Risk accountability

Responsibility must be shared

Risk Governance 2020

EY believes financial services firms face a sea change in how they approach risk governance.

Risk accountability is one component of this overall effort.

The transformation required will take a comprehensive, multi-year effort to substantively complete. To remain at the forefront of today's market, firms should adopt an integrated approach that capitalizes on the value gained from upgrading risk governance: placing an equal focus on financial and nonfinancial risks in the short and long term, embedding evolving regulatory and supervisory expectations, and delivering tangible results in a cost effective manner. We call it *Risk Governance 2020: a shift from satisfactory to effective and sustainable.*

The succession of control and conduct failures since the 2007–08 financial crisis has caused significant concern among global and domestic regulators. Initially, the failures were tied to pre-crisis actions and behaviors, resulting in major regulatory focus on building and strengthening risk and control functions. More recent Libor and Forex manipulation has been a game-changer. In the eyes of regulators and other key stakeholders, significant conduct and control failures continue

Given the industry's heavy investment in risk and controls over the past five years, regulators faced a choice: should they double down on existing controls-based solutions or establish a new governance paradigm? It's now clear that their preference is a fully functioning three-lines-of-defense model that engenders real front-line accountability for all risks inherent in the businesses and functions where those risks originate, and allows all three lines to work effectively, both individually and together, to identify, measure, monitor and control those risks.

Regulators have backed up their views with specific requirements. In the UK, the Financial Conduct Authority and Prudential Regulatory Authority are implementing the Individual Accountabilities Regime (IAR), which greatly expands the responsibilities of senior managers and cascades accountability deep into the organization.[1] Implementing the IAR effectively depends heavily on a functioning three lines of defense framework. In the US, the Office of the Comptroller of the Currency (OCC) issued its Heightened Standards for risk management and governance to outline clear requirements on the three lines.[2]

1 *"Strengthening individual accountability in banking and insurance – responses to CP14/14 and CP26/14," Prudential Regulatory Authority, March 2014.*

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

Building a better working world

All of this follows work by the Basel Committee of Banking Supervision[3] and the Financial Stability Board[4] on the three-lines-of-defense model. Increasingly, regulatory requirements can be found across financial services.

Risk accountability is the guiding spirit of new regulatory guidelines, and the preferred mechanisms are three robust lines of defense. The challenge for the industry will be to make true accountability a reality over the coming years.

The current approach to risk faces challenges

The three-lines-of-defense model has existed for years. However, in many financial service firms, the model has become flawed in its application:

- **Limited, or no, front-line accountability for risk**. Significant investments in, and reliance on, second-line risk and compliance functions have, ironically, undermined front-line accountability in some institutions over time. Front-line business units may have nominal, if any, responsibility for risks they create in their day-to-day activities, other than compliance with financial-risk limits; in practice, the second line has been held primarily accountable. As evidence, regulators point to the fact that, after many major conduct and control failures other than those with clear perpetrators (e.g., traders manipulating prices), it tends to be compliance or risk executives who get demoted or fired, not front-line leaders. Moreover, the front-line focus on nonfinancial risks is often insufficient.
- **The second line having limited scope and not sufficiently focusing on aggregate risks**. Although second-line functions have grown significantly, they focus insufficiently on key aggregate nonfinancial risks, notably conduct, legal and IT risks. In some cases, the second line has not done enough independent analysis of aggregate risks, relying too heavily on other control functions (e.g., legal) or taken unchallenged front-line information, aggregated it and reported it upward or applied necessary limits. More independent analysis is required.

  Some firms do have clear front-line accountability for all risks, and many were winners through the financial crisis. For them, building out a larger second or third line seems more of a regulatory requirement than a business imperative. The reality is, having a strong second-line identify, measure, monitor and mitigate aggregate risks and offer effective challenge of the front line is important, as is a high-quality assurance process; these reinforce, rather than undermine, front-line risk accountability.
- **The third line – internal audit – must adapt its coverage and skill sets to accommodate changes to the front and second lines and other requirements**. First, internal audit is affected by broadening front- and second-line responsibilities and having to focus equally on financial and nonfinancial risks. Second, complying with new regulations – e.g., IAR, stress testing, capital planning and ring-fencing – increases the third line's workload. Third, audit is being given specific new responsibilities, such as evaluating the risk governance framework and the firm's risk culture. For some, this will require additional resources and new competencies. For most, it will require new approaches and tools to be developed.

Incremental changes over the years created design issues for the three lines. The placement of control and risk professionals in the front line, and quality control and validation teams in the second line, has brought "mini defenses" into the model. Firms talk of "1a/1b, 2a/2b defenses" and struggle to determine if these arrangements are still adequate. The provision of advice from the second or third line to the front line also causes concern. On the one hand, providing broad advice – especially early on when it can impact decision-making – can deliver materially better outcomes from a risk and control perspective; on the other, providing advice can potentially undermine independence.

For many firms, a significant realignment and resetting of responsibilities may be required.

3 "Corporate governance principles for banks – Consultative document," Basel Committee on Banking Supervision, October 2014.
4 "Principles for an Effective Risk Appetite Framework," Financial Stability Board, November 2013.

Reimagining the model

Tinkering around the edges of the model will not make a significant difference. For many firms, a significant realignment and resetting of responsibilities may be required.

Making the three lines of defense functional in today's regulatory and competitive environment requires six major steps:

1. **Adopt an activities-based approach to redesigning the three lines**. Traditionally, firms have categorized overall organizational units or functions as part of either the front or second line, based on whether key processes or activities in the function were risk taking or risk monitoring. However, this approach fails to consider implications to the firm's risk profile of functions not typically treated as front line, despite activities in those functions directly resulting in risk generation (e.g., Treasury), enabling revenue-generation or risk-taking activities (e.g., IT or operations), or indirectly influencing the risk profile of the firm (e.g., finance heavily influences risk and compliance budgets). Taking an activities-based approach – especially where a function or unit in part generates or supports risk taking or, conversely, where a "control" function in part supports the businesses – greatly enhances the quality of the three-lines-of-defense model.

2. **Clarify roles and responsibilities of the three lines**. Each line needs a clear sense of what its risk responsibilities are: in essence, the front line owns all the risks inherent in the business or function, the second line owns the measurement and monitoring of aggregate risks, and the third line provides assurance that the risk governance framework operates effectively as a whole. It is important to agree how the lines function together: how much can each line rely on another, and what risk assessments can be shared? The three-lines-of-defense model is as much about the system as a whole as it is individual line responsibilities. Second- and third-line independence should be protected, but effective partnering is essential.

3. **Explain individuals' roles and competencies**. Ultimately, the three lines comprise a set of individuals. Once the broad framework is realigned, firms should re-evaluate and communicate each individual's role within their unit, so all are fully aware of their risk management responsibilities. This is most critical for front-line senior executives, since the weight of new regulatory responsibilities falls most heavily on their shoulders. Ambiguity greatly undermines personal accountability.

   In many critical areas, this means translating broad statements of intent into practicable responsibilities. For example, every firm will state it has zero tolerance for market manipulation, but translating policy into practice requires careful thought. A policy that makes front-line senior management responsible for assessing ways in which their own people could manipulate the markets they participate in – and for implementing prevent-and-detect controls in light of that analysis – would be practical. Senior managers can be held responsible for the rigor of the analysis and the quality of the controls, without being held accountable for every illegal act of subordinates.

   Inevitably, after clarifying individual roles, it becomes apparent that each individual's competencies must be critically assessed. Having the right people in the right roles, in the context of the right framework, is key. This requires firms to have a deep understanding of the competencies required for specific roles across the three lines of defense.

Incentive structures and performance management approaches should be reassessed so they align with, and reinforce, the redesigned three lines and their roles and responsibilities.

4. **Clean up design ambiguity**. Even though regulators have been clear on their overall expectations for the three lines, they have avoided being overly prescriptive on the details to allow for differing approaches to accommodate differing circumstances. However, firms do need to address several common design aspects of the three-lines model:

   - 2b or not 2b? The presence of distinct control functions within the front line (in-business risk and compliance officers or quality assurance) or the second line (independent validation and verification) creates distinctions (e.g., 1a vs.1b, 2a vs. 2b). These arrangements may not need to be restructured, but a set of mechanisms should be implemented that reinforce segregation of duties, including the governance model, organizational reporting lines, reinforced risk behaviors and documentation to articulate how risk is managed and how the lines of defense interact.

- Crossed reporting lines? Many firms believe that by having in-business risk and compliance officers who report to the second line, the firm maintains front-line responsibility for risk. This arrangement can cover a range of tasks, such as risk strategies, risk data generation and reporting, and model validation. Regulators have sometimes contributed to the confusion on these arrangements, leaving firms with tough questions on what best enables prudent risk taking and strong risk management.

  In practice, reporting lines can be misleading, and an activity-based assessment can prove useful. The critical factor is whether risk professionals are acting in a first- or second-line capacity or with an independent mindset. Are they monitoring risks and limits, offering objective analysis, and are their compensation and career path independent of the front line? Or are they advising front-line management on specifics, such as managing portfolio risks and appropriate hedging strategies, or on whether a particular transaction is compliant with applicable law and regulation, and does front-line management have material influence over their compensation and career?

  If the answers tend to the former, those front- line risk professionals should retain dual reporting lines; that connotes their second-line role. If the latter is more accurate, those risk professionals should be considered front line, and reporting lines to the second line should be removed. Obviously, if specific front-line risk professionals are balancing multiple first-and second-line activities – in one context guiding risk strategies in the business and in another offering effective challenge – consider focusing them on their front-line risk roles, remove dual reporting and reassigning their second-line risk or compliance roles to others.

- Advice or no advice? Some argue that the second and third lines should not advise the front line on risk and control approaches, because it undermines their ability to independently monitor and challenge the front line. One legitimate way to address this issue is to put the necessary advisory capabilities into the front-line business unit. However, regulators are not pressing that approach. They recognize that receiving such advice can be invaluable for the front line because the second and third lines can share best practices from other parts of the business or from outside the firm. In fact, certain requirements (e.g., the OCC's Heightened Standards) specifically require the input of the second and third lines of defense in areas such as strategic planning. Further, second- and third-line involvement in strategic business discussions can help those functions continue to adapt their monitoring and oversight activities to keep pace with business dynamics. However, the intent is to give the second and third lines a "seat at the table" and the ability to provide risk and control insights. They must not get drawn into, in effect, business decision-making, executing on strategy or designing risk controls, lest both their independence and the front line's accountability get undermined.

Line	Responsibilities
Front	▸ Owners of risk related to their activities – identify, measure, monitor, control and report all financial and nonfinancial risks
Second	▸ Identify, measure, monitor, control and report all aggregate risks ▸ Develop the risk management framework and maintain an independent, aggregative view of risk ▸ Provide a risk viewpoint into strategic planning, impending regulatory changes and guidance on front-line risk management responsibilities
Third (i.e., internal audit)	▸ Provide a view beyond control adequacy to broader subjective matters (e.g., risk culture) ▸ Independently assess the effectiveness of the risk governance framework in its entirety

5. **Adopt the right governance structure**. Firms should re-evaluate how the board and senior management oversee the three lines of defense. At the board level, it may behoove boards to consider different approach, particularly across audit and risk committees. In some ways, current board oversight may not be engendering an integrated oversight approach; going forward, firms need to ensure the three lines function well as a system. This may require, for example, adopting working groups to oversee major transformation of the three lines of defense. Similarly, senior management may need to adapt its committee structure to better align with the three lines.
6. **Confirm the capabilities**. Once the three-line redesign and the governance framework are in place, each line must rethink what capabilities it requires to succeed. Inevitably, firms may need to adopt:
   - Firm-wide common risk taxonomies
   - Standardized risk and control assessment approaches that enable a stronger focus on more forward-looking risks and nonfinancial risks
   - Common platforms for storing, accessing and monitoring risk and audit assessments and remedial work
   - Stronger data analytics
   - Centralized testing and validation capabilities

Over time, firms may move toward adopting formal approaches to evaluating and monitoring controls on a front-to-back basis. Some firms have already appointed executives to oversee the whole control structure and to drive a holistic approach to strengthening – not merely adding to – the control environment.

Transformation is on the horizon

The initial response of many terms to renewed regulatory focus on the three lines has been to tinker tactically with existing design – the 2a/2bs. By contrast, those facing the UK's new accountability regime, and those properly understanding the intent of the OCC's Heightened Expectations or regulations of this kind in other sectors, realize the scale of change required is significant.

Such change takes time. Firms need to continue managing risks on a day-to-day basis, while also managing broad changes to the three lines of defense and implementing new capabilities to make it function.

The reality is large firms' risk and control apparatus are complex and huge, with some employing many thousands of professionals. This colossal task brings to mind the analogy of an oil tanker: changing directions and realigning the work of the crew/team will take effort and time. On its current course and motion, the tanker could hit the rocks, and changing direction by a degree or two does little to avoid that happening. However, regulators' views are clear: a further transformation of the practice of risk governance beyond what has occurred to date is required in the near to medium term. Over time, a major course correction is required. Having a strategic road map to manage such change is essential.

Americas

Peter Davis
Principal
Ernst & Young LLP
+1 212 773 7042
peter.davis@ey.com

Tom Campanile
Partner
Ernst & Young LLP
+1 212 773 8461
thomas.campanile@ey.com

Ted Price
Senior Advisor
Ernst & Young LLP
+1 416 943 3597
ted.price@ca.ey.com

Mark Watson
Executive Director
Ernst & Young LLP
+1 617 305 2217
mark.watson@ey.com

EMEIA

Chris Bowles
Partner
Ernst & Young LLP
+44 20 7951 2391
cbowles@uk.ey.com

Patricia Jackson
Senior Advisor, Risk Governance Lead
Ernst & Young LLP
+44 20 7951 7564
pjackson@uk.ey.com

Asia-Pacific

David Scott
Partner
Ernst & Young Advisory Services Limited
+852 2629 3614
david.scott@hk.ey.com

About EY
EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Ernst & Young LLP refers to the individual client-serving member firms of Ernst & Young Global Limited operating in the UK, US. Ernst & Young refers to the client-serving member firm of Ernst & Young Global Limited operating in Hong Kong. For more information about our organization, please visit ey.com.

EY is a leader in serving the global financial services marketplace
Nearly 43,000 EY financial services professionals around the world provide integrated assurance, tax, transaction and advisory services to our asset management, banking, capital markets and insurance clients. In the Americas, EY is the only public accounting organization with a separate business unit dedicated to the financial services marketplace. Created in 2000, the Americas Financial Services Office today includes more than 6,900 professionals at member firms in over 50 locations throughout the US, the Caribbean and Latin America. EY professionals in our financial services practices worldwide align with key global industry groups, including EY's Global Wealth & Asset Management Center, Global Banking & Capital Markets Center, Global Insurance Center and Global Private Equity Center, which act as hubs for sharing industry-focused knowledge on current and emerging trends and regulations in order to help our clients address key issues. Our practitioners span many disciplines and provide a well-rounded understanding of business issues and challenges, as well as integrated services to our clients. With a global presence and industry-focused advice, EY's financial services professionals provide high-quality assurance, tax, transaction and advisory services, including operations, process improvement, risk and technology, to financial services companies worldwide.

CK0939
1504-1441892
ED none

ey.com