www.pwclegal.de

Redefining the three lines of defence (3LoD) model during a time of prolonged pandemic preparedness and location-independent working

pwc

Table of content

Quick Take

Traditionally financial services firms designed their 3LoD models including how and where their control functions carry out their duties when interacting with business and operational units very much on the basis of an office-centric working environment. COVID-19 has changed all of this. Financial services firms generally and their risk models specifically have had to evolve out of necessity and also respond to new operating models, new ways of working (remotely/hybrid) and ultimately the role of technology.

As various (often rolling) lockdowns took hold, financial services firms and their staff (but equally supervisors) swapped office space for an assortment of living or spare rooms and remote working spaces. Financial services firms have had to extend their 3LoD models into those private spaces. Both remote working and location-independent working arrangements have taken hold across various types of financial services firms. This "new work mix" is likely to co-exist as alternatives to more traditional office-centric work and do so well beyond the end of the pandemic and a return to more normal operating conditions.

Consequently, a whole new dynamic has been introduced into the relationship between employer and employee and a number of legal and regulatory considerations – as explored in separate Background Briefings available from PwC Legal's RegCORE. Greater decentralisation and digitalisation but also, to a certain extent, democratisation were rapidly deployed across firms as part of this shift. Firms will want to (continue to) adapt their 3LoD models to take account of this new "new normal" in working arrangements. They will also want to ensure their 3LoD models reflect the range of specific internal and external threat factors that can arise and pose a risk to a financial services firm's operational and digital resilience, especially where existing (pre-COVID-19) risk conventions as well as systems and controls need to be adapted to remain effective.

Equally during this move to a new work mix, changes were advanced in July 2020 by the Institute of Internal Auditors (IIA). Those changes amended the 3LoD model to what is now known as the "Three Lines Model". For sake of simplicity this Background Briefing uses the overarching term of 3LoD as opposed to distinguishing between the two approaches given that the principles discussed below apply to both models.

All parts of financial services firms have been affected by COVID-19 and which have successfully weathered the storm with short-term fixes may need longer-term solutions. Firms will want to review and redefine, regardless of business sector and/or model, how they run systems that identify, mitigate, measure and manage the set of risks they are faced with in a post-COVID-19 business environment. Some firms, notably those with a corporate culture of client-centricity and employee empowerment may find driving that change easier. Nevertheless, combined offerings from RegTech providers and external counsel may assist firms in moving to a more digital enabled 3LoD model that can cover both office-centric risks as well as the range of challenges posed from prolonged working from home arrangements.

The evolution of the 3LoD model for financial services firms

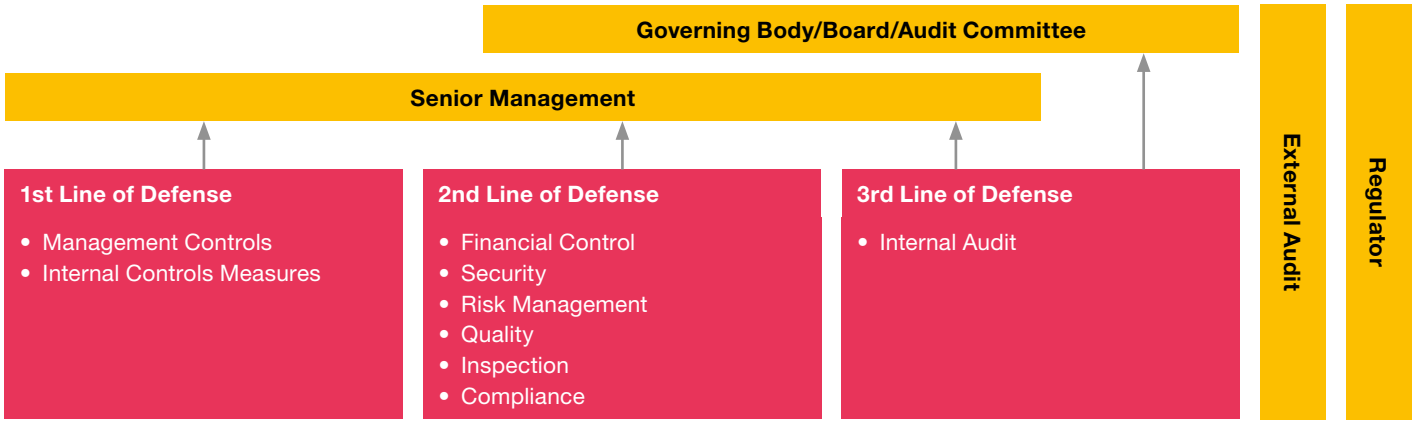
The notion of a Three Lines of Defence (3LoD) model has a long history of use, such as in military, sports and other fields, that predates its use in financial services firms from roughly the 1990s onwards. The 3LoD model itself interoperates with and serves as a cornerstone of firms' target operating models (TOMs) along with their governance, risk and compliance (GRC) management frameworks and the corresponding internal control systems (ICS) as well as the role of the audit function.[1]

The 3LoD approach assists financial services firms in setting defined roles and apportioning responsibilities across a corporate structure. This serves to strengthen the firm's corporate governance, compliance and risk management as well as enabling it to (i) better manage the business needs and staff; (ii) set a clear(er) chain of responsibility and allocation of which staff performs which functions; and(iii) better identify, mitigate and manage risks that apply to the firm as a whole.

In the 3LoD model each line has its own unique role and responsibilities to play:[2]

1. The 1st line of defence (1LoD) refers to the unit(s) that own and manage the risk. Every function is a risk owner for the risks it produces so 1LoD does not apply "just" to business units;
2. The 2nd line of defence (2LoD) reports to senior management and refers to those risk management and (compliance) control functions[3] to help build and/or monitor the 1LoD controls; and
3. The 3rd line of defence (3LoD) provides independent assurance and the internal audit function provides assurance on the effectiveness of GRC controls including on the operation of the 1LoD and 2LoD controls. Internal audit is independent of management with a direct reporting line to the governing body and/or audit committee of a regulated financial services firm.

Each of the lines of the 3LoD are also susceptible for review by the external auditors and financial services regulators. Under the traditional pre-July 2020 3LoD model the individual lines were set up as follows:

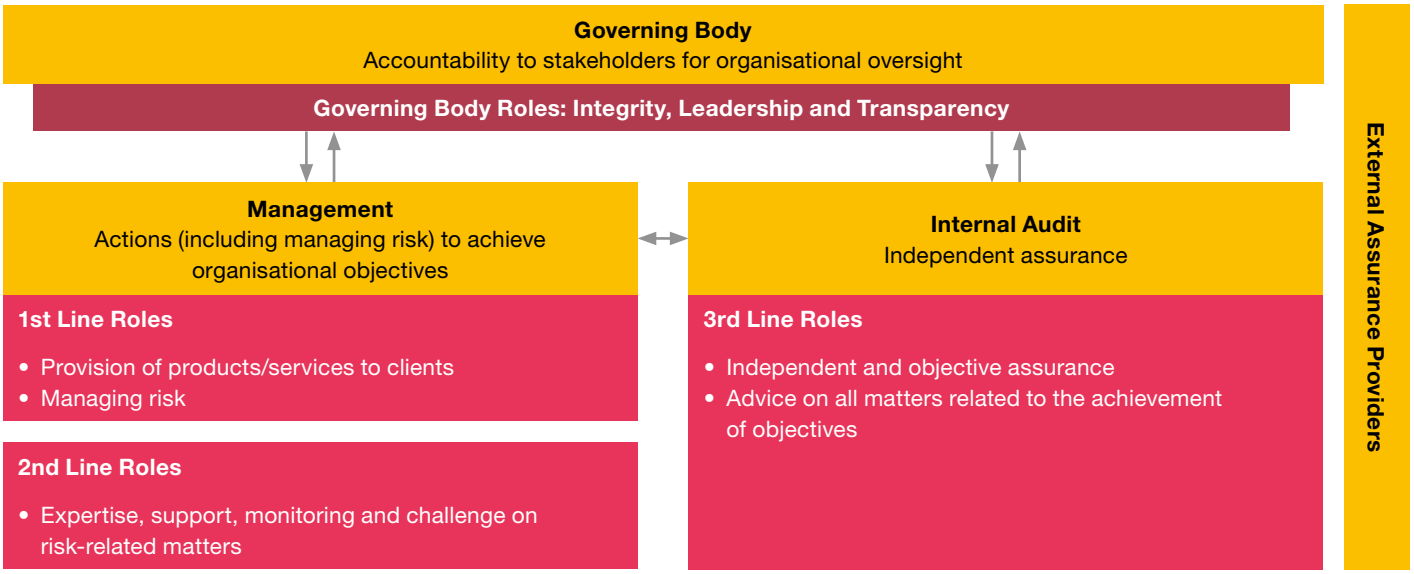


[1] In application of the model to the risk management within financial institutions, the term was first coined by the UK's Financial Services Authority (FSA) – now the Financial Conduct Authority (FCA), in 2003, as part of its Policy Statement regarding operational risk frameworks. For more see: Financial Services Authority, Building a framework for operational risk management: the FSA's observations, FSA, 2003.

[2] The 2013 position paper of the Institute of Internal Auditors includes what is considered to be the formal definition of the 3LoD and their roles. See: IIA Position Paper: The Three Lines of Defence in Effective Risk Management and Control from January 2013 which was also updated in July 2020 available here as the Three Lines Model.

[3] Risk management and (compliance) control functions are designed to facilitate and monitor the implementation of effective risk management practices by management throughout the organisation, assisting risk owners (i.e., 1LoD and elsewhere) in defining target risk exposure and providing adequate risk reporting. The principal purpose of compliance functions is to monitor compliance with applicable laws and regulations. It is common for multiple control functions and thus also compliance teams to operate within an organisation, with responsibility in areas such as health & safety, human resources, legal, supply chain, environmental or quality.

Under the July 2020 revisions, various new principles and a slight amendment to who should be taking the lead on what and when, were introduced. This can be visually represented as follows:



Despite the slight changes in models, certain aspects of the overall framework remain open to interpretation and debate. These remain regardless of where the lines are based but may also be complicated where firms' functions are operating siloed and decentralised and there's inability to resolve issues in person, whether in a meeting room or in a more informal setting. One such area that is often critiqued is if the 3LoD identifies control deficiencies in the 1LoD, does this only reflect issues in that line or also indicate a weak 2LoD?[4] Furthermore, as many of the critics of the 3LoD model have argued, there is, in some firms, often an overlap in activities, which is inefficient (e.g., compliance testing and audit testing on the same data). It can also create a false sense of security, namely in the 1LoD, that, even if they are not very diligent in their risk management activities, the 2LoD and the 3LoD can pick up the slack as they are primarily tasked with identifying the 1LoD gaps and issues.[5]

Then there are circumstances where 3LoD can be counterproductive. Imposing overtly excessive or unreasonable burdens on the 1LoD in terms of the extended complexities of the 3LoD model and the control environment is also undesirable, for the traditional 1LoD (i.e., the business) is what generates the revenue and keeps the entire financial institution running. Therefore, a delicate balance needs to be achieved between the roles, responsibilities and expectations imposed on each line.

[4] In such a hypothetical example: on the one hand the 1LoD weaknesses may be attributable to 2LoD for (i) setting up a weak overall framework; (ii) providing unclear policies and minimum control standards; (iii) poor 1LoD framework implementation oversight; and/ or (iv) weak 2LoD controls for failing to detect/ address the issues. On the other hand, however, risk owners are primarily responsible for identifying and managing their own risks, and thus holding the 2LoD accountable for every 1LoD deficiency is also problematic.

[5] This issue is even more prominent in the 2LoD and 3LoD functions, as they are also risk owners (i.e., 1LoD) for the risks they generate – e.g., various OR risks, such as those relating to HR activities, IT, legal, compliance, etc. Consequently, the role of the 2LoD (and to a certain extent 3LoD) becomes two-fold – performing their traditional "line" role, while being subject to a 2LoD (and 3LoD) control from within their "own" line. This not only requires additional resources (i.e., providing additional 1LoD-type risk officers per each 2LoD for their own 1LoD risks), but it also raises concerns regarding independence and conflict of interests (e.g. a 1LoD type risk officer in a 2LoD function performing 1LoD control over their own colleagues and even superiors).

Equally, overly zealous control functions are also challenging. In a perfect world, the control frameworks would be ideal and there would rarely be risk events and risk appetite would not exist as a concept or at least not as prominently. However, financial institutions tend to be complex entities in an ever-changing environment – both from a regulatory and technological perspective. Hence, it is not always easy to identify or manage risks in an existing 3LoD model in particular one that is operating outside of the office under COVID-19 and emergency operating conditions. Some commentators have even, regardless of COVID-19, queried whether a fourth line might be needed at some point. It remains to be seen whether this will indeed follow but for the moment regulatory authorities have been lukewarm to reinvent an established model but rather ask that efforts concentrate on adapting the existing model to the new realities of COVID-19 and the new work mix as well as the risks that emanate from such non-office working environment.[6]

COVID-19, decentralised and digital operating models, remote working and new risks

Financial services firms' traditional and revised 3LoD models have historically largely been designed with an office-centric based environment in mind. The same is true in how that 3LoD for their group and individual legal entity TOMs. Strategic but also control functions, notably GRC experts responsible for designing, deploying and delivering the 3LoD and TOM on a daily basis have had to recalibrate their risk paradigm to cover new types of risk and risk appetites, including those that arise from digital operating models, as well as remote and location-independent working models as well as to rethink the associated controls.

Financial risk (FR) but more importantly, non-financial risk (NFR) and notably operational risk (OR), has itself largely continued to focus on risks originating in the office. Such TOMs and 3LoD models were certainly not designed with prolonged pandemic preparedness in mind nor the changes (but also opportunities) being advanced by increased decentralisation and digitalisation of how business is done. Control functions i.e., GRC staff, are certainly challenged in how to supervise conduct outside the office.

The move to mass-adoption and shift to a remote-working and/or location-independent working environment across financial services firms and for a longer period than originally anticipated has put the 3LoD model as well as many a TOM through its paces.[7] New types of NFR and notably OR have emerged from this extension of where the 3LoD model is deployed i.e., swapping the office for the living room or kitchen table in private households or working on a location-independent basis from much further afield. As stated above, firms have had to and continue to adapt. It is unclear whether business lines understand what their actual risk tolerance is in light of this new environment. Should it be the same as the one prior to the COVID-19 crisis? Probably not. In traditional banking, controls are not always fully automated or can be executed online/remotely.

Certain new risks, notably an increase in financial crime, cybercrime, regulatory, reputation and legal risk in the event of (or certainly perception of) deteriorating advice standards and increased cases of misselling all have the potential of increasing where office-centric work becomes more decentralised. The increase in compliance risks may also be attributable to the human factor – not having a compliance officer walk the trade floor may be sufficiently tempting for some bad actors to exploit. Some such issues, however, should be fairly easy to mitigate, considering that most of the trade-related activities are automated (e.g., trades requiring a supervisor's approval, inability to breach thresholds, etc.). This is only the case, however, if the financial institution's IT infrastructure is not compromised.

---

[6] With intensified supervisory oversight, a revision in July 2020 to the 3LoD model, some commentators have for some time queried whether there is need for a new line and thus a move to a 4LoD model. For instance see: I. Arndofer, A.Minto, The "four lines of defense mode" for financial institutions. Financial Stability Institute Occasional Paper No 11. Bank for International Settlements, December 2015. The 4th Line is comprised of the financial institutions' mandatory external auditors, as well as their supervisors. It is perhaps an exaggeration to consider the statutory external auditors as an actual line of defense, as they focus mainly on the accuracy of financial data and reports, which is a form of control, but not to the extent to render the "creation" of a new line. Some more unorthodox control functions, however, may fit the 4LoD profile better – for instance the power in the Section 166 and 166a skilled persons review in the UK's Financial Services and Markets Act 2000, as amended, or the United States Federal Reserve's imposed monitors i.e., supervisors positioned on-site, which financial institutions are subjected to in case of significant deficiencies. Although these parties are external and, like the statutory external auditor, do not report to a firm's senior management, they do perform various reviews (incl. 2LoD and 3LoD testing and remediation validation work), oversee the implementation of controls, and very often give their opinion on the final status of the remediation efforts – e.g., by certifying that a certain remediation program is now complete, and the topic is no longer under intensified supervisory scrutiny. Hence, they (in-)directly also inform senior management about the risks and issues faced by the organisation and the progress made in addressing them.

[7] Further Background Briefings from PwC Legal's RegCORE on "Planning for prolonged pandemic preparedness – a primer for financial services firms for 2022" and on "Remote working: planning for beyond the COVID-19 pandemic" please see our dedicated Thought Leadership section

Moreover, standard client-related activities, such as client onboarding and Know-Your-Customer processes, can suddenly become a lot more risky and difficult to manage in while the 3LoD model is decentralised. There has been an increase in money laundering (ML) and terrorist financing (TF) risks because the COVID-19 crisis has opened up new possibilities and types of abuse (e.g. ML/TF disguised as donations to COVID-19 NGOs, etc., as well as a growing threat of ML and TF via video games or online platforms). The EBA has reminded financial institutions to continue monitoring transactions and to pay particular attention to unusual activities. Nonetheless, the relevant financial investigation units (FIUs) may not always be able to receive timely reports or assess the suspicious activities in a comprehensive manner. Notably, this may be the case, as the EBA pointed out, in COVID-19 impacted sectors such as cash intensive retail businesses and companies involved in international trade, etc. Although these examples may be appropriate under normal conditions, it is unclear whether consumers' actions are the same during the current pandemic, and what would really constitute "unusual" behaviour. For instance, many NGOs, businesses and private individuals have started campaigns to support local shops, products and industries. Similarly, with people practicing social distancing, and general issues relating to products' supply and demand, many purchases are made online via companies involved in international trade, located in somewhat exotic destinations. Thus, FIUs may be buried in an overwhelming amount of reports, or not be able to fully assess all ML/TF risks, as businesses, individuals and supervisors face the "new normal".

In response to such change in working environments as well as the continued impact and uncertainty caused by COVID-19, regulatory policymakers and supervisory authorities[8] have published various updates and measures, with the aim of mitigating the financial impact of the current situation, with most of the non-financial actions (i.e., recommendations/ guidelines, etc.) having a direct impact on the risk management environment (and thus the 3LoD model) of the financial sector. The EBA has emphasised the need for 'digital operational resilience' – business continuation, adequate information and communication technology capacity, security risk management and cyber security, based on an adequate internal governance and internal framework. This in practice means that control and risk officers across all lines might need to rethink their traditional activities and apply them in a completely digital environment. We expect to see a number of additional rulemaking instruments in 2022 and 2023.

In many ways this makes sense given that a lot of supervisory staff, much like the firms and staff that they supervise, are also working remotely often and possibly, for Banking Union supervisory authorities, not in Frankfurt or Brussels but back in their country of origin and/or in sunnier climes. Most notably, the EBA had urged all NCAs to plan their supervisory activities, including inspections, reviews, and other activities, in a pragmatic and flexible way, with the expectation to postpone those that are deemed non-essential. In this context, the EBA has recommended that supervisors make use of their supervisory tools to support but also to alleviate the immediate operational burden on firms within the respective sectors in their mandate.

This is particularly true when considering that most of the financial institutions had to quickly transition to remote operating models. In theory this should not have been a problem as financial institutions are meant to have business continuity options available (e.g., in case of a hurricane, prolonged power shortage, etc.) as set out in relevant business continuity plans (BCPs), as well as contingency plans, regardless of whether pandemic-specific planning was considered in both design and implementation. Irrespective of this, the majority of BCPs may never have been intended for prolonged situations such as the current COVID-19 crisis, where the majority of services are provided online and where most of the staff are working remotely.

Equally, risk owners (i.e., traditional business lines) are now under pressure to continue generating profit at times of financial stagnation. This could continue to lead to riskier market behaviour, for some firms at least, beyond the normal risk appetite of the given business line. At the same time, some EU initiatives, national reliefs, and communications from legislators and financial market rulemakers and supervisors focus on providing support, through new financial products but also forbearance for existing products.

[8] Notably the European Supervisory Authorities (the ESAs comprised of the European Banking Authority (EBA), European Securities and Markets Authority (ESMA) and the European Insurance and Occupational Pensions Authority (EIOPA)) as well as the Banking Union Supervisory Authorities such as the European Central Bank (ECB) at the head of the Single Supervisory Mechanism (SSM) and the Single Resolution Board (SRB) at the head of the Single Resolution Mechanism (SRM) along with the respective national competent authorities (NCAs).

Making 3LoD fit for purpose for the time ahead

In light of the above, what should firms do? If remote working and location-independent working is here to stay and co-exist with office-centric roles, then the 3LoD model that firms have had to adapt, often haphazardly, to such arrangements will also require changes to make sure it is fit for purpose in particular for prolonged pandemic preparedness and the new work mix persisting. Firms need to develop new policies, processes, practices, systems and controls to manage the new risk paradigm but also how to encourage good conduct from employees by adapting old controls so they are fit for purpose.

This approach also applies to the firm's broader internal control system i.e., the ICS that is used by the GRC and supports a firm's delivery of its TOM. Firms should not reduce vigilance on their controls across all LoDs. As additional risks arise, firms should consider it essential to maintain an environment that will provide comfort to the different internal stakeholders, management, clients and external parties that activities are being kept under control.

Handling execution gaps and ensuring consistency and appropriate documentation of controls are probably the biggest concerns when it comes to moving to a more permanent 3LoD, TOM and ICS on a paperless and remote working basis. Consequently, firms should closely monitor whether controls continue to operate effectively and rapidly adapt the way controls are performed and documented to make sure that all key controls can still be evidenced for upcoming reviews via the firm's GRC platform, which may be upgraded to use robotics, artificial intelligence, or any relevant digital support and technology as appropriate. There are a number of benefits to push for that investment now as opposed to postponing it to the future.

Some of those wider-reaching reforms might involve firms applying lessons learned but also pushing for bold new reforms such as:

1. Revisiting and amending their governance arrangements:
   a. To recalibrate the terms of reference on composition (in attendees) and frequency of meetings of boards and sub-committees, including to embrace the use of remote and/or hybrid meetings that are held along the lines of more equitable standards, with a greater efficiency and better audit trails (partly due to consensual recording);[9]
2. Increasing the frequency of periodic reassessments of their:
   a. policies and processes and amending them, where possible, to enable sustainable corporate governance arrangements as catered to the realities of the digital environment while not undermining debate in decision-making as well as set controls such as four-eye checks but also in assessing the resilience of the business, as well as the 3LoD's role in identifying, mitigating, measuring and managing risks from traditional vectors, but also the growing set of cyber-related threat vectors, which apply across the whole of a business offering, notably for those aspects that qualify, depending on the relevant regulators as "critical economic functions";
   b. IT infrastructure and consideration of the resilience of the systems to: (i) to provide remote access (to both clients and employees); and (ii) to maintain cyber security in light of the increased cyber and information risks. Furthermore, close attention should be paid also to the critical systems' availability and potential back-ups. The same also applies to how to facilitate multi-device support such as certain persons using tablets in addition to laptops to review documents due to inability to print large-scale meeting packs or other documents remotely. While welcome from a paper-reduction perspective, it does drive up the IT-penetration risk footprint;
3. Rethinking how control functions collaborate with the business units but also the interaction between 2LoD and 1LoD functions across jurisdictions and client types that are part of a firm's TOM. This includes adopting a more dynamic risk governance framework embracing:
   a. a risk tailored GRC management: in which a model should reflect the risk appetite, tolerance and internal constraints as they apply to business units and jurisdictions (as well lockdown and restriction realities) rather than apply a general overtly centralised approach;
   b. improved activity-based ownership: which means that it is not always 1LoD that owns all risk activity but instead that accountability is apportionment that allows fluidity between LoDs provided that accountability is assigned appropriately;
   c. a digital-first risk governance model: that applies digital solutions focused on reflecting the reality of the digital operating model, remote and/or location-independent working arrangements;

[9] At the outset of triggering crisis management measures, many firms called extraordinary meetings and ad-hoc internal meetings that on average lasted longer as firms scrambled for solutions. As firefighting turned to firms' moving to embrace more strategic planning, firms that moved to creating environments where remote and/or hybrid meetings allowed for greater dialogue (as opposed to dominance by certain actors) and better outcomes. Equally, a number of firms have found that the logistics and costs (including carbon footprint) of arranging and hosting meetings may cheaper and easier to organise in a remote setting. Issues however arise, where the persons in the (virtual) room have never met before or do not have a sufficient bond. These are in addition to problems such as connectivity, conference call fatigue, and absenteeism. Those issues might but there is no certainty that they will be overcome by the next generation of video conferencing including through virtual reality and metaverse solutions.

d. a more data-driven and technology empowered risk mapping and horizon scanning solution – which can streamline the risk assessment (including suspicious activity and transaction monitoring as well capture trends in financial crime, fraud and misconduct and regulatory responses) of firms as well as aligning preventive, detective and reactive capabilities of the firm on a risk-based proportionate approach that is agile and scalable when needed to support the operations across all LoDs;

4. Given the current set of challenges, firms may need to create additional controls from existing known areas of risk (specifically NFR and OR), as well as those that arise as a result of additional COVID-19 relief being offered by legislators and/or financial supervisory policymakers. The following GRC functions such as:
   a. the risk management function should be involved in the risk discussions and decisions of the business lines and management to inform them whether these remain within the risk appetite and strategy of the firm in particular as COVID-19 changes behaviour. The risk management function also needs to frequently re-run its assessment of the risks in this crisis period to ensure all risks are identified in due time and fit in within the risk appetite framework and risk tolerance levels;
   b. the compliance function, which should be alerted to changes in customer behaviour (social risks). Firms should revise the thresholds applied to transaction monitoring to detect suspicious and/or financial crime such as laundering activities, while making sure that the volume of alerts remains manageable – in particular while resources are operating on a remote working basis. The detection of illegal transactions compared to legitimate activities is particularly difficult, and in the current operating conditions, several opportunities arise for criminals to exploit the existing vulnerabilities of people, processes and systems (e.g., fraud attempts such as raising funds for fraudulent charities);
   c. the internal audit function should consider the direct and indirect risks identified by management, starting from the assessment of the measures to ensure continuity (crisis management), then verifying that associated risks and medium to long-term implications have been considered.
5. Setting up lines of communication bilaterally or via industry associations with contacts at peers but also with competitors, so as to align actions and share, including via external counsel, best practice, as well as to scenario plan potential reforms advanced by supervisors and reviewing the measures taken above in both an agile and dynamic manner.

While some of the considerations above may be in various stages of development across financial services firms, some of the changes and improvements in adapting the 3LoD and/or the Three Lines Models will continue to evolve. A strong risk culture is now more crucial than ever for financial services firms regardless of sector and business model. Such culture includes risk awareness, risk management and related risk-assessment decisions. Specifically, this may also include embedding risks within behaviour, attitudes and norms, which may help to overcome the difficulties firms will face.

The tone from the top i.e., from the executive and management function is one of the key drivers to reinforce risk culture, supported by the tone from the middle to ensure important messages cascade across and into the organisation as well as driving the risk culture from the bottom-up albeit this becomes difficult where such efforts are only set in the virtual boardrooms or townhall meetings.

Lastly there are areas of the 3LoD model whether in the office-centric or new work mix that may be missing across certain firms. Specifically, this extends to ESG and climate risks as overarching issues affect financial services firms. As a response, some firms have taken the options in:

1. Defining their approaches and responsibilities to ESG and climate risk. This extends to client, customer and third-party relationships as well as the policies, procedures and overall mandates and strategies both for in the office-centric and remote-working environment;
2. Developing an ESG roadmap and overarching strategy with defined targets and timelines to incorporate climate risk and ESG decision making and reporting. This however raises concerns as to whether a company can and indeed should extend into private arrangements of employees in their respective remote-working arrangements; and
3. Preparing to embed horizon scanning and risk-mapping of ESG risks and implementing new and adapting existing relevant policies and processes to identify, mitigate and manage those ESG and climate risks as they apply to a specific firm as well as what expectations the firm and employees should meet.

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from these announcements as well as those in the pipeline ahead of the next supervisory cycle. If you would like to discuss any of the items mentioned, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal's RegCORE Team via: de_eufinreg@pwc.com.

Contact

Dr. Michael Huertas LLM., MBA
Partner, Head of Financial Institutions
Regulatory Europe
PwC Legal Deutschland
Mobile: +49 160 9737-5760
michael.huertas@pwc.com

About us

In today's rapidly evolving marketplace, our clients are increasingly concerned with business collaborations, restructuring, mergers and acquisitions, financing and questions of social responsibility. They need legal security when dealing with such complex issues. That is why we work closely with PwC's tax, human resources and finance experts and draw on the resources of our legal network in more than 100 countries to deliver comprehensive advice. Whether a global player, a public body or a wealthy individual, each client can rely on a personal account manager to address his or her specific legal needs. This dedication helps us ensure our clients' long-term business success.

PwC Legal. More than 220 lawyers at 18 locations. Integrated legal advice for the real world.