

# A Different Perspective on Three Lines of Defence for the Compliance Officer



**Author: Paul Coady**, Global Head of Financial Crime Risk (FCR) Education & Culture, Deutsche Bank & Member of the Ethics Committee.

The three lines of defence framework ('3LoD') provides an essential foundation for firms to define, assign, and manage risk-related accountabilities and responsibilities. A strong understanding and appreciation of 3LoD is generally assumed amongst compliance officers. If asked "*What is the three lines of defence framework?*" most of us will quickly reference each line of defence and describe, perhaps with a little hesitation, who sits in each line (e.g., Business Divisions, Compliance, Internal Audit). This understanding provides a necessary basis for 3LoD but many of us, and our related stakeholders, can often struggle to explain "*How do the three lines of defence actually work in practice?*". A clear understanding and ability to articulate the answer can be invaluable for many reasons and can allow us to leverage the 3LoD when engaging, influencing, and managing our compliance stakeholders, particularly the often more challenging business stakeholders.

The related training provided by firms often only references the different lines and who sits within each of them and this can lead to limited practical understanding of 3LoD. An analogy for enhancing such understanding is how we learn to drive a car for the first time. A driving instructor wouldn't focus only on the component parts e.g., "*...there's the steering wheel, the pedals and the handbrake, now off you go*". Learning to drive, or learning the 3LoD, does start with understanding the component parts. However, we must also be helped to see, experience, and practice how to make the parts best work together and what to do when something isn't working. A different perspective on 3LoD can support a more practical understanding of compliance and the business, as outlined below. This starts with asking ourselves a simple question and considering some of the most common responses.

## Who owns compliance risk for the firm?

### We all do

This is often the most common response. But, but how can a firm share the actual ownership of compliance risk across multiple businesses, functions, locations and potentially tens of thousands of employees? While we all undoubtedly have compliance responsibilities and some personal ownership (e.g., information security), we cannot all own the risks of the firm. Many of us have become desensitised to the difference between risk 'accountability' and 'responsibility' as these are terms often used interchangeably in firm-wide training, and culture and conduct campaigns. It is essential that we appreciate how risk ownership, accountability, and responsibility differs across our firm's stakeholders.

### The Business

We must all appreciate, understand why, and be able to articulate how the business divisions own compliance risk for the firm.

Business stakeholders may not understand or accept this and may assume that all related accountability and responsibility sits with their compliance function. They may also find it difficult to understand why significant resources and investment should be provided to a function that doesn't generate revenue and could actually restrict or impede revenue generation. Our response to such views should be that the business owns compliance risk because we cannot separate the accountability from decision-making. The business makes decisions every day that create compliance risk e.g., how it sells its products, who it sells them to, and what advice they give clients. If those businesses and their employees were able to receive all of the rewards, benefits, and bonuses arising from the risks they take but were not also held accountable for the issues, breaches, damage or consequences arising from the same risk taking, what would be their incentive for avoiding unnecessary risks or doing the



right thing? This would create a moral hazard as their decision-making and risk-taking would be influenced only by reward and not by consideration or fear of the related consequences. A key reason the first line of defence exists is to ring-fence and ensure appropriate placement of ownership with the creators of the risk. This ownership requires the business to determine, manage, and own their business-level risks, controls, and issues on which we can advise, support, and guide. However, regardless of business pressures, resources, workload or their unwillingness or inability to get things done, we cannot 'decide' or 'do it' for them.

### The Compliance Function

We must all understand and accept that we don't own compliance risk for the firm. We use our expertise to partner and advise the business in identifying, assessing, and managing their compliance risks. We must also set risk appetite, provide risk-type control and support a second line assurance of first line controls e.g., risk assessment, and controls testing. Such activity will often lead to the identification of gaps, issues, and weaknesses which, although identified by the compliance function, will be owned by the business. A key reason the second line of defence exists is to ring-fence and ensure our appropriate independence from the business. It is also critical that

we do not deliberately or inadvertently stray into the first line of defence. We must know how and where to draw the line in business partnership. The business is in the first line of defence because it is the creator of the risk. But what if someone else was to deliberately, or inadvertently, make their decisions for them? What if we told them how to do the deal, directed the way they did business, or decided and managed their business level controls for them? This could, even with the best of intentions, mean that we have actually made the decisions that have created the risk. As a result, we may lose our independence and become the owners of the risk and the related consequences.

As compliance officers, it is essential that we all practically understand the 3LoD and further our basis understanding beyond the component parts. We should all receive and provide more training on 3LoD throughout our firms and this is best achieved through relevant, relatable, and engaging cases, examples, and scenarios. Where more advanced training is required, we must focus on learning that helps us to better control the car and to avoid the pot-holes ahead rather than having to read every detail in the car's entire user manual.