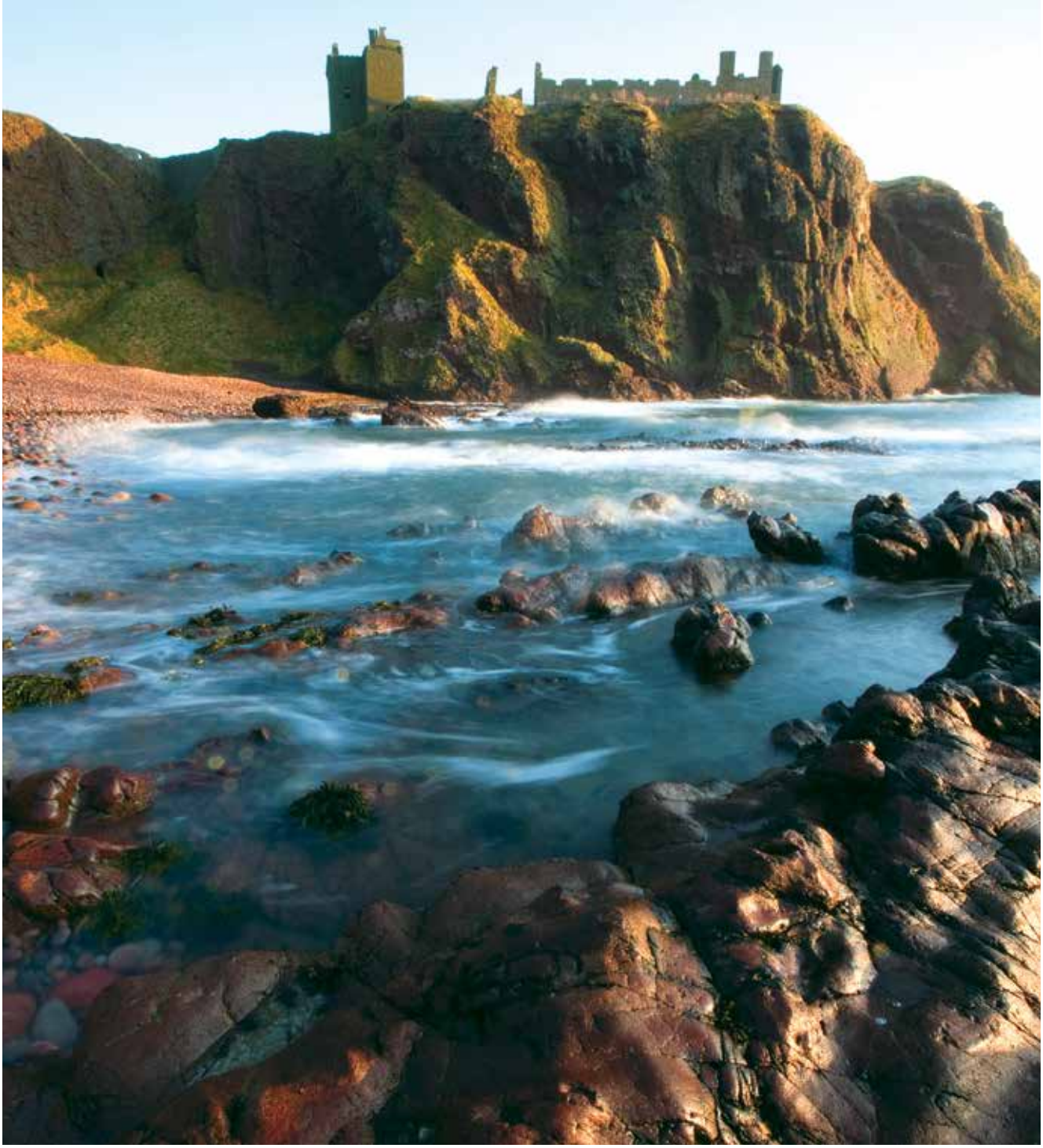

# THREE LINES OF DEFENSE IN FINANCIAL SERVICES

## FIVE SIGNS THAT YOUR FIRM IS LIVING A LIE – AND WHAT TO DO ABOUT THEM

MARK ABRAHAMSON • MICHELLE DAISLEY • SEAN MCGUIRE • GEORGE NETHERTON

Ask any bank or insurance company today about how they organize themselves to manage the risks they face and you will undoubtedly hear about their "three lines of defense": risk taking, risk oversight, and risk assurance. Broadly, the first line is made up of the risk takers – who must own and track the risks they generate. The second line is an independent body within the organization that sets risk-taking limits and ensures that all risks are being appropriately managed. The third line audits and verifies the efforts of the other two to ensure that nothing falls through the cracks. (See Exhibit 1.)

This conceptual framework has governed the industry's approach to risk management for some time, but few financial services firms are really "walking the walk" when it comes to putting this into practice. In the summer of 2013, the United Kingdom's Parliamentary Committee on Banking Standards lambasted British financial services firms for paying lip service to the framework: "Responsibilities have been blurred, accountability diluted, and officers in risk, compliance, and internal audit have lacked the status to challenge front-line staff effectively." More recently, the Basel Committee on Banking Supervision revised its principles for banks in part to "strengthen the guidance on risk governance, including the risk management roles played by business units, risk management teams, and internal audit and control functions (the three lines of defense), as well as underline the importance of a sound risk culture to drive risk management within a bank."

The fundamental foundations of the model are sound: They are designed to offset asymmetric information, incentives, and natural optimism. And certainly, empowering professional pessimists to give voice to the "glass half empty" view of the world is sensible governance. But use of the model to deliver effective risk management requires a level of specificity and thoroughness that, to date, has largely been lacking from the industry. As a concept, the three lines of defense may be comforting. But without concrete follow-through by senior managers and boards, they can only provide a false – and perilous – sense of security.

## LIVING A LIE

There are five common signs that a financial institution might be purportedly "adopting" the three lines of defense, yet might not be living the three lines of defense in practice, in the sense of consistent and rigorous implementation – in other words, living a lie. This exposes the business to bad outcomes: off-strategy losses, groupthink, overconfidence, onerous control costs, or key judgments left unchallenged. These problems often come about because the business, risk, and audit functions have failed to jointly agree on risk ownership and activities in a holistic and comprehensive way, and senior management has failed to retain a sufficient level of granularity to be confident the model is genuinely being implemented.

The first of these signs is a "theater of the abstract." Institutions adopt the model, but fail to build out a list of risk activities and translate them into appropriate policies, process changes, and job descriptions. Worrying words might be: "It's more of a high-level construct here" and "our processes are about people making the right decision – not what hat they wear."

Another sign of a fundamental problem is not knowing whose line it is – that is, not clearly separating out roles to avoid underlapping

EXHIBIT 1: THE "THREE LINES OF DEFENSE" FOR FINANCIAL SERVICES

THE THREE LINES OF DEFENSE FRAMEWORK HAS LONG GOVERNED THE FINANCIAL SERVICES INDUSTRY BUT HAS RARELY DELIVERED EFFECTIVE RISK MANAGEMENT

1. ACCOUNTABILITY

*People who benefit from taking risks should be accountable for those risks*

2. INDEPENDENT CHALLENGE

*Given asymmetric incentives, short-termism, and the natural optimism of risk takers, an independent control function is required to ensure risks are identified, controlled, and managed within appropriate boundaries*

3. ASSURANCE AND REVIEW

*Independent assurance that the risk taker and risk controller interaction is working*

**Source:** Oliver Wyman analysis

and overlapping. "We cover all three lines of defense" is not what you want to hear from any team in the organization. Allocating multiple lines to one person or group, or creating "safety blanket" teams to satisfy regulators, completely undermines the model.

A third indicator is that only the easy questions about risk are getting answered. "The model doesn't fit the reality of some parts of the business" is a clear warning sign. The firm may be failing to assign explicit responsibility for sensitive topics or grey areas, or to account for new and emerging risks, such as cybersecurity.

Just like contempt, familiarity can also breed complacency: "It's been like this for years, everyone knows their role." A strong and up-to-date risk management system requires regular updating to counter drift and ensure that all risks are accounted for.

Or worse, there can be a glaring gap between what executive teams assume the lines of defense teams are focusing on and what is actually happening, in part due to broad mandates. Unless key tasks are explicitly owned by a team, second line resources may remain overwhelmingly devoted to regulatory compliance and risk modeling. Words a senior manager never wants to hear, but often does, are: "We're not sure if that is a first or second line responsibility."

## BUILDING A DEFENSE THAT WORKS

If a financial-services firm is exhibiting one or more of these signs, it may be time for an intervention at the C-suite or board level. Poor risk management is expensive, inefficient, and dangerous: Redundancy of roles and processes cost money and add to red tape, without delivering better outcomes. Decision making slows when mandates are unclear and people

lose confidence in the model. Finally, the board and regulators may unwittingly believe that the firm has comprehensive, independent, and expert independent challenge when it doesn't – a state of affairs that will quickly come to light in the event of a business or market failure.

Of course, the three lines of defense are intended as a framework, one that must be tailored for each firm's unique circumstances and business model. But there are some commonalities to its effective use. Critically, the second line – independent oversight – must ensure both top-down and bottom-up risk capture: It owns the risk identification process – including external and emerging risks – and reports on risks to the board and senior management. But it also should be charged with ensuring that senior management and board discussions on risk at the strategic level are occurring regularly, with outcomes incorporated into risk parameters, to create an effective feedback loop. Equally, it's important that the third line, assurance, goes beyond simply auditing the other two lines on a stand-alone basis, and takes responsibility for ensuring the relationship between the two is neither too close nor too distant.

As a concept, the three lines may be comforting. But without concrete follow-through, it can only provide a false sense of security

Beyond this, clear documentation and communication, fully embedding the model, regular testing and refreshment, and evidence of independent debate and challenge are necessary to make risk management a living, breathing part of the organization.

With sufficient clarity of thinking, management drive, and determined execution, the three lines of defense can be transformed from "words to live by" to a functional bulwark that can protect the business in good times and in bad. But to be truly effective, the model needs to evolve as the business evolves.

**Mark Abrahamson** is a London-based principal, **Michelle Daisley** is London-based partner, **Sean McGuire** is a London-based partner, and **George Netherton** is a London-based principal in Oliver Wyman's Financial Services practice.