change to business operations and risk-management approaches, CEOs will undoubtedly find them compelling. Heads of Compliance, Risk and Internal Audit confront the issues the report addresses on a daily basis, as do heads of business divisions. Chief Operating Officers or Chief Control Officers will be interested to know the difficulties faced by their peers. Boards, with their overall role of governance and oversight, will find the recommendations useful. Finally, regulators should take note both of our recommendations for direct action from them, and of the challenges experienced by regulated firms in implementing such a ubiquitous model

The three lines concept works by insisting on the division of the financial institution's staff into three independent groups. The first line is often described as the business', those staff that are the primary revenue generators for the firm and their immediate support network - this is where risks and their mitigating controls largely sit.

The second line of defence is described as a combination of risk management and compliance functions united in the role of providing, variously challenge, oversight, and assurance in relation to the first line.

The third line of defence relates to internal and external audit, responsible for reviewing and reporting on the work of both of the other two lines. The prevention of harm is the ultimate goal to which all parties subscribe. The institute of Internal Auditors: The Three Lines of Defense in Effective Risk Management and Control (January 2013)

Whilst most can agree with this sort of broad-brush description of the model - which this report adopts as a definition of the Three Lines model - difficulties have typically arisen in defining the detail. Nowhere has this been more marked than in defining the correct dividing line between the first and second line of defence, both in terms of correctly defining their populations, but also in terms of the allocation of controls responsibilities between them.

This report seeks to explore these challenges and to propose solutions, by pooling the candid views of 29 senior first line of defence representatives from a broad cross-section of international financial institutions.

Respondents were typically performing as Chief Operating Officers, Chief Controls Officers or Heads of First Line Operational Risk. Representatives of Armstrong Wolfe and FTI initially interviewed each individual separately to canvas views on the effectiveness of the three lines of defence and, in particular, to explore areas which were not working as well as they might

From the interview process a strong consensus emerged amongst the respondents, with a marked convergence on four highly complementary pain points. These were:

- Lack of clarity in roles and responsibilities of the first line
- An ambiguous second line mandate
- Duplication of activities and inefficiencies
- Balance of resources across the lines

To further explore these pain points', the original respondents reconvened in a series of workshops. Recognising that no two organisations are the same, the goal was to evolve a series of principles against which financial institutions could self-evaluate and take appropriate corrective action. The principles were as follows:

- The first and second Line should have a unified risk outlook
- Respective mandates for the first and second lines should be formalised and documented in order to ensure a common understanding of roles and responsibilities across the lines.
- Line 1B (where it exists) can and should be made sufficiently independent of aspects of the business
- To be effective, testing should be organised in a standard, principled way across the first and second lines of defence
- v. The requirement of the second line to be independent from the business function should not preclude the second line from performing an advisory role for the first.
- Duplication of tasks between the first and second line should be minimised.
- Policy owners should consider the end-to-end execution, implementation and testing required to make a policy effective.
- The allocation of resources across the three lines should be reviewed if it is deemed to be beneficial towards the aim of delivering a more robust efficient and effective control environment.

These principles lead to a series of Recommended Actions for the institutions themselves as well as for regulators. Though not an exhaustive list of potential remedial measures, they act as a generalisable set of useful first steps. For the institutions, the actions are:

- Banks should perform an end to end review and cataloguing of existing risk and control activities performed by business and product.
- To ensure alignment, create a common understanding and transparent view of all risk and control activity
- Formalise and document the mandates for the first and second lines.
- Where duplicative risk and control activity is identified, assess the rationale for it to exist.
- Where a Line 1B exists, assess whether it can be deemed "sufficiently independent of the business that it supervises, and if not, what steps could be taken to address it.
- Assess the appropriateness of resourcing and skillsets deployed against risk and control activities across both first and second line.
- When establishing new policies and procedures, or making substantive changes to existing ones, ensure that these are designed from an end to end perspective, with engagement and input from all stakeholders across both first and second line that are potentially impacted by the policy.
- Agree and document a standardised testing methodology

The workshops noted that regulators have been quick to espouse the three lines model but have been relatively silent on the details that institutions have wrestled to interpret. It was also noted that in the enforcement action taken in the early 2010s, there has been an unintended consequence of a significant increase in the size of the second line in many institutions, concurrent with a growing demand for migration of risk and control responsibility to the first line. It was noted that wide-ranging enforcement action and heavy fines which followed the financial crisis and continuing misdemeanours, prompted firms to significantly increase the size of the second line. This was concurrent with a major push for the first line to demonstrate full ownership and control of their risks.

Accordingly, the recommendation to regulators is to assist by conducting some form of thematic review, scaled in accordance with resources and priorities, that addresses the manner of implementation of the three lines of defence. In order to encourage adoption of the principles outlined in this report, Regulatory acknowledgement of the existence and usefulness of the these principles as a point of reference (this is not to suggest endorsement) in tandem with some form of thematic work would form a solid foundation of best practice for the industry.

Armstrong Wolfe would like the thank all of the participants in this process for their time and valuable contributions.

3. Background

Since its original formulation, the Three Lines model has been almost universally accepted by financial institutions and regulatory bodies across the globe as the standard foundation for risk management frameworks. The model has evolved over time, with regulators, firms and professional bodies coming to adopt diverging approaches to its implementation from the mandate and responsibilities of the lines to the distribution of resources across them. The emergence of new risks and the corresponding need to reflect them within the framework has exacerbated this divergence.

3.1 A brief history of the Three Lines model

The earliest references to the Three Lines model by an industry body can be found in a 2010 paper by the European Confederation of Institutes of Internal Auditing ('ECIIA) and Federation of European Risk Management Associations ('FERMA") European. In that paper, the model was treated as a description of the sources of information consulted by the board and CEO in overseeing and monitoring risk management - and not formal guidance of how to create an effective risk management framework.

The description of the role of each line is therefore basic: the first line is operational management, which has ownership, accountability and responsibility for risks; the second line is comprised of the risk management function and compliance, which facilitates and monitors the implementation of controls by the first line; the third line is the internal audit function, which provides assurance (ECIIA/FERMA, 2010).

FCA: Thematic Review TR14/15 - Best execution for payment for order flow (July 2014). ECIIA FERMA: Guidance on the 8th EU Company Law Directive (article 41) (September 2010). The institute of Internal Auditors: The Three Lines of Defence in Elective Risk Management and Control (January 2013).

The first comprehensive formulation of the Three Lines model is widely recognised to have come from the Institute of Internal Auditors ('11A) in 2013. This paper defined each of the lines as follows:

> *'As the first line of defence, operational managers own and manage risks. They are also responsible for implementing corrective actions to address process and control deficiencies.'*
>
> *'The second line) functions to ensure the first line of defence is property designed, in place, and operating as intended.'*
>
> *'Internal audit provides assurance on the effectiveness of governance, risk management, and internal controls.'*
>
> **(Institute of Internal Auditors, 2013)**

The IIA has periodically issued follow-up guidance to clarify the role of each of the lines, and the principles which underpin effective implementation of the model, most recently in 2020. The principles presented in this update modified slightly the definition of each line's roles and responsibilities.

The first line of defence leads on risk management, and establishes and operates necessary reporting structures - ensuring compliance with legal, regulatory and ethical obligations.

4. Pain Points

While there is generally wide-ranging support for the concept of the model - echoed by our first line practitioners - the challenges primarily lie with its implementation. Participants reported similar experiences with the Three Lines model, including identical or closely related implementation challenges. Among these common pain points, we noted some key overarching themes, which emerged across the interviews and workshops:

4.1 Lack of clarity in roles and responsibilities

Across the three lines of defence, there is a notable lack of clarity around the appropriate allocation of roles and responsibilities, particularly between the first and second line.

From the first line perspective, the respective mandates of the first and second line are not clearly outlined, and there was said to be "more grey than black and white". Across the board, firms hadn't made a conscious effort to formally document these mandates internally, but participants also noted a lack of prescription in the regulations and guidance to support institutions in achieving a common understanding.

Often, regulatory guidance is unclear and divergent across jurisdictions; different regulators may have differing interpretations of the first and second line functions. Many interviewees recounted the emergence of a line '1A' and '1B' partly as an answer to the regulatory expectation that the first line own and control their risk, with 1B acting as an independent monitoring function which sits within the first line. However, this had not clarified the mandate of the first line and potentially serves to muddy the role of the second.

4.2 Unclear second line mandate

The mandate of the second line is ambiguous and conflicting between a check and challenge function on one hand, and an advisory role on the other.

The participants' interpretation of the second line function oscillated between an advisory role and one focused on challenge and assurance. Some outlined that there needs to be a clearer distinction between the performance of controls, the reperforming of controls, and then auditing or challenge of the controls. This issue was often cited as stemming from the second line's interpretation of the need for 'independence, and a lack of clarity surrounding what this independence ought to entail. This ambiguity called into the question the exact manner in which the second line is to add value, and the bounds of their role to the extent that they still further the business' interests. This is not to say that participants did not perceive value-add from the second line-expanding its advisory function to include regulatory horizon-scanning and identification of emerging risks is seen by some participants as an obvious way for the second line to have a greater tangible and positive impact on the wider business.

Some participants also noted that the regulators have not clearly outlined the mandate of the second line and, when they have, it has set unrealistic expectations such as for the second line to have "endless challenge without boundaries" - challenge which, in particular, extends beyond the accepted risk parameters and risk tolerance within which the firm is comfortable operating. The natural divergence in risk appetite between the first and second line exacerbates this divide, preventing an aligned approach to managing risks and increasing instances of second line push-back.

Unclear distinction between first and second line - The two themes described above, a lack of clarity in roles and responsibilities and an unclear second line mandate are essentially two sides of an identical problem:

There is a nebulous boundary between first and second line functions. This singular issue was the dominant one around which the workshop discussions centred, and was fundamental to the other challenges identified. An often-cited example in the workshops that reflects this theme was the issue of where monitoring and surveillance controls ought to sit. The technical vernacular of traders is such that a second line officer may not be able to understand and therefore properly monitor the trading activity, however, it can equally be argued that the first line lacks the independence to perform this function.

Participants noted that independent surveillance monitoring is a common regulatory expectation - but there is a lack of clarity around whether it necessarily follows that independence must fall within the second line. This raises the question of how independence should be defined; this appears to be a key principle underpinning the second line's mandate, but it is ill-defined and most banks did not have a clear understanding of what it ought to mean.

Many participants agree with the idea that independence does not necessarily sit in any particular line: with the right reporting or incentive structures in place, sufficient independence from relevant business processes could be created in the first or second line.

Despite this consensus, there was a reluctance amongst the participants to identify operational principles which rigorously divide the first and second line. This reluctance was due to the intrinsic link between the mandate of the second line and regulatory oversight, in combination with the relative paucity of guidance. Participants felt that they ran the risk of regulatory censure in moving processes to the first line (even when it made clear operational sense) from the second, given the regulatory focus on robust second line mandates and resourcing. The combination of uncertainty from the regulatory guidance and banks' own hesitance resulted in this being the primary, underlying issue faced by most firms.

4.3 Duplication and inefficiencies

Often there is a duplication of activities by the first and second lines leading to operational inefficiencies in the risk management framework.

The lack of clarity around the mandate of the second line- and particularly around its requirement for independence - translates into the practical issue of inefficient or ineffective control frameworks. Participants highlighted duplication of activities across the first and second lines, most notably in the realm of testing. It was felt that a lack of trust had developed between the lines as a result of siloed approaches: the first line may not trust the second to have the appropriate understanding of the business, and the second line may not trust the first to effectively carry out controls. Hence, the second line tended to exercise its check-and-challenge mandate by repeating first line functions. This is also linked to the second line's belief that it needs to repeat controls to demonstrate independence, rather than exclusively check and challenge. This problem remained even with the presence of an established 1B function.

There was variance in the kind of duplication discussed by participants. It was often seen that in carrying out a particular function, the second line would effectively reperform controls from scratch using completely different processes, methods, data sets and systems when compared to the first line, where they felt that first line output was unreliable. On the opposite end of the spectrum, other participants noted that the second line would exactly duplicate the work of the first line-calling into question whether the veracity of the first line's conclusion was even being checked at all. An often cited example of such duplicative activities was testing controls. Respondents argued that this was not necessarily due to an internal misunderstanding of the Three Lines model, but fear of regulatory censure if testing was not perceived to be independent. Both scenarios can cause inefficiency, or inconsistent and unreliable results.

This is not to say that duplication is always inefficient in performing different analysis, the second line can provide an alternative perspective which, when covering high-risk situations, can provide security and assurance. Part of the challenge of running an efficient second line function is discerning which type of duplication is appropriate in a given risk management context. However, when duplication of activities between lines is the norm rather than the exception, it does beg the question of whether resources are being used most efficiently. It is these unnecessary duplicative exercises which consume capacity from the second line that could be better exercised elsewhere, for example, to consider emerging risks.

There was consensus that the workload for managing risk was being increasingly moved to the front office; as the risk owners according to the model, which is broadly seen as a reasonable step. However, as a result of the perceived need for independent check and challenge, participants commented that the second line would feel obligated to re-perform many of these processes - and was reluctant to cede responsibility for these processes to the first line. When combined with the fact that many participants noted a potential deficiency in the business expertise of the second line to perform these functions, this meant that the first line was also reluctant to relinquish control performance.

4.4 Balance of resources

The number of resources assigned to each line of defence do not appropriately reflect the responsibilities held by them.

Given the three issues outlined above, it is unsurprising that the question of how to effectively balance resources across the three lines was vital to our first line practitioners. Many participants felt that the widening responsibilities and accountabilities of the first line-exacerbated by the prevalence of line 1B-were not being matched by a commensurate increase in resources. Participants were comfortable with the increasing responsibility, but often felt they did not have influence over the necessary budgets to execute these responsibilities. Meanwhile, in the aftermath of heightened regulatory oversight in the early 2010s, the second line function had grown in size while seeing its mandate blurred with that of the first.

Participants agreed that there were sufficient resources across the three lines to ensure risks were adequately controlled. However, achieving an effective balance between the lines was not a simple matter of transferring resource from the second line to the first. Furthermore, many participants described a reluctance to redistribute resources, or investment, from the second line to the first line - even when such reallocation could result in the elimination of inefficiencies - due to the risk of regulatory criticism.

Remedying the divide in skillset between the first and second lines was also viewed as essential by a majority of participants. Targeted hiring practices, compensation structures and investment in training were all identified as measures participants had taken. It was also noted by numerous participants that investment in technological solutions to automate and integrate processes across the lines could be an effective means of breaking down siloes - provided there was sufficient understanding and oversight of the solutions being utilised.

5. Principles

Our first line practitioners often reverted to the same idea: a need for greater clarity regarding the shape the Three Lines model ought to take. This entails not only internal coordination and formalisation on the mandates of each line, but also further guidance from the regulator. Further information around what poor and best practice looks like would address the primary pain point identified: a lack of clarity around roles and responsibilities between the first and second line.

This is not to say that the banks themselves had not taken any action. By distilling the workshop conversations, some key principles emerged which define ways in which banks can interpret and implement the Three Lines model. These principles can be used as a mirror or a checklist for firms to assess their own application of the framework and to what extent they have met these guiding standards. These principles are then used as a basis for actions which firms can take if they identify gaps. By making these changes, a clearer and more consistent application of the Three Lines model should emerge. We also note that regulatory acknowledgement of these principles as a foundation of best practice would encourage adoption amongst regulated firms.

5.1 The first and second line should have a unified risk outlook

By laying the groundwork for a robust and united risk taxonomy, the first and second line should construct their Three Lines model on the basis of a risk-sensitive consensus. This consensus should be formed around such matters as risk parameters, controls and tolerances. For instance, the first and second line should have a unified understanding of the weightings - and justifications thereof – that are assigned to different components of a Business Risk Assessment.

Adopting this principle helps not only to form clear communication lines at the outset, but also to reconcile the naturally conflicting risk appetites between the first and second lines. It is notable that we see the effects of not adopting this principle reflected in both the issues raised during the review, and our experience of performing or investigative functions on behalf of regulators. At the heart of many control environment failures is a fundamental divergence in risk outlook and approach between the first and second line.

5.2 Respective mandates for the first and second lines should be formalised and documented to ensure a common understanding of roles and responsibilities across the lines

These roles and responsibilities should subsequently be agreed upon and aligned e.g. in RACI ('Responsible, Accountable, Consulted, Informed') format. Clear and precise allocation of roles and activities in a well-documented manner will help to minimise the grey area between first and second line functions. Conducting the exercise of aligning in a RACI format will also help identify duplicative mandates and activities.

It is more than likely that there is no, singular allocation of responsibilities that can act as a one-size-fits-all; however, the aim is to provide internal certainty based on the pre-agreed risk outlook of each individual institution. This also means that merely conducting a RACI mapping within a particular line is not a sufficient measure-alignment across lines is crucial, and any allocation of responsibilities must therefore be done jointly between first and second line.

5.3 Line 1B (where it exists) can and should be made sufficiently independent of aspects of the business

Independence as a principle does not dictate that it must sit within a particular line. 1B functions can legitimately act as an independent and autonomous member of the first line, provided there are appropriate internal structures in place. It is important to note that independence of line 1B is built with respect to a particular function - this informs what we mean by 'sufficiently independent'. In order for 1 to be considered sufficiently independent from a function to be delegated supervisory tasks, it should, for example, have its compensation arrangements and escalation reporting decoupled from those of that function.

In addition to independence, Line 1B should also demonstrate the appropriate skillset to be delegated supervisory tasks. This, in turn, should allow the second line to place greater reliance on the first line performance of controls, thus offering opportunities to reduce duplication

5.4 To be effective, testing should be organised in a standard, principled way across the first and second lines of defence

To drive the standardisation of testing, the first and second line should reach a consensus on all material aspects of the testing framework-including the dataset that is analysed across all lines with respect to a particular risk. Verification or challenge should be generated through different analytical parameters and outcomes applied to this dataset; a balance must be struck between testing being checked or challenged through exact duplication of the process, and through being performed in a vacuum without regard for the process that is being checked. Where appropriate, the first line can perform testing provided it can demonstrate independence in carrying out that testing. However, the second line should also have a mandate to verify control efficacy through conducting its own testing in line with the factors outlined previously. The third line should assess and validate independence of the testing process, as well as its effectiveness.

5.5 The requirement of the second line to be independent from the business function should not preclude the second line from performing an advisory role for the first

Advising the business function is considered a powerful second line value-add, and it is important to note that the ideas of independent challenge and advisory are not mutually exclusive. The second line should look to expand its advisory function to include regulatory horizon-scanning and identification of emerging risks - this was an area which many participants viewed as a weakness in their firms.

5.6 Duplication of tasks between the first and second line should be minimised

If duplication is deemed to be necessary, it should be pre-agreed amongst the appropriate business, process and risk owners- with an overarching view that duplication is the exception rather than the norm. Participants agreed that some level of duplication can ensure that no gaps are left unchecked for high-risk areas.

However, if multiple processes are repeated dis-proportionately by both the first and second line, inefficiencies are created which eat into other important roles played by both functions. Banks should focus on developing a consistent understanding of the end-to-end processes and controls and work collaboratively to minimise duplications.

There is no singular solution for every bank regarding which tasks should and should not be duplicated - it is up to individual first and second line teams to draw from the consistent risk taxonomy they have created and build a system that works for them.

5.7 Policy owners should consider the end-to-end execution, implementation and testing required to make a policy effective

Creating a policy that does not keep in mind the efficacy of its execution wastes time both for those who write it and those who attempt to implement it. Participants indicated concern regarding an overzealous and gold-plated approach to policy setting.

This is characterised by insufficient engagement and dialogue with stakeholders to understand how to effectively implement the policy and achieve the desired outcomes in an effective and proportionate manner. This can lead to an overly complex set of rules and testing requirements which are not commensurate with the underlying risks that the policy is looking to mitigate. Such policies can also extend beyond the risk parameters within which the firm wishes to operate - which can be partially alleviated through adherence to principle 5.1.

5.8 The allocation of resources across the three lines should be reviewed if it is deemed to be beneficial towards the aim of delivering a more robust, efficient and effective control environment.

For example, if some controls have been shifted to the first line reflecting their agreed upon mandate, it should follow that additional resources are also moved to the first line, to ensure cost efficiency. To this end, firms should consider the end to end resourcing and skill sets required to ensure the effective implementation of policies and co if that means a re-calibration of resourcing between the first and second line as a result of reduced activity now being conducted by the second line.

"Firms should consider the end to end resourcing and skill sets required to ensure the effective implementation of policies."

6. Recommended Actions

Based on the principles above, we have formulated a set of recommended actions for banks. While we have noted throughout this report that there is no universally generalisable solution to the challenges banks face in implementing the Three Lines model, the actions below act as a useful set of first steps.

6.1 Banks should perform an end to end review and cataloguing of existing risk and control activities performed by business and product.

This should include all related front, middle and back-office first and second line functions that are engaged in the design and execution of the product and business area.

6.2 Create a common understanding and transparent view of all risk and control activity.

This will ensure alignment, identify potential areas of overlap and duplication, and allow for challenge on the extent to which activity might be required and assess potential gaps or areas for enhancement.

6.3 Formalise and document the mandates for the first and second lines.

This process should include a review of escalation pathways, documenting roles and ownership for all risk, control and assurance activity along RACI principles. Moreover, the formalisation should be driven and agreed by both first and second line.

6.4 Where duplicative risk and control activity is identified, assess the rationale for it to exist. This assessment will involve asking with following questions:

- Is the duplicative activity proportionate and in line with the risk thresholds agreed for that business/ function?
- Does the duplication seek to address a shortfall in controls executed elsewhere? If so, can the root cause of the original shortfall be addressed?
- Is the duplication in place due to concerns of the integrity or competency of controls undertaken elsewhere? If so, how might that concern be addressed?
- Can the same result be achieved through assurance, challenge and/or audit activity rather than full duplication of activity?

6.5 Where a Line 1B exists, assess whether it can be deemed "sufficiently independent" of the business that it supervises, and if not, what steps could be taken to address it:

- Are the reward, compensation and promotion arrangements independent of, and de-coupled from, the business it supervises and supports?
- Do escalation pathways allow for a formal reporting of risk and control issues /metrics & MI, into the appropriate second line stakeholder groups, and are these processes agreed and documented?
- Does Line 1B have the appropriate skillsets and bench-strength to be delegated supervisory tasks, and are robust succession strategies in place for all key roles?

6.6 Assess the appropriateness of resourcing and skillsets deployed against risk and control activities across both first and second line.

This should be done in parallel with the end to end review and cataloguing mentioned above. Where the review indicates a change in roles or activity performed by a function, consider whether upskilling or resource reallocation is required.

6.7 When establishing new policies and procedures, or making substantive changes to existing ones, ensure that these are designed from an end to end perspective, with engagement and input from all stakeholders across both first and second line that are potentially impacted by the policy.

This will ensure clear understanding of the rationale behind them, their alignment to the risk principles and tolerances of the firm, and the expectations and obligations of the impacted stakeholders. Policy creators should seek input on both the design of risk and control requirements to monitor adherence to them - including potential challenges or constraints to their execution - and agree proposed strategies to address or mitigate them.

6.8 Agree and document a standardised testing methodology.

This methodology should be clearly documented with input from first and second line and approved by both lines. In particular, the methodology should cover the identification of standardised datasets and systems with respect to particular risks, and clarify the type and/or extent of duplication that is proportionate to the risk appetite of the firm.

Historic and embedded perspectives on the 3LoD

Executive Summary

1. Introduction

1.1 The First Line Business Controls Working Group were asked to re-examine the principles and actions that flowed from the 'The 3 Lines of Defence: A view from the First Line' report that was published in 2021 (the '2021 Report').

1.2 Members of the Working Group were asked to participate in a survey (the 'Survey') to assess how far the principles and actions articulated in that report had been embedded in their organisations, with a view to alleviating the 4 key 'pain points':

a) Lack of clarity in roles and responsibilities of the First Line

b) An ambiguous Second Line mandate

c) Duplication of activities and inefficiencies

d) Balance of resources across the lines

1.3 This document summarises the collective opinions expressed within the Survey.

2. Key messages arising from the Survey

2.1 The responses to the Survey tentatively suggest that respondents continue to perceive the 4 pain points as such and agree with the recommendations in the 2021 Report.

2.2 The Survey highlights, however, that little progress has been made by respondents expressed in implementing actions to remedy those pain points. For example, there were only a handful of instances where more than [50%] of respondents considered specific principles or actions to be fully embedded in their operating model and none where more than [75%] of respondents agreed with that sentiment.

2.3 Reasons for this appear to be linked to:

a. **The size of the challenge facing respondents:** The issues highlighted by the 2021 Report and explored further in the Survey stem from fundamental structural challenges inherent in the application of Three Lines of Defence model to complex and evolving operating models.

b. Lack of clarity and agreement, across stakeholders, as to what good looks like and how changes might be implemented. Opinions remain, for example, on the topic of 1B teams – in relation to which some respondents feel overwhelmingly positive whilst others had categorically discounted it as a feasible model.

c. **Resourcing:** The Survey shows that practitioners have been unable to resolve the resourcing challenges that were identified in the 2021 Report. Widening responsibilities in the First Line still have not been matched by a commensurate increase in resources. Only a handful of respondents [6] felt able to agree that an assessment of the appropriateness of resourcing and skillsets deployed against risk and control activities in the First and Second Lines was fully embedded in their operating models. Perhaps even more alarming is that fewer respondents [5] felt able to agree that the principle of the reviewing the of allocation of resources to deliver an improved control environment had been fully embedded.

Survey participants felt these issues strongly. Respondents commonly raised concerns that resourcing was considered in each of the three lines in isolation and that a perceived resource imbalance between the First and Second Lines was a cause of tension.

a. The diverse regulatory approaches to the Three Lines of Defence model make it hard for industry best practice to emerge and facilitate change.

b. The existence of other pressing items on the respondents' change agenda. Responses to Covid, including adapting to changing ways of working, along with the war in Ukraine and an increasingly bleak economic environment have all occupied bandwidth within the COO community over the last 18 months and will continue to do so. One respondent noted that "[…] often we are fire fighting and responding, and not given the time or budget to really set ourselves up for success."

3. Other issues identified by the Survey

3.1 The Survey also identified a small number of issues (i.e., topics in relation to which respondents expressed particularly low levels of confidence and/or polarised strongly polarised opinions).

3.2 These issues predominantly relate to the importance of commercial awareness in the Second Line are somewhat linked to the key messages highlighted above and will inform future work on this topic (see Section 4 – Next steps below).

a. Respondents felt that the Second Line often failed to consider the viability of policy implementation and execution in the context of commercial operations and failed to apply a commercial lens to cost benefit analysis in risk mitigation.

b. Respondents expressed similar concerns about the lack of emphasis placed upon risk tolerance and appetite by the Second Line when considering taxonomies/risk management frameworks.

c. The theme also appeared to inform responses regarding the Second Line's advisory role, where respondents felt that horizon scanning was overly focused on the regulatory landscape to the exclusion of other risks facing the business.

d. Respondents also questioned whether enough Second Line colleagues had the skills and experience to be able to perform advisory roles effectively.

4. Next steps

4.1 The results set out in this report suggest that practitioners feel increasingly confident in what they are working towards in the implementation of the Three Lines model but are less clear on how to get there and that greater assistance would be welcomed in this area.

4.2 Our work so far has made it irrefutably clear that there is no universally applicable solution to the challenges that institutions face in implementing the Three Lines of Defence model. Nonetheless, some challenges seem more fundamental than others. While we have seen some tentative progress in addressing the other 3 pain points, the challenges concerning the balance of resources across the lines seems particularly entrenched.

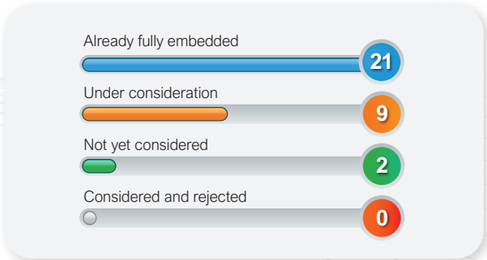
4.3 In an effort to move the discussion forward, we are proposing further engagement with the Working Group during the second half of 2023 to identify principles for suitable operating models to address the 'pain points' and create a foundation for best practice.

Survey responses: Principle

Q1: The first and second line should have a unified risk outlook

By laying the groundwork for a robust and united risk taxonomy, the first and second line should construct their Three Lines model on the basis of a risk-sensitive consensus. This consensus should be formed around such matters a risk parameters, controls, and tolerances. For instance, the first and second line should have a unified understanding of the weightings — and justifications thereof - that are assigned to different components of a Business Risk Assessment.

Adopting this principle helps not only to form clear communication lines at the outset, but also to reconcile the naturally conflicting risk appetites between the first and second lines. It is notable that we see the effects of not adopting this principle reflected in both the issues raised during the review, and our experience of performing or investigative functions on behalf of regulators. At the heart of many control environment failures is a fundamental divergence in risk outlook and approach between the first and second line.



Comments:

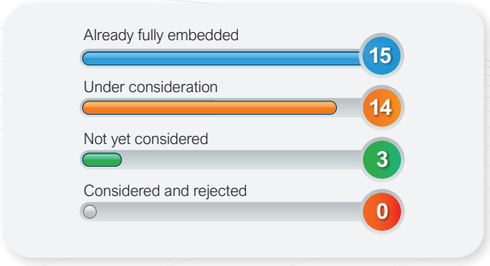
1. The implementation of a risk taxonomy is inherently impacted by the difference in views between 1LOD / 2LOD around risk tolerance. The 1LOD has a risk appetite and a sense of commercial viability that is factored into its construction of a risk management framework. The 2LOD does not factor appetite or tolerance into their views.
2. We work well with our second line risk partners most of the time. It would help if sometimes had a better understanding of our business, as they can be generalist's.
3. Partnership in place for control design and setting parameters and tolerances in a number of areas but not fully embedded in all areas.
4. Common risk taxonomy, control inventory and assessment framework.
5. Although there is regular review and challenge of top risks, ICBCS does not have a fully unified nor embedded consensus on risks between the 1st and 2nd lines. Given the independence, we'd expect some divergence.
6. Embedded in design and taxonomies, inner and outer thresholds of risk appetite measures are agreed across LODs, etc. That isn't to say that disagreements on materiality don't arise, but the framework is generally agreed, and the goal is to align on measures and weightings and significance of risk.
7. Although fully embedded, it is a topic of continuous assessment and improvement to ensure efficient process and communication flow.
8. Occasionally different interpretations of risk parameters occur through RCSA between 1st and 2nd line, however the framework adopted to guide 1st and 2nd line is unified.
9. We have an agreed risk taxonomy. We are transitioning to risk appetite being set and owned by the first line. Risk tolerances and appetite are in the process of being established in the first line and agreed by the second.

1. Whilst we do have a consistent Framework our compliance risks will no longer be assessed by the business as part of their 1LOD RCSA, instead Compliance will be undertaking their own assessment (All very new for Q3 2022 so outcomes TBD).
2. In Europe, Controls are largely operated by the second line on behalf of the business so there is no divergence. Where first line operates controls - these are fully aligned with second line. This work well for a small firm, but we may have to reconsider if we grow a lot in Europe.
3. Unified approach anchored to Risk Management Practice Framework.
4. Cross-functional engagement across the 3-lines is very strong, leading to high levels of collaboration, assisted in part by size and proximity of the organisation.
5. 1st, 2nd and 3rd line share their respective risk outlooks but do not necessarily or always converge on the risk ratings (which is reasonable given independence).
6. Partially.

Q2: Respective mandates for the first and second lines should be formalised and documented to ensure a common understanding of roles and responsibilities across the lines

These roles and responsibilities should subsequently be agreed upon and aligned e.g. in RACI ('Responsible, Accountable, Consulting, Informed') format. Clear and precise allocation of roles and activities in a well-documented manner will help to minimise the grey area between first and second line functions. Conducting the exercise of aligning in a RACI format will also help identify duplicative mandates and activities.

It is more likely that there is no, singular allocation of responsibilities that can act as a one-size-fits-all; however, the aim is to provide internal certainty based on the pre-agreed risk outlook for each individual institution. This also means that merely conducting a RACI mapping within a particular line is not a sufficient measure – alignment across lines is crucial, and any allocation of responsibilities must therefore be done jointly between first and second line embedded but still a way to go to get a robust and united taxonomy.



Comments:

1. Fairly well implemented.
2. Roles and responsibilities between 1LOD / 2LOD are in various states of maturity depending on the specific risk factor. The Financial Risks have mature roles and responsibilities defined. However, the non-financial risks are still undergoing processes to clearly define roles between 1LOD and 2LOD.
3. We have clear accountabilities, and each executive has a statement of accountability which clearly outlines what he or she is accountable for.
4. Roles and responsibilities are clear in some areas but not in all areas.
5. Business Management and Control has drafted a team charter aimed at better defining roles and responsibilities in the COO and Control function and there have been similar approaches undertaken by 2LOD. These are not standardised and therefore cannot be considered embedded within our operating model, but we continue to deliver continuous improvement which could lead to a RACI style approach over time.
6. More clear in some areas than other. Generally clear in principle but confusion can arise in the details as to where to draw the line on setting standards (2nd line) and execution/how to implement (1st line).
7. Similar to previous question, this is formalized and documented, but at times, resource constraints affect the ability to fully implement these Roles and responsibilities without issues arising from time to time.

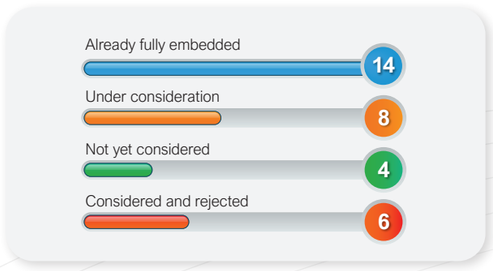
While roles and responsibilities must be agreed and documented, they must also be flexible enough to enable business growth in a dynamic market and geopolitical environment.

8. We are currently working to move more responsibilities to the first line, such that second line become a pure assurance function. For instance, this would mean first line risk setting policies and standards for the business to comply with. This in turn for instance would mean first line risk hiring compliance experts, cyber experts, to translate regulation, set policy and define standards. Currently this is done by the second line.
9. Some trader mandates are in place, but very immature, other lines mandates are unclear and undocumented and it's difficult to gain buy in to prioritise this.
10. Roles are clearly defined but not in RACI format.
11. There could be formal documentation for some but not all areas but there would always be a common understanding between both lines, and this could be communicated through meetings, emails etc.
12. Progress has been made, questions around value of formally documenting, thereby possibly creating another cottage industry, opposed to a clear understanding that already exists are being resolved.
13. We have started to embed Firstline Controls but respective mandates between 1 and second line should be more formalised and documented still.

Q3: Line 1B (where it exists) can and should be made sufficiently independent of aspects of the business

Independence as a principle does not dictate that it must sit within a particular line. 1B functions can legitimately act as an independent and autonomous member of the first line, provided there are appropriate internal structures in place. It is important to note that independence of line 1B is built with respect to a particular function – this informs what we mean by 'sufficiently independent.' In order for 1B to be considered sufficiently independent from a function to be delegated supervisory tasks, it should, for example, have its compensation arrangements and escalation reporting decoupled from those of that function.

In addition to independence, Line 1B should also demonstrate the appropriate skillset to be delegated supervisory tasks. This, in turn, should allow the second line to place greater reliance on the first line performance of controls, thus offering opportunities to reduce duplication.



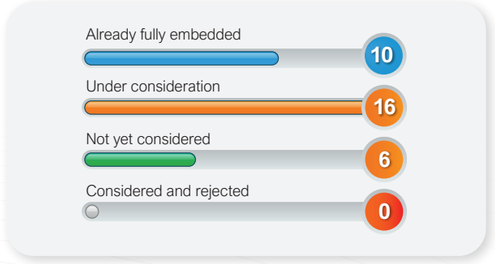
Comments:

1. COO Office for Trading is reporting to Global COO of Markets, not to Global Head of Trading.
2. Current level of independence is appropriate.
3. The idea of a 1.5 / 1b line has been rejected. The 1LOD risk and controls team that sits within the 1LOD clearly sits within the business. There is no attempt to generate some sense of independence between that team and the business. We have found that trying to create this additional layer is what causes the confusion and blurring of Roles with 2LOD. Instead, we have adopted a framework that re-enforces that the 1LOD risk and controls team is truly part of the business.
4. First line controls is sufficiently independent of the business, with a direct reporting line into our divisional CEO. The pay structure for 1B is different, with more base and fixed pay and less variable.
5. Examples: Market surveillance and AML checks.
6. Line 1B exists but within the IB does not perform delegated supervisory tasks but instead work to enable via data, systems and process the supervisors to be able to perform efficiently.
7. The line 1B function ultimately reports up to the Head of Global Markets. Given our scale, there are no plans to change this model.
8. There is no such thing as 1B. It is a failed concept as it provides neither 1LOD or 2LOD benefits. It is a sign of a firm that has not gotten comfortable with the way the 1st line will choose to execute its responsibilities, which may include delegation and internal R&R definitions where accountable executives (i.e. business CEOs) drive the tone from the top through the 1st line risk and control teams.
9. This function does this within Global Markets division, reporting lines are via GM COO into Head of Global Markets. In this case, it is independent from heads of Trading and Sales management.
10. The NFR is part of the business.
11. Mixed model of independence depending on the aspect of 1LoD under consideration.
12. First line risk management is aligned under the COO. This can create a conflict of interest where the COO's key explicit performance measure is profitability, the components being to maximise revenues and minimise cost. Business restrictions to bring risk within tolerance may therefore be overlooked, or short cuts on remediation made in the name of cost. First line risk management should be aligned under the SMR of the business, as they have a vested interest to limit their personal liability and will make decisions that are overall more rounded. Risk management can be seen as a tick box exercise by others. Something that we have to be SEEN to be doing, versus in substance ensuring the foundations are secure as a primary goal.

1. It's not that its under consideration - it's in place but it's not working well. Primary reporting lines are to the Risk function globally (NOT regionally), but local matrix lies are to the business. So, for independence on compensation etc. it works, but in practice some risk functions are almost too defensive of the business and its control environment and do not challenge them - it's a cultural issue in my opinion (My opinion may SIGNIFICANTLY differ here to the other State Street respondent in this regard...). I feel strongly that the skillset for Control operation is not where it needs to be, and our Supervisory Framework is not robust/well embedded. We do not have specific control operation functions.
2. Where we have Line 1B they are independent. Team in 1B and second line are highly skilled and experienced.
3. Line 1B is centralized under the Markets COO, and generally operates independently from the sales and trading desks. Escalation and compensation, however, are not independent from the business overall.
4. There is currently no firm 1B formally recognized - there should be in my opinion due to the evolution of the oversight model.
5. To be considered in light of size and complexity of business to ensure not adding an unnecessary level of bureaucracy as opposed to a beneficial control framework, that is already in situation.
6. Embedded to the extent that it can be while 1st line controls is still part of the 1st line business (as it should be).

Q4: To be effective, testing should be organised in a standard, principled way across the first and second lines of defence

To drive the standardisation of testing, the first and second line should reach a consensus on all material aspects of the testing framework – including the dataset that is analysed across all lines with respect to a particular risk. Verification or challenge should be generated though different analytical parameters and outcomes applied to this dataset; a balance must be struck between testing being checked or challenges through exact duplication of the process, and through being performed in a vacuum without regard for the process that is being checked. Where appropriate, the first line can perform testing provided it can demonstrate independence in carrying out that testing. However, the second line should also have a mandate to verify control efficacy through conducting its own testing in line with the factors outlined previously. The third line should assess and validate independence of the testing process, as well as its effectiveness.



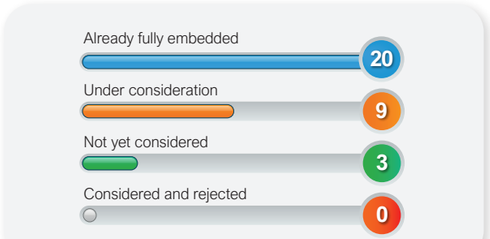
Comments:

1. The control testing framework has been clearly defined and embedded. All three lines of defence fully understand their roles.
2. At present we have some overlap between 1st, 2nd and 3rd line. We have tried to delineate this by saying the 1st line has a monitoring and control role, which is BAU activity, the 2nd Line assurance teams do independent thematic reviews and audit continue to perform independent audits on behalf of the board. We have also instigated a consolidated 2nd and 3rd line assurance and audit plan, to avoid duplication.

1. 1LoD Assurance testing and Compliance testing are in place (along with other 2LoD reviews) but not fully aligned in terms of risk based scope and approach with the business.
2. 1st Line testing performed alongside 2LoD testing and things like SOX. Challenge is both a growing volume of key controls to test, shortened time frame within which to test and the increased standard that testing needs to follow (e.g. SOX level).
3. There are scheduled reviews and testing delivered by 2nd and 3rd LOD i.e. compliance, operational risk assurance and assurance / unrated audit work. 1LOD performs testing of certain controls, particularly dealing room controls governing sign offs, bestex and other key front office controls.
4. Coordinating and collapsing testing activities is still a challenge. Regulatory expectations drive a “more is always better” approach and it take maturity and credibility to start rationalizing.
5. 1st Line control testing, not fully in place. 2nd Line is in a better place and do have continuous testing across 1st line processes and controls. More work needs to be done to effectively test within 1st line. Audit is also in a position to do its independent testing and validation of these controls and processes.
6. Not clear on the value of second line testing, if there is first line testing and internal audit.
7. First question should be ‘why’ are we testing in order to stop doing legacy box ticking. Then, for items we agree are critical to test, we should ask ‘how’. we must get away from needing humans to do testing. By using machines as much as possible, we free up humans to add value to the purpose of testing - to identify what’s not working and fix it.
8. Control testing is performed on a monthly/ quarterly basis as part of BAU by the first line risk management function. A more fundamental question on the control testing is firstly are the controls even effective or are we taking false comfort in green light controls that actually don’t make a difference. Putting the effectiveness of controls to one side, I find Audit has professional methods of testing and assurance based on data sets, and structured analysis. However often second line appear to be hit and miss. I am often confused as to why a certain area has even been selected for review. Second line need to ensure they share their methodology for areas being tested/reviewed. Third line being trained experts in reviews should set the methodology/ practices to be applied across all reviews to ensure quality of reviews.
9. 1st and 2nd line testing functions are now more aligned on WHAT will be tested to avoid duplication, but they are not using the same frameworks nor datasets - teams in both lines are very small so the focus is on testing as many areas as feasible (NOT on a risk based approach but now aligned to Critical business functions as priority).
10. 1L performs testing, but it is less formal than 2L testing and not relied upon by 2L testing. It serves as an internal “maintenance” and early warning vehicle.
11. Control testing is embedded but the standardized and communicated cross functional approach is less formal.
12. No operating model has been implemented for robust testing. Control self assessment framework only in place but not yet operational. Some 2nd line assessment is performed but 2nd line framework is not harmonised at all with that framework used by 1st line.
13. Generic testing approach is well co-ordinated and managed across the first two lines and infrastructure allows for the application of a standardised and consistent data set.
14. Different testing approaches - some discussion on avoiding duplication and being efficient but 3 lines model is an impediment to standardised, shared testing.
15. 1LOD testing has been withdrawn due to the intensive nature of 2LOD testing underway - in fact 2LOD testing is viewed as overly burdensome and duplicative in certain areas, much of this driven by local regulatory requirements.

Q5: The requirement of the second line to be independent from the business function should not preclude the second line from performing an advisory role for the first

Advising the business function is considered a powerful second line value-add, and it is important to note that the ideas of independent challenge and advisory are not mutually exclusive. The second line should look to expand its advisory function to include regulatory horizon-scanning and identification of emerging risks – this was an area which many participants viewed as a weakness in their firms.



Comments:

1. Partly embedded.
2. 2LOD has evolved into an oversight function that reviews & challenges the work performed by the 1LOD. This role includes providing proactive guidance, where applicable.
3. The 3LoD model is quite immature in Australia, so we are going through the process of where the 2nd LoD are trying to find their feet. In order to provide that advisory role, they will need to upskill the teams. Pre the 3LoD model in UBS 20 years ago, I think we had better 2nd LoD people who were independent, but also provided advice on how to do business more safely i.e. I am not sure the whole 3 LoD model has helped.
Not sure. Some 2LoD teams are reluctant to provide advisory as it conflicts with challenges, others are more comfortable with doing both.
4. Partly done but depends on the 2LoD function, the org structure and individual personnel and their willingness to operate in this manner.
5. Compliance advisory teams are split out from those doing the testing and truly operate in this capacity including current and emerging prudential risks.
6. Agreed in principle especially for compliance professionals to be both advisory and provide challenge - in operation different individuals are better at this than others; it can create confusion for some individuals.
7. Although fully embedded, the horizon scanning aspect of the function needs further improvement beyond the current focus on regulatory landscape component. A focus on other areas of risk to the business needs improvement.
8. Clear from P+P but not always evident from the way individuals in the second line perform their roles. Also, not always aligned with regulators expectations.
9. Area of debate and not fully embedded. A cyclical journey, 2LoD did have advisory capability, then moved to check and challenge only, potentially results in lost capability. Advisory capacity under review.
10. Need an optioned in responses to say partially embedded. Areas of 2nd line risk are at different levels of maturity. Some areas have the skills, knowledge and talent to advise, others would like to be able to advise as well as challenge but are not yet mature enough to do so.
11. We have an advisory function and also a horizon risk scanning team and committee. However, I do not see why advisory needs to be independent. Advisory (being deal advisory) would be better placed sitting within the business working with the desk heads.

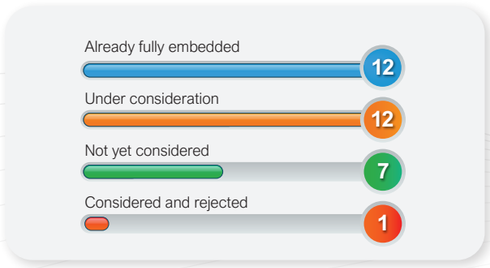
13. Our Compliance SLOD are really only Advisory in the GM compliance function. There is then a separate testing function at the Legal Entity level testing core compliance risks. There is a weakness in horizon scanning and emerging risk.
14. However - the propensity for the 2LOD to provide advise whilst on paper exists in practice is eschewed by the 2LOD.
15. The degree to which this is done is different between various 2nd line of defence functions.
16. Close alignment and strong co-operation allows for second line to act in an advisory function across all aspects of second line functions, very much operate in a healthy collaborative manner.
17. Generally, the case but can be individual or group dependent - some 2nd line groups are more reluctant to be advisory than others.

Q6: Duplication of tasks between the first and second line should be minimised

If duplication is deemed to be necessary, it should be pre-agreed amongst the appropriate business, process and risk owners – with an overarching view that duplication is the exception rather than the norm. Participants agreed that some level of duplication can ensure that no gaps are left unchecked for high-risk areas.

However, if multiple processes are repeated dis-proportionately by both the first and second line, inefficiencies are created which eat into their other important roles played by both functions. Banks should focus on developing a consistent understanding of the end-to-end processes and controls and work collaboratively to minimise duplication.

There is no singular solution for each bank regarding which tasks should and should not be duplicated – it is up to individual first and second line teams to draw from the consistent risk taxonomy they have created and build a system that works for them.



Comments:

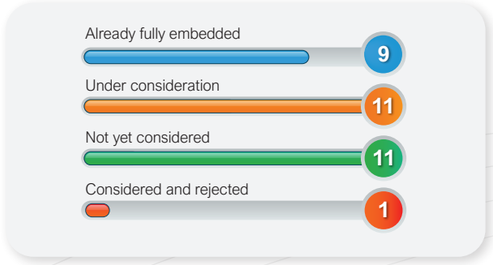
1. Duplication of tasks depends on the specific risks - some are more advanced and clearly defined than others.
2. As our 3 LoD model evolves we will get more efficient, but ideally, I don't think there should be any duplication.
3. Majority of controls are performed in the 1LoD, but this has evolved organically rather than clearly documented by generic and specific policy statements.

1. Duplication in surveillance, testing and in some reporting but can be impacted by org structure, change of leadership and also regulatory pressures.
2. Effort is taken to co-ordinate operational risk assurance, compliance testing and internal audit to avoid thematic duplication or gaps. 1LOD has a voice and can influence the thematics, especially if aligned to top risks.
3. Largest challenges surround legacy Compliance activities where surveillance needs to mature to a utility that supports both supervision/front line control and second line oversight/monitoring.
4. Getting better due to cost pressures.
5. Reduction in duplication continues to be a focus.
6. Same comment about maturity level across areas of risk.
7. This problem is amplified when the lens applied is a process one and/or there is a matrix org structure with country/regional priorities vs group/global. The solution is to look at it from a risk lens end to end. The PO process owner of where the risk materialises manages the end to end risk across all upstream processes. Second line more to a pure assurance role to allow first line to be held accountable for risk management.
8. Only testing has really been duplicated and this is reducing as topics are aligning - the compliance function does not operate or oversee (monitoring) controls so there is no duplication as it's all in FLOD.
9. Duplication is relatively low, though perhaps not well-understood where it does exist.
10. Nice in principle but without the formalized coordination and RACI - difficult to control.
11. There is significant duplication. Please see the previous example of testing 'self assessment.
12. Continually under discussion to ensure tasks reside in the most appropriate area and duplication is avoided, again benefited by the size of the organisation and proximity of teams.
13. Considerable overlap built into the model.
14. Duplication of processes is rejected as much as possible unless mandated by a regulator.
15. The duplication of tasks is still an area where improvement can be made.
16. Primary focus has been on the handover from 2nd line to 1st line. There hasn't been any organised effort to review duplication.

Q7: Policy owners should consider the end-to-end execution, implementation and testing required to make a policy effective

Creating a policy that does not keep in mind the efficacy of its execution wastes time both for those who write it and those who attempt to implement it. Participants indicated concern regarding an overzealous and gold-plated approach to policy setting.

This is characterised by insufficient engagement and dialogue with stakeholders to understand how to effectively implement the policy and achieve the desired outcomes in an effective and proportionate manner. This can lead to an overly complex set of rules and testing requirements which are not commensurate with the underlying risks that the policy is looking to mitigate. Such policies can also extend beyond the risk parameters within which the firm wishes to operate – which can be partially alleviated through adherence to principle 5.1.



Comments:

1. Policies are implemented by 2LOD who often do not consider the viability of implementation. This point creates the basic conflict between 1LOD and 2lOD risk and control teams.

2. Our organisation is immature in this respect. Our 2nd LoD policy owners do not consult the business well/ early enough and they don't apply a risk v cost commercial lens to what they are writing. As a result, we get gold plated detailed procedural type, rather than principles based policies.

3. Policies tend to be aspirational and not always aligned to an agreed operating model and control environment to enable compliance.

4. Work on policy framework underway to create a more structured approach with improved consultation but we still have a fragmented policy environment and some issuance lacking consultation with all relevant stakeholders.

5. The principle above is well understood and effort is taken to ensure that policies are operationalised. There is, however, room for improvement either due to the sheer volume (300+) or cases where the level of detail is not consistent and can lead to over engineered policies which are difficult to implement.

6. Front line input into Policy issuance is an agreed need, but often poorly executed in practice, leading to the problem laid out in the principle. A senior committee or even Board sub-committee can be used for approval of Policies to give a "vote" to both LODs, but this is not yet in practice.

7. Regional/Local Policy process does follow the approach described above. Global or home office policies tend to have gaps in implementation and soliciting feedback ahead of finalizing them.

8. An area of continued debate and challenge. There continues to be vertical policy owner control cascade for specific risk types in the risk taxonomy with horizontal business process risk controls augmenting centralised policy controls. Challenges are raised with at times, over complicated/over zealous vertical control cascades.

9. Process are not yet fully mapped which is a prerequisite for end to end policy and testing implementation This mapping is currently being completed.

5. I agree with the statement, but responses don't seem to make sense. The point here seems to be around the ability of banks to operationalise a policy. This is becoming more impactful as data and technology infrastructure plays a bigger role in operationalisation.

6. That is why policy setting needs to move away from the second line to the first line. Also, policies need to be set across risk rather than process, as there are often overlaps e.g., Fraud policies will be managing the same risks in many instances as Cyber. e.g. payment gateways, yet we can end up with two different policies with two different requirements but managing the same risk.

7. Policy implementation is largely left to the first line of defence. Whilst there is some representation of FLOD in policy working groups there is little guidance or thought from policy owners on practical application and no thought on testing that I am aware of.

8. Policy owner's sensitivity to execution is inconsistent and not formally codified as a key responsibility.

9. However - the current environment and dare I say it, a lack of commerciality in the various LODs means a natural tendency to over control and be overly conservative in the interpretation of regulatory compliance. The concept of zero tolerance for any form of regulatory breach.

10. All new policy discussion and review of existing ones is a co-ordinated process across relevant functions with opportunity to review/comment from interested parties as well.

11. Not always in place effectively.

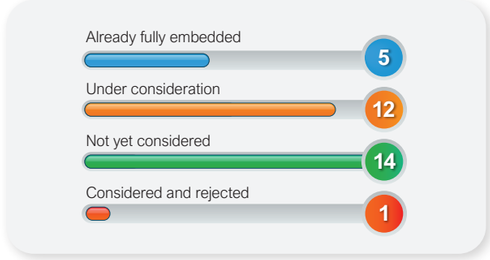
12. This is an ongoing issue created by 2LOD.

13. Stakeholder communication can be further improved when considering / designing and/or implementing policies.

14. 1st line is consulted with draft policies and process and control implementation is consideration prior to finalisation.

Q8: The allocation of resources across the three lines should be reviewed if it is deemed to be beneficial towards the aim of delivering a more robust, efficient and effective control environment

For example, if some controls have been shifted to the first line reflecting their agreed upon mandate, it should follow that additional resources are also moved to the first line, to ensure cost efficiency.



Comments:

1. Resources are often considered in a vacuum (e.g., does 1LOD or 2LOD have the right resources), but has not yet been evaluated for re-allocation between the lines of defence.

2. Everybody looks at their resourcing in isolation. Some responsibilities move from the 2nd to the 1st line, but it is very unusual to move the headcount, which creates inequity and creates tension.

3. Some focus on this, but not working fully with 2LoD tasks moved to 1LoD and not always with resource.

4. Tasks and responsibility moving to the first line but often without resources and in addition the resources previously performing them are then redeployed onto more 2LoD activity (challenge, review) which can also induce demand on the 1LoD.

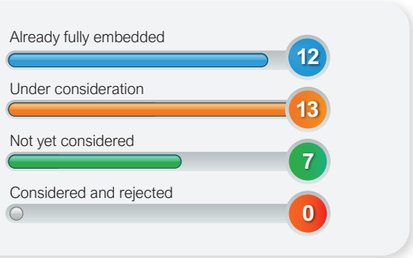
5. Area of continuous assessment and conversations with senior management. Not fully there across 3LOD functions.

6. Each group assesses its staffing needs, but activities do not necessarily move with resources in many cases, particularly because the “sending” unit often is anticipating other activities it will continue or begin performing.
7. Like many banks on the street, we would strongly argue that there is a significant resource imbalance between 1LOD and 2nd / 3rd. To address this, 1LOD constructively challenges both lines. We don’t see fungibility between the lines and haven’t, to date, moved resource from 2nd or 3rd to 1st line.
8. Not considered when 3LoD implemented.
9. The above statement makes sense and is rather obvious in my mind. Shift resources with the work from second to first line. First line risk will be incentivised to maximise risk buy down per resource and drive pragmatic solutions.
10. This is an area we have significant issues in. Almost all controls moved to FLOD without resource and then SLOD cut resources also so it’s not necessarily a case of recalibration but of right sizing the resource pools in both lines, especially outside of the US.
11. Resourcing is the key sticking point - tangential but in the example of APAC CDO - zero resource allocations provided.
12. Resourcing is planned separately by the three defence lines. No end to end view considered.
13. Never an easy set of discussions to reach agreement, but generally feel right outcomes are reached, noting that due to size and nature of business, the instances of such moves is relatively infrequent.
14. Although there is an increase in the transfer of controls to the first line this does not automatically lead to a re-allocation of resources.
15. This is considered on a case by case basis. In general, though, my experience is that resources are not moved but are reviewed and considered thematically and as part of yearly resource planning.

Recommended Action

Q1: Banks should perform an end to end review and cataloguing of existing risk and control activities performed by business and product

This should include all related front, middle and bank-office first and second line functions that are engaged in the design and execution of the product and business area.



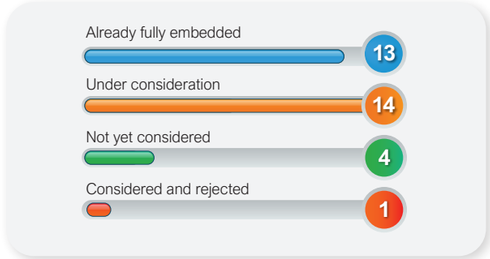
Comments:

1. We are in the process of mapping our Value Chains (E2E processes) across all our businesses and plan to be finished in 3 months. This has been a useful exercise to understand our gaps / duplication / manual processes and has helped to shape an investment case to optimise our E2E going forward. More importantly, it has created a virtual community across the 1st and 2nd LoD that support that product, who now share a common purpose.
2. Done and covered in Control inventory but complicated by frequent re-orgs.
3. This happens through a combination of the RCSA process and also the inventory on controls owned by 1LOD.
4. The RCSA creates the risk and control catalogue / inventory - it is not done by function.
5. Not fully implemented yet, but definitely in the execution phase and therefore beyond just “under consideration”.

1. The task is something that all of us know is critical - this is the WHAT. The challenge is the how. With so many moving parts, having structured data sets and interlinked risks with common triggers and standard definitions is where we all want to get to. However often we are firefighting and responding, and not given the time or budget to really set ourselves up for success. Second line need to play a more active role in ENABLING more effective risk management. A big part of the Group Head of OR role should be leveraging tech to enable First Line to be able to discharge their responsibilities more effectively.
2. We don’t consistently have process maps and some areas have weak control inventories. Our control inventories are not standardised - people write their own controls, which makes it difficult to align across businesses.
3. Recent program to assess and document risk and control framework.
4. Needs enhancing and maturing - there is a library of controls but consistency / applicability / independent review / RACA etc needs enhancing.
5. The view is built based on activities and processes and does not include the product dimension as of now.
6. An existing Risk and Control Self Assessment process, which is independently managed is in operation.
7. There are many risk & control descriptions and periodic reviews have been done. However, not all risks and controls are described in detail.
8. For 1st line functions. This does not include 2nd functions. E2E is in the process of being implemented.

Q2: Create a common understanding and transparent view of all risk and control activity

This will ensure alignment, identify potential areas of overlap and duplication, and allow for challenge on the extent to which activity might be required and assess potential gaps or areas for enhancement.



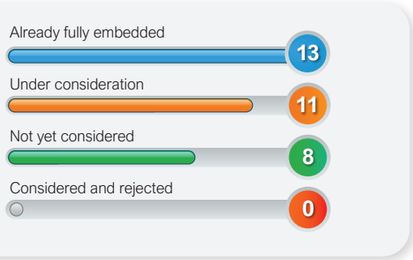
Comments:

1. No homogenised mapping across the 3 LoDs.
2. Partially embedded.
3. The Firm has implemented a centralized taxonomy of risks, controls, and impacts / likelihoods.
4. Embedded in our risk and rcsa framework.
5. Alignment is essential to avoid gaps / overlaps.
6. Lines of defence established.
7. Controls are reviewed by 2LoD and Risk & Control Self Assessment is done by 1LoD and 2LoD but not always with the lens of overlap and duplication.
8. For the main areas of potential overlap this is understood but requires bold decision making to address.
9. This is the direction of travel but, per prior answers, there is work to be done to achieve a common view.
10. Not a separate exercise - the RCSA provides the view of common risks and common controls or control types.
11. A central golden source for non-financial risk and control information exists.
12. The only practical approach has to be based on materiality.

1. We have a robust detailed risk taxonomy. So, there is a common understanding. However, the number of risks is extensive and hence creates a challenge in itself from the sheer volume. So common understanding of risk and control activity is key, however being very intentional at the outset on the level of detail and being intelligent around the structure is critical.
2. Fully embedded in line of business. Likely implemented in T&O, but not as much transparency between line of business and T&O.
3. Extensive endeavour.
4. Review of data remediation to produce a more consistent and simplified risk and control taxonomy.
5. Whilst this has been considered in control testing and is improving, control operation and oversight lies within FLOD so there is little or no duplication, but also a lack of SLOD presence.
6. Single source of truth reporting and common standards.
7. Significant progress toward this goal, but not fully mature.
8. This can best be described as work in progress.
9. Again - maturity of the model needs enhancing.
10. We have identified the key risks within our business and is evident in how we manage it. For example, our Risk and Control Self Assessment Testing is broken down by the Risk Types.
11. This is already done but at broad, macro level. It lacks the granularity to spot effective operational gaps. Building such a granular view is a challenge.
12. (A) Common understanding and transparent view of activity exists but it has not been used to review areas of overlap and duplication.
13. Risk and Controls are documented more and more but there is still no full alignment/ transparency of the activities yet across all functions involved.
14. Sometimes implicit in process mapping but not an explicit piece of work - would be valuable.
15. Again, the existing RCSA process provides this degree of transparency and understanding through both the infrastructure in place to record, as well as the forums in which discussion and challenge takes place.

Q3: Formalise and document the mandates for the first and second lines

This process should include a review of escalation pathways, documenting roles and ownership for all risk, control and assurance activity along RACI principles. Moreover, the formalisation should be driven and agreed by both first and second line.



Comments:

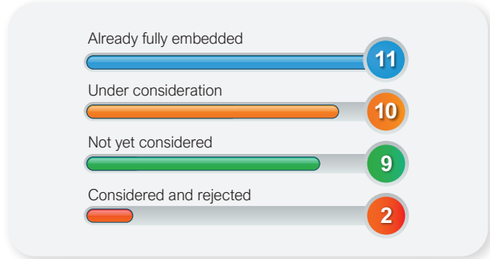
1. Partially embedded.
2. Depending on the risk type, mandates have been documented that clearly define RACI for 1LOD / 2LOD teams.
3. We have formal statements of accountability.
4. This is done but not as formally with all the points noted (e.g. RACI, escalation pathways).
5. Partially formed and embedment is work in progress.

1. The roles and responsibilities of each line of defence are defined in the risk management framework and picked up in governance documents (Policies, Charters); escalation standards and routines are laid out in the governance framework and policies that establish key risk committees and delegations of authority from the Board down into the business lines and by risk type (Market, Credit, Model). It is hard to see the need to create a detailed RACI type view of this as the framework is fairly clear and easy to apply in particular situations as they arise - there may be politics or debates that prevent it from being applied at lower levels, but that leads to discussion and escalation of disputes, and there is no lack of understanding of the concepts by the leadership/decision makers.
2. Mandates are formalised however are at such a high level they leave a lot open to interpretation. The art is in getting the mandates to the right level of detail and precision to minimise grey.
3. FLOD traders in FX have mandates (but lack of monitoring at an individual level - this is a WIP) but no other LFOD functions have it and no SLOD functions have defined mandates.
4. We may need additional documentation and RACI maps. Roles and escalation are clear. Easy in a small firm.
5. Maturity and formal consistency of RACI approach required.
6. The mandates exist but should be reviewed.
7. Applied mandates are relatively well understood, consideration around approach to formal documentation is under review.
8. Although mandates have been documented this has only been completed at a high level and there remains significant areas of greyness.

Q4: Where duplicative risk and control activity is identified, assess the rationale for it to exist. This assessment will involve asking with following questions:

1. Is the duplicative activity proportionate and in line with the risk thresholds agreed for that business/function?
2. Does the duplication seek to address a shortfall in controls executed elsewhere? If so, can the root cause of the original shortfall be addressed?
3. Is the duplication in place due to concerns of the integrity or competency of controls undertaken elsewhere? If so, how might that concern be addressed?

Can the same result be achieved through assurance, challenge and/or audit activity rather than the full duplication of activity?



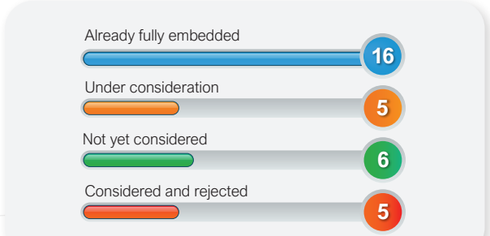
Comments:

1. Sufficiently embedded
2. A specific exercise to identify duplication has not been performed across all risk factors.
3. If we have competent people who co-ordinate across the 3 LoD, I don't see why we need any duplication.
4. Very little duplicative risk and control activity occurs - majority is in 1LoD.

5. Often the duplication is because of a historical regulatory or management decision and does not correlate with the risk involved or the underlying effort required e.g. Testing and Surveillance are two activities that are duplicated, are high effort and large in scope but proportionally highlight relatively few issues in and of themselves.
6. There have been some clear examples of duplication which have been identified and remediated along with corresponding policy, committee and procedural governance changes. Duplication between 2nd and 3rd line testing has been improved through better co-ordination of the testing and audit schedule.
7. Duplication tends to exist in areas where the controls are less mature, more manual, and accordingly there is a lack of confidence and credibility that the risk area is well-managed.
8. Tackled on a case by case basis.
9. Need some duplication and checks.
10. N/A given controls being in FLOD.
11. There is a conscious effort to not have duplicative work between lines.
12. No duplication due to being small firm.
13. No formal approach to this.

Q5: Where a Line 1B exists, assess whether it can be deemed "sufficiently independent" of the business that it supervises, and if not, what steps could be taken to address it:

1. Are the reward, compensation and promotion arrangements independent of, and de-coupled from, the business it supervises and supports?
2. Do escalation pathways allow for a formal reporting of risk and control issues / metrics & MI, into the appropriate second line stakeholder groups, and are these processes agreed and documented?
3. Does Line 1B have the appropriate skillsets and bench-strength to be delegated supervisory tasks, and are robust succession strategies in place for all key roles?

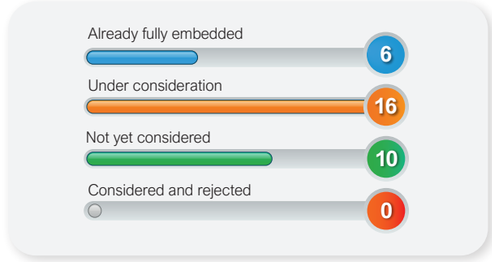


Comments:

1. The 1B team is not considered independent and is delegated the responsibility to support risk management and control evaluation by the Executive in charge of the business.
2. We have a different comp structure for 1B - higher base, more LT variable (not linked to perf) and a smaller short term variable, based on performance.
3. We don't have the scale - just a handful of people in 1B. They are very experienced but stretched thinly across GM and regionally. The skillset is good and is deployed effectively in dealing and challenging risk and control issues.
4. Line 1B does not exist - if #1 was "true," the better talent would not want to be in the function (they would feel distant from the business and may as well work in 2nd line); Q#2 has nothing to do with 1B as a good metrics program in front line will have business input and transparency to business leadership and 2nd line; for Q#3, see above re #1 (i.e. the best talent does not want to be Line 1B).
5. Line 1B not an accepted concept here.
6. As previously mentioned, I believe this should be aligned under the business head, whose priorities will be aligned to SMR and limiting personal liability and hence drive the right outcomes also for the business and shareholders.
7. 3 remains work in progress.
8. 1. Yes 2. Not SLOD, FLoD governance which feeds Corporate Governance (FLoD & Corp governance does include SLOD participants).
9. Reward and comp may not be completely separate in a few instances of 1B.
10. Line 1B work mainly on formulating guides and framework for implementing and operationalising 2nd line Policy. For example, 2nd line policy requires control assessment and line 1b develops frameworks and tools for a testing or self assessment operating model.

Q6: Assess the appropriateness of resourcing and skillsets deployed against risk and control activities across both first and second line

This should be done in parallel with the end to end review and cataloguing mentioned above. Where the review indicates a change in roles or activity performed by a function, consider whether upskilling or resource reallocation is required.



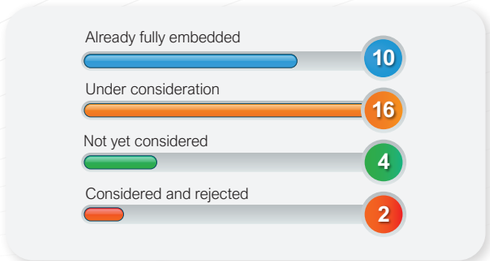
Comments:

1. Annual review of skillsets for risk and control staff is performed to ensure that skillsets align with responsibilities.
2. We are looking at skills across the 1st and 2nd line and need to bring in more product specialists, as we have too many generalist's.
3. Resourcing is considered by each function and particular focus is given to key controls - but not with a first and second line view.
4. Some areas where 1LoD required to hold expertise (e.g. Cyber) because 1st line needs to be accountable are ones where the ability to leverage IT experts as first line makes sense but org structures can complicate this if IT commonly thought of as separate to businesses.
5. We are constantly reviewing the risk profile and dealing continuous improvement in the risk framework or dealing new control requirements. There is limited capacity to add headcount to the function currently.

6. Not clear a comprehensive review would justify its cost.
7. We are in the midst of building a competency framework for different risk roles.
8. A skillset review was done in business risk only but nothing tangible appears to have come from it.
9. Constant evolution.
10. Training and/ or recruitment of staff always considered.
11. There is duplication and overlap. The matter is being addressed.
12. Given resource challenges and difficult labour market this remains an ongoing challenge.

Q7: When establishing new policies and procedures, or making substantive changes to existing ones, ensure that these are designed from an end to end perspective, with engagement and input from all stakeholders across both first and second line that are potentially impacted by the policy

This will ensure clear understanding of the rationalise behind them, their alignment to the risk principles and tolerances of the firm, and the expectations and obligations of the impacted stakeholders. Policy creators should seek input on both the design of risk and control requirements to monitor adherence to them – including potential challenges or constraints to their execution – and agree proposed strategies to address and mitigate them.

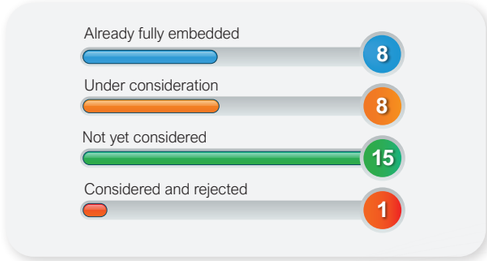


Comments:

1. Policies are established by the 2LOD and do not always consider operational viability, commercial viability, or risk appetite.
2. We are struggling to get our 2nd LoD to put in place a robust policy consultation process, to ensure the policies they write are executable efficiently and commercially, to mitigate the risk.
3. This is in place, but policies are sometimes aspirational and 1LoD is not involved sufficiently to agree split in responsibilities and whether remediation programmes are required to meet policy expectations.
4. Policy writing is getting better and is more structured but across a complex org, stakeholder engagement is not always sufficient and that can lead to post implementation discussions to address nuances previously missed.
5. This is an area of continuous improvement. There are certainly policies which could be reviewed, streamlined or better operationalised. Some standardisation is required as policies come due for review.
6. Work in progress - agreed in principle but often executed poorly.
7. Policies are written at the Enterprise level in corporate areas. 2nd lines, which are part of corp areas vary in maturity. While many have processes for engagement as described, others are not mature enough.
8. What is stated above and in many of the previous principles is WHAT, and I cant see anyone disagreeing. The challenge isn't the What it is the HOW.
9. End to end is not considered as many are corp wide encompassing very different businesses (not just GM but Custody etc.) therefore whilst FLOD is involved in some policy discussion, its left to FLOD teams to implement.
10. Largely considered.
11. Maturity review required.
12. This action is in early stage development. Step one is document the end to end view.
13. This is best practice - not always achieved in reality.
14. 2LOD consistently fail to consider the resource implications or practicality of policies they publish.

Q8: Agree and document a standardised testing methodology

This methodology should be clearly documented with input from first and second line and approved by both lines. In particular, the methodology should cover the identification of standardised datasets and systems with respect to particular risks and clarify the type and/or extent of duplication that is proportionate to the risk appetite of the firm.



Comments:

1. Testing methodologies are clearly defined across all three lines of defence.
2. Our testing could do with some standardisation, so we need to look at this in the future.
3. In place, but insufficient dialogue between 1lod and 2LoD.
4. Testing has been discussed as there are too many controls to test to too high a standard for it to be done with lack of common standards, across competing framework and LoD and in duplicate. However no immediate success in gaining agreement on how this should work. Testing is very duplicative and there is no agreement on which group should defer to the other or "stand down" - regulators seem happy to have multiple testing types and approaches over the same risks, making rationalization difficult to sell.
5. Not clear the value this would add.
6. This is needed but has not been discussed internally as far as I am aware.
7. FLOD and SLOD testing are separate processes globally, FLOD is aligned to critical business services, SLOD is aligned to top compliance risks at the legal entity level.
8. 9. We do not have standardised testing methodology.
9. 10. A standardised testing / assessment framework has been developed by line 1B. It's has been well received by 2nd line but not yet enshrined in a formalised policy.
10. 11. No formalized documentation but we do align both first and second lines in terms of outcome and approach.

7. References

Appendix: Methodology

We began by conducting a total of 29 interviews with first line representatives from banks across America, Europe and Asia-Pacific. The aim of these conversations was to uncover each participant's experience with the Three Lines model and expose any problems they may have encountered.

We then ran a series of workshops with a number of first line representatives, many of whom had also been interview participants. The purpose of these workshops was to initiate further discussion around the key challenges faced by these financial institutions and to better understand, and validate, whether they accurately represent the experience of participating banks. This also partly served to glean any additional findings in a group discussion format around possible solutions to those challenges, as actions either for the regulator or for the banks themselves.

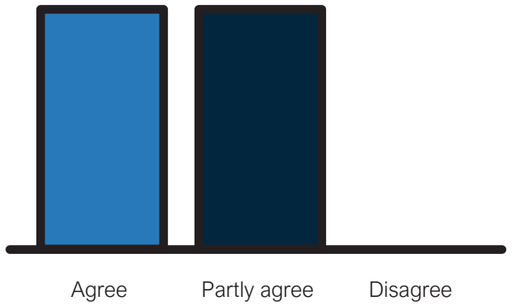
A number of key themes emerged which represented the challenges faced by these global banks regarding the Three Lines model - We then distilled these themes into four key pain points. These were the core challenges underpinning the range of themes illuminated throughout the discussions and workshops.

Theme	Risk
Balance of resourcing between lines 1 & 2 - view that in totality it's probably OK, just in the wrong place Skill level in the second line - lack of business understanding, poor quality of challenge Lack of second line value add - should provide more intelligence and horizon scanning	
Duplication of controls	
Skill level in 3rd line - use of scripts and tendency to box ticking, lack of knowledge of the business	
Regulatory concerns - gold plating and seeking perfection, view that second (to an extent the third) don't want to be caught in a situation where something did slip through, and the regulator might criticise them	
Need for definition, clarity and consistency between first and second line roles	
Lack of clarity and consistency between regulators / Regulator language use entrenching practises and ideology	
Refinements to the model not reinvention - design less of an issue than implementation	
Need for mobility between the lines	
Lack of trust or communication between lines of defence	

APAC 1LoD Data

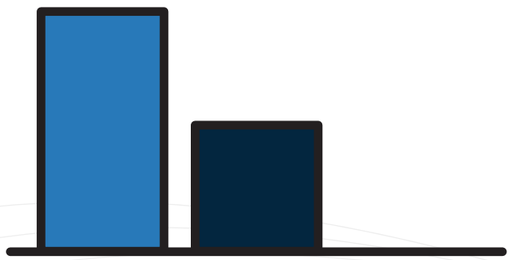
Survey Results

Q1. The role of the control officer is to specifically manage the statutory obligations of SMR on behalf of the CEO. This is to ensure effective risk identification, assessment, remediation, governance and control effectiveness.



"You need the risk owner to be responsible as an SMR to discharge their responsibility."

Q2. The role should be viewed as being responsible for key components parts of the risk management chain; identification, assessment, governance, and control effectiveness, but not remediation with resides with the respective process/control owners.



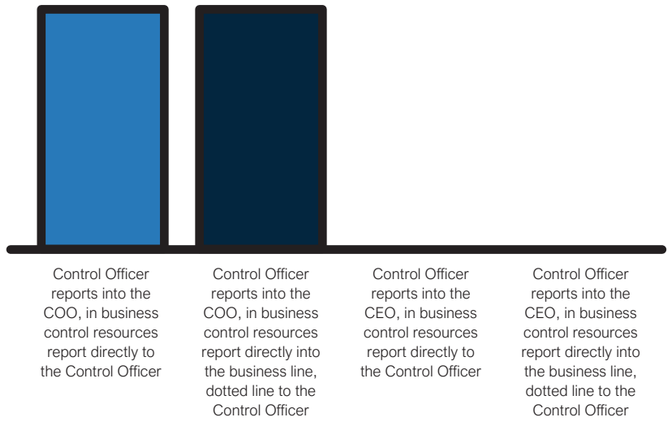
"Sometimes for BCO to run on behalf"

"Control Officer, NFR lead play a key role in helping the SMR

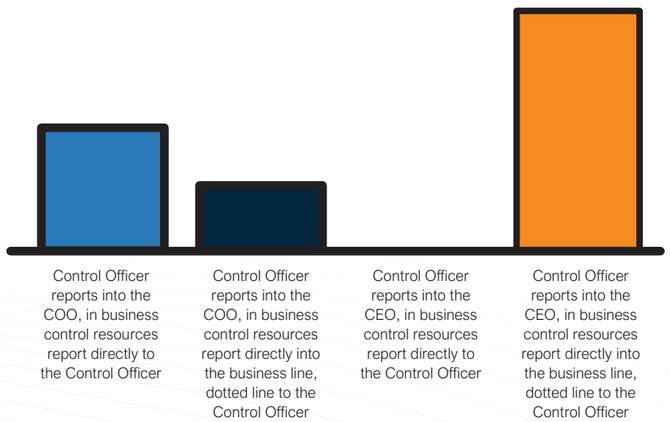
Q3. The role of the Control Officer is to provide informed and objective counsel to the CEO upon request, to enable the CEO to make informed decisions on: decision to stop, restrict continue business; what to escalate; what to prioritise funding on.

"The NFR lead should act as the trusted advisor to help manage the risks within the appetite."

Q4. Which operating model is established at your organisation?



Q5. As an independent assessment, which model serves the interests of the business best?



Contact

Maurice Evlyn-Bufton
CEO Armstrong Wolfe
maurice.evlyn-bufton@armstrongwolfe.com

Piers Murray
Chief Operating Officer, US & Puerto Rico
piers.murray@armstrongwolfe.com

Terry Yodaiken
Global Head of Wealth & Asset Management
t.yodaiken@armstrongwolfe.com

Find us on LinkedIn: Armstrong Wolfe

Find us on LinkedIn: Women in the COO Community

ARMSTRONG WOLFE™