



ASIA PACIFIC FINANCE AND RISK SERIES

# WHOSE LINE IS IT ANYWAY?

DEFENDING THE THREE LINES OF DEFENCE

# “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 UK's 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."<sup>1</sup> 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 US Office of the Comptroller of the Currency (OCC) published its "heightened standards" guidelines<sup>2</sup> 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<sup>3</sup> that risk governance frameworks "should include well-defined organisational responsibilities for risk management, typically referred to as the three lines of defence." Similarly, the Committee of Sponsoring Organisations (COSO) published in July 2015 its "Leveraging COSO across the Three Lines of Defense" in collaboration with the Institute of Internal Auditors (IIA); which mapped COSO 2013's 17 principles against the Three Lines of Defence model with the aim of improving the effectiveness of risk management systems through improved communications on risk management and control.

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.

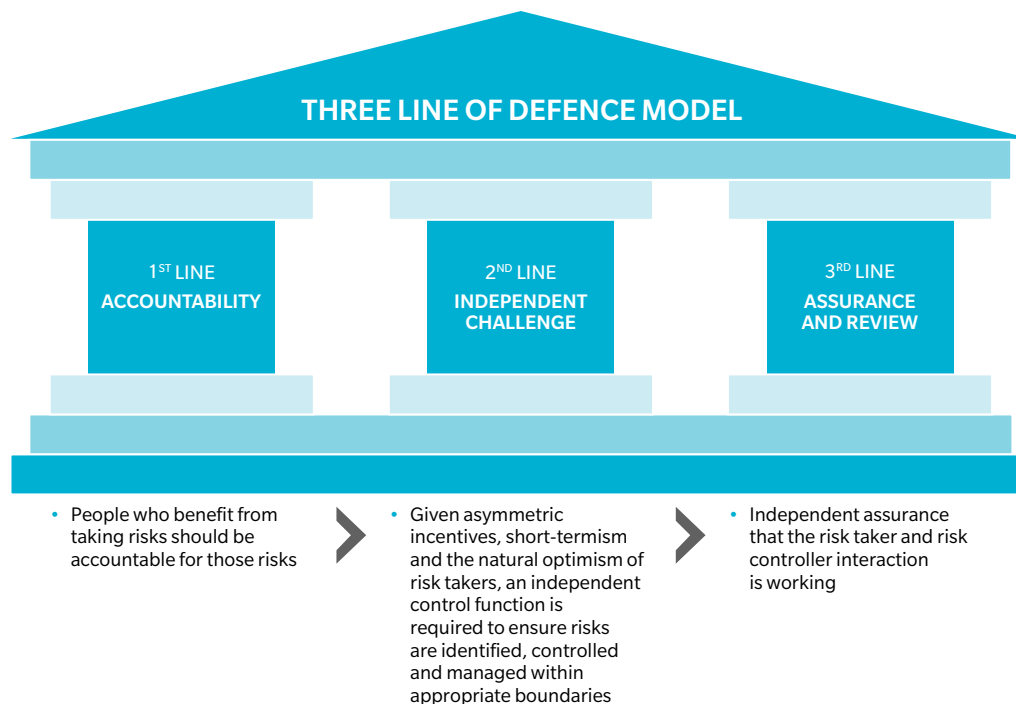
2 Office of the Comptroller of the Currency, "OCC Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches; Integration of Regulations," September 2014.

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



Source: Oliver Wyman

- **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, 2<sup>nd</sup> 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.

## Exhibit 2: Five signs that you are living a lie

SIGN		WORRYING WORDS	DESCRIPTION
1	Whose line is it anyway?	<p>"We play more of a line 1B role here"</p> <p>"If the Business Unit Risk team are 2<sup>nd</sup> line, what line is Group Risk?"</p> <p>"In reality, we cover all three lines of defence"</p>	<ul style="list-style-type: none"> <li>Widely differing opinions about who plays what role in which process</li> <li>Frequent allocation of 1<sup>st</sup> and 2<sup>nd</sup> line roles to one team or person</li> <li>"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</li> </ul>
2	So abstract it is absurd	<p>"It's more of a high level construct here – we don't think it's appropriate to make it a bureaucratic mess"</p> <p>"Our processes are about people making the right decision – not what hat they wear"</p>	<ul style="list-style-type: none"> <li>Organisations have "adopted" the model but lack specificity to make it meaningful</li> <li>High level guidance is not translated into job descriptions, policies or process design</li> </ul>
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"	<ul style="list-style-type: none"> <li>Reluctance to resolve the grey areas where 3LoD requires judgement in implementation</li> <li>See <b>Common Pitfalls Checklist</b> in exhibit 2</li> </ul>
4	Complacency breeds contempt	"It's been like this for years – everyone knows their role"	<ul style="list-style-type: none"> <li>Risk function organised in a different era and not overhauled since</li> <li>Model not updated for constant revolution in financial risk management</li> </ul>
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"	<ul style="list-style-type: none"> <li>Key tasks not explicitly owned or assigned to a particular team/line</li> <li>Risk function has broad mandate but resource is overwhelmingly regulatory and risk modelling focused</li> </ul>

Source: Oliver Wyman

Exhibit 3: Common Pitfalls Checklist for Three Lines of Defence

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

Source: Oliver Wyman

How can the modern board director have full confidence in the reports they receive and the systems that are in place?

# 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:

Exhibit 4: The risks of claiming adoption of the Three Lines of Defence

EXPENSIVE	INEFFICIENT	DANGEROUS
<ul style="list-style-type: none"> <li>Redundancy of roles where poorly articulated or insufficiently well understood</li> </ul>	<ul style="list-style-type: none"> <li>Slow decision making as unclear mandates lead to prevarication</li> </ul>	<ul style="list-style-type: none"> <li>Significant risk exposures may not be appropriately governed or controlled without a comprehensive perspective</li> </ul>
<ul style="list-style-type: none"> <li>Significant additional process burden which does not actually deliver better risk management outcomes</li> </ul>	<ul style="list-style-type: none"> <li>Too much resource entangled in too few processes</li> </ul>	<ul style="list-style-type: none"> <li>Lack of personal and departmental accountability facilitated by grey areas</li> </ul>
<ul style="list-style-type: none"> <li>Lack of clarity results in management unwilling to reduce red tape without greater confidence in the model</li> </ul>	<ul style="list-style-type: none"> <li>Lack of confidence in model leads to highly disruptive knee-jerk response to regulatory or board enquiry</li> </ul>	<ul style="list-style-type: none"> <li>False sense of security provided to management and board by referring to but not implementing Three Lines of Defence</li> </ul>

Source: Oliver Wyman

Financial services organisations in the 21<sup>st</sup> 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, as evidenced by its explicit referencing in regulation and guidance around the world. For example in Australia, APRA has recently set out updated prudential standards and guidelines for risk management<sup>4</sup> that explicitly state the importance of the three lines of defence model. In Asia, regulators are looking towards Europe and US for guidance where we have seen strengthening of the Three Lines of Defence concept.

<sup>4</sup> See APRA Prudential Standard CPS 220: Risk Management and CPG 220 – Prudential Practice Guide Risk Management

# 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 5: Features of an effective Three Lines of Defence

	<b>DOCUMENT</b>	<p>Documented rationale for how and why and where the Three Lines of Defence is implemented in practice</p> <ul style="list-style-type: none"> <li>• Process-by-process view, not a function-by-function view – ensure full coverage by starting from the risk, rather than the team</li> <li>• Up to date, and reflected in resource allocations</li> </ul>
	<b>EMBED</b>	<p>Fully embedded and universally and consistently understood</p> <ul style="list-style-type: none"> <li>• Consistent response to the questions of who plays which role for which process from the relevant teams</li> <li>• A common understanding of the compensating controls when (for entirely logical reasons) there is deviation from the norm</li> </ul>
	<b>TEST</b>	<p>Periodic testing of how this works in practice</p> <ul style="list-style-type: none"> <li>• Regular reviews to test the breadth and depth of independent challenge</li> <li>• Reviews mix broad coverage with focused deep dives on areas of complexity or observed issues</li> </ul>
	<b>REFRESH</b>	<p>Regularly refreshed for changes in the business</p> <ul style="list-style-type: none"> <li>• 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</li> <li>• Reviewed after major changes to the business (M&amp;A, major change in product mix, enter new markets)</li> </ul>
	<b>EVIDENCE</b>	<p>Finally, evidence of constant debate and challenge – if the answer is easy, it’s probably wrong</p>

Source: Oliver Wyman

---



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.

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.

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](mailto:info-FS@oliverwyman.com) or by phone at one of the following locations:

ASIA PACIFIC  
+65 65 10 9700

AMERICAS  
+1 212 541 8100

EMEA  
+44 20 7333 8333

#### AUTHORS' CONTACT INFORMATION

**Michelle Daisley**

Partner, Finance and Risk Practice  
+44 20 7333 8333  
[michelle.daisley@oliverwyman.com](mailto:michelle.daisley@oliverwyman.com)

**Sean McGuire**

Partner, Insurance Practice  
+44 20 7333 8333  
[sean.mcguire@oliverwyman.com](mailto:sean.mcguire@oliverwyman.com)

**Mark Abrahamson**

Principal, Finance and Risk Practice  
+44 20 7333 8333  
[mark.abrahamson@oliverwyman.com](mailto:mark.abrahamson@oliverwyman.com)

**George Netherton**

Partner, Insurance Practice  
+44 20 7333 8333  
[george.netherton@oliverwyman.com](mailto:george.netherton@oliverwyman.com)

**Anthony Bice**

Partner, Insurance Practice  
+612 8864 6555  
[anthony.bice@oliverwyman.com](mailto:anthony.bice@oliverwyman.com)

**Cheah Wei Ying**

Principal, Finance and Risk Practice  
+65 65 10 9700  
[weiYing.cheah@oliverwyman.com](mailto:weiYing.cheah@oliverwyman.com)

[www.oliverwyman.com](http://www.oliverwyman.com)

Copyright © 2016 Oliver Wyman

All rights reserved. This report may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman and Oliver Wyman accepts no liability whatsoever for the actions of third parties in this respect.

The information and opinions in this report were prepared by Oliver Wyman. This report is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman has made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman disclaims any responsibility to update the information or conclusions in this report. Oliver Wyman accepts no liability for any loss arising from any action taken or refrained from as a result of information contained in this report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages. The report is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This report may not be sold without the written consent of Oliver Wyman.