OLIVER WYMAN

WHOSE LINE IS IT ANYWAY?

DEFENDING THE THREE LINES OF DEFENCE

AUTHORS

Michelle Daisley, Partner

Sean McGuire, Partner

George Netherton, Partner

Mark Abrahamson, Principal

MARSH & McLENNAN COMPANIES

"How do you organise a financial services firm to manage risk effectively?"

This question is seldom answered without the conversation turning to the "Three Lines of Defence" framework. Yet this ubiquitous model receives only lukewarm support from those who use it.

In this short note, we argue that there's a self-fulfilling prophecy being played out in the tepid attitude of users. Institutions are "adopting" the Three Lines of Defence in a half-hearted way and are accordingly reaping half-baked risk-management outcomes.

We believe that the philosophical foundations of the model are sound, but that it will only deliver effective risk management when coupled with a specificity and thoroughness in implementing it that has largely been absent from the industry to date. The challenge for C-Suite executives and board members is to diagnose whether their organisations are truly "walking the walk" or merely "talking the talk."

Ambiguity on this topic is dangerous. Putting aside the matter of inefficiency, without a healthy functioning risk-management framework in place, firms can be exposed to risks being taken by a small number of people with asymmetric incentives to the detriment of the business, the customers and the industry. Add to this a false sense of security being provided to the board and supervisors on the comprehensiveness of independent and expert challenge and you have a precarious state of affairs.

THE SELF-FULFILLING PROPHECY

In the summer of 2013, the Parliamentary Committee on Banking Standards published their report, and devoted two pages to lambasting British Financial Services firms' reliance on "The Maginot Lines of Defence."[1] Their criticisms were that a concept of unknown provenance had led to endless rounds of simply ticking the boxes and very little real management of risks. Too many accountants, not enough accountability.

In Q4 2014, the Office of the Comptroller of the Currency (OCC) published its "heightened standards" guidelines[2] on risk governance, including an attempt to redraw the Three Lines of Defence that would have the banking industry engage properly with the model. Shortly after, the Basel Committee on Banking Supervision (BCBS) reminded the banking industry[3] that risk governance frameworks "should include well-defined organisational responsibilities for risk management, typically referred to as the three lines of defence." The model is here to stay, at least for the foreseeable future.

And yet, in our experience across banking, insurance and asset management, this is a pervasive but unloved model. Clients consistently "adopt" the Three Lines of Defence model, but few place real confidence in it, few have anchored their risk management philosophy to this concept at a genuinely practical level, and few senior managers are prepared to put their faith in it when it's their livelihood that's on the line.

We believe, however, that reluctance to commit to the framework is itself the primary driver of the ineffectiveness perceived in its implementation.

1 Parliamentary Commission on Banking Standards, "Changing Banking for Good," June 2013.

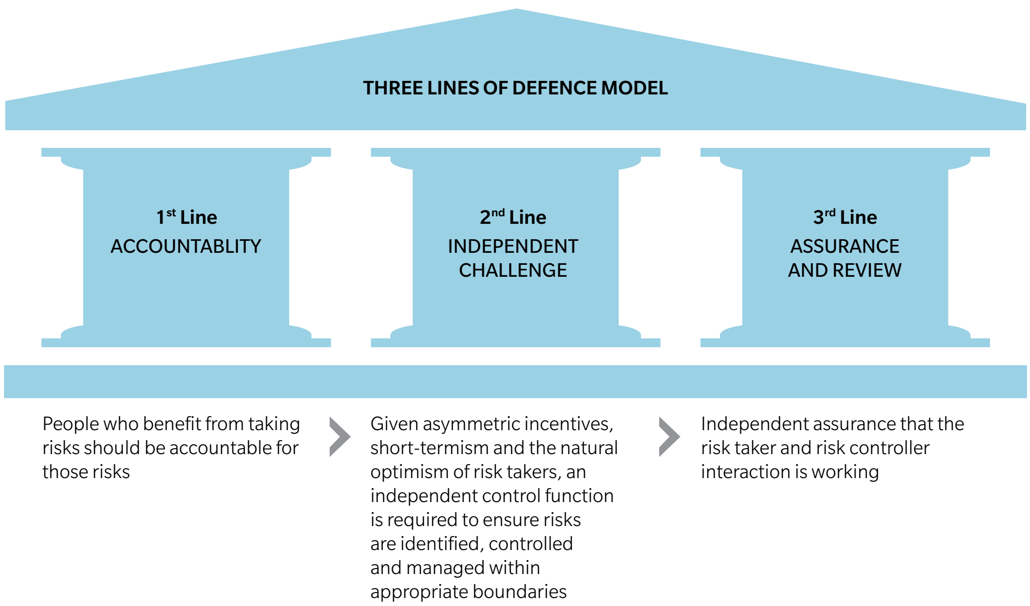
2 Office of the Comptroller of the Currency, "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations," September 2014.

3 Basel Committee on Banking Supervision, "Corporate governance principles for banks," July 2015.

THE UNDERLYING PRINCIPLES OF THE MODEL

Despite the criticism, we believe that if put to sensible professionals unscarred by personal experience, the key tenets of the Three Lines of Defence would be met with a resounding chorus of approval:

Exhibit 1: Three Lines of Defence Model



- **Materiality-based risk management.** Independent challenge is most required where the ability to increase the risk is greatest – formulating strategy, pricing products, managing capital and mergers and acquisitions, etc.
- **Independence of the risk management function.** Those individuals playing a challenger role must be legitimately independent, as evidenced throughout the organisation (reporting lines, governance, remuneration, etc.)
- **Constructive and collaborative approach.** In addition to providing independent challenge, 2nd line risk managers will need to adopt a constructive and collaborative approach to deliver better business outcomes and avoid a “them and us” divide
- **Rational, principled framework.** This should not be a rigid model that constrains sensible behaviour, generates workload and creates artificial barriers in the business, but a rational, principled framework providing guidelines and clearly set out compensating controls and governance wherever the standard model is flexed

HOW IS YOUR ORGANISATION DOING?

If the principles underlying the framework, then, make sense, the real issue is in their consistent and rigorous implementation – and in presenting evidence of this to top management. How can the modern board director have full confidence in the reports they receive and the systems that are in place? We have set out a list of five tell-tale signs the organisation is living a lie, and a checklist of common and complex areas.

FIVE SIGNS THAT YOU ARE LIVING A LIE

SIGN	WORRYING WORDS	DESCRIPTION
1 Whose line is it anyway?	*"We play more of a line 1 B role here"* *"If the Business Unit Risk team are 2nd line, what line is Group Risk?"* *"In reality, we cover all three lines of defence"*	• Widely differing opinions about who plays what role in which process • Frequent allocation of 1st and 2nd line roles to one team or person • "Assurance safety blanket" teams created by managers (especially under e.g. the Senior (Insurance) Managers Regime(s)) to provide regulatory attestation as wider model not trusted
2 So abstract it is absurd	*"It's more of a high level construct here – we don't think it's appropriate to make it a bureaucratic mess"* *"Our processes are about people making the right decision – not what hat they wear"*	• Organisations have "adopted" the model but lack specificity to make it meaningful • High level guidance is not translated into job descriptions, policies or process design
3 Only answering the easy questions	*"The model just doesn't fit the reality of some parts of the business, and we are practical about that"*	• Reluctance to resolve the grey areas where 3LoD requires judgement in implementation • See *Common Pitfalls Checklist* in exhibit 2
4 Complacency breeds contempt	*"It's been like this for years – everyone knows their role"*	• Risk function organised in a different era and not overhauled since • Model not updated for constant revolution in financial risk management
5 Mind the gap	*"We know credit is our biggest risk, but the team has been so focused on Solvency II, we haven't looked at the portfolio in detail for some time"*	• Key tasks not explicitly owned or assigned to a particular team/line • Risk function has broad mandate but resource is overwhelmingly regulatory and risk modelling focused

Exhibit 2: Common Pitfalls Checklist for Three Lines of Defence

		CLEAR ROLES	1ST LINE ARE MANAGING RISKS	2ND LINE PROVIDE EFFECTIVE CHALLENGE
1	Risk appetite	☐	☐	☐
2	Business planning	☐	☐	☐
3	Capital management	☐	☐	☐
4	Risk/capital measurement	☐	☐	☐
5	KPI definitions/targets	☐	☐	☐
6	Credit origination/underwriting	☐	☐	☐
7	Pricing/product design	☐	☐	☐
8	M&A	☐	☐	☐
9	IT	☐	☐	☐
10	Funding/liquidity	☐	☐	☐

GETTING IT WRONG – WHAT'S THE WORST THAT COULD HAPPEN?

The risks of claiming adoption of the Three Lines of Defence and crossing your fingers at the same time are serious:

EXPENSIVE	INEFFICIENT	DANGEROUS
• Redundancy of roles where poorly articulated or insufficiently well understood • Significant additional process burden which does not actually deliver better risk management outcomes • Lack of clarity results in management unwilling to reduce red tape without greater confidence in the model	• Slow decision making as unclear mandates lead to prevarication • Too much resource entangled in too few processes • Lack of confidence in model leads to highly disruptive knee-jerk response to regulatory or board enquiry	• Significant risk exposures may not be appropriately governed or controlled without a comprehensive perspective • Lack of personal and departmental accountability facilitated by grey areas • False sense of security provided to management and board by referring to but not implementing Three Lines of Defence

Financial services organisations in the 21st century, with thousands of highly complex and technical decisions taken each day, rely on a system to be manageable. Creating order out of chaos is a Sisyphean task, but one which falls to managers and governors of modern financial services organisations. Ensuring this system is fit for that purpose is a regulatory imperative, and with the introduction of new requirements like the Senior Managers and Senior Insurance Managers Regimes[4] in the UK, it has become a personal imperative as well.

4 See FCA CP15/9: Strengthening accountability in banking: a new regulatory framework for individuals and PRA CP26/14: Senior insurance managers regime: a new regulatory framework for individuals.

WHAT DOES "GOOD" REALLY LOOK LIKE? HOW TO KNOW WHEN YOU REALLY HAVE ADOPTED THE THREE LINES OF DEFENCE

Financial services firms are complex, and we think it unhelpful and unrealistic to assume firms should channel resources into a theoretically pure implementation of the Three Lines of Defence model. It is, after all, intended as a framework for managing risk that can and should be tailored to each firm, and applied at a granularity that makes sense.

This sensibility notwithstanding, an effective implementation of the Three Lines of Defence does share the following common features. How many of these do you have in place?

Exhibit 3: Features of an effective Three Lines of Defence

DOCUMENT

Documented rationale for how and why and where the Three Lines of Defence is implemented in practice

- Process-by-process view, not a function-by-function view – ensure full coverage by starting from the risk, rather than the team
- Up to date, and reflected in resource allocations

EMBED

Fully embedded and universally and consistently understood

- Consistent response to the questions of who plays which role for which process from the relevant teams
- A common understanding of the compensating controls when (for entirely logical reasons) there is deviation from the norm

TEST

Periodic testing of how this works in practice

- Regular reviews to test the breadth and depth of independent challenge
- Reviews mix broad coverage with focused deep dives on areas of complexity or observed issues

REFRESH

Regularly refreshed for changes in the business

- Appropriateness of current model challenged periodically, and resourcing and mapping of the Three Lines of Defence should be closely linked to the Emerging Risk processes
- Reviewed after major changes to the business (M&A, major change in product mix, enter new markets)

EVIDENCE

Finally, evidence of constant debate and challenge – if the answer is easy, it's probably wrong

Thorough and rigorous implementation of the Three Lines of Defence requires clarity of thinking and determination in execution. When the Three Lines of Defence framework is adopted with insufficient rigour, it is often because of an inability to get business, risk, and audit to jointly agree on the activities required and the ownership for each risk. Institutions will need to answer the difficult questions as well as the easy ones, and ensure the framework addresses the risks of each area appropriately as the business evolves. It's time to get started.

Oliver Wyman is a global leader in management consulting that combines deep industry knowledge with specialised expertise in strategy, operations, risk management, and organisation transformation.

For more information please contact the marketing department by email at info-FS@oliverwyman.com or by phone at one of the following locations:

EMEA
+44 20 7333 8333

AMERICAS
+1 212 541 8100

ASIA PACIFIC
+65 6510 9700

www.oliverwyman.com

OLIVER WYMAN