大成 DENTONS

Re-assessing the Three Lines of Defense (3LoD) model during a time of continued crisis and remote working

May 6, 2020

QuickTake:

COVID-19 has changed how and where compliance is managed. Office space has largely been exchanged for an assortment of living rooms and remote working spaces. Regardless of an eventual return to normality, the new normal may be quite different to what was previously accepted operating conditions for financial services firms, as well as the internal and external threat factors and failings that pose a risk to a financial services firm's resilience. This will likely prompt a re-think by all types of firms, regardless of business sector and/or model, of how to run systems that identify, mitigate, measure and manage the set of risks they are faced with. Combined offerings from RegTech providers and external counsel may assist firms in moving to a more digital enabled 3LoD model that is equally required to work remotely as well as cope with the range of challenges posed from prolonged working from home arrangements.

Introduction

Before it made its appearance in the financial services sector, the so called "Three Lines of Defense" *(**3LoD**)* model[1] had already been utilized by the military, in sports, and other fields. It also became a focal point of financial institutions' corporate governance, as it gives structure and defined roles, enabling (i) companies to better manage their business needs and staff; (ii) employees to perform their tasks in a clear(er) chain of responsibility; and (iii) supervisors and management to identify risks for the firm in question. Since various previous crises, 3LoD has, now firmly taken center stage in financial services target operating models (**TOM**s). It has rarely had to face, however, the challenges posed by preparing for prolonged pandemics.[2]

Good corporate governance could be described, inter alia, as a well-structured organization with pre-defined roles, responsibilities, policies and procedures, and that there is no need to further "branch out" a portion of the overall risk framework into a separate model – i.e. the 3LoD model. Moreover, as corporate governance has been dubbed by the De Larosière Group[3] as *"one of the most important failures"*[4] that led to the 2007- 2008 Global Financial Crisis (**GFC**), it is important to understand that a financial institution that lacks mechanisms to ensure a strong risk management framework and a clear separation of roles and responsibilities, lacks good corporate governance. Therefore, the 3LoD model and good corporate governance are intertwined, as the former supports the latter, should there be a good corporate governance in place, or facilitates its creation, where one is lacking.

Consequently, sound 3LoD and operational risk (**OR**) frameworks have become essential to what is deemed to be a viable financial institution with good corporate governance. And if corporate governance was put to the test with the GFC, the 3LoD model is now facing its own test with the socio-economic impact of the COVID-19 crisis, as financial services firms and their counterparties and clients are facing challenges that they may have never considered, or at least not ones of such a magnitude.

These issues are very different in their nature and include corporations having to focus on business continuation at a time when their employees are working remotely, at risk of new elaborate money laundering schemes seeking to exploit the weakest (usually human element) part of the chain, which can lead to compliance failings. There is also pressure from businesses and also from end-consumers and (partially) supervisors, which all expect financial institutions to be able to cope in a digital operating model performing in ways they never considered before. This Background Briefing looks at some of those issues, as 3LoD may need a rethink as firms continue to operate under what may be a very different set of operating conditions.

1 In the context of financial institutions, the term was first coined by the UK's Financial Services Authority (**FSA**) - now the Financial Conduct Authority, 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 See coverage available **here**.

3 The High-Level Group on Financial Supervision in the EU was tasked by the European Commission with the question how to organize financial institutions and markets supervision following the GFC; how to strengthen European cooperation on financial stability oversight, early warning and crisis mechanisms and how EU supervisors should cooperate globally. For more see: High-Level Group on Financial Supervision in the EU, *Report,* 25 February 2009, Brussels.

4 *Ibid,* pg. 29.

The 3LoD model

The 3LoD model became a prominent element in financial institutions' OR frameworks in the post-GFC period, when various rules and regulations were introduced at the European Union (**EU**) and EU Member State level. It goes without saying, however, that financial institutions were already utilizing some types of 3LoD models prior to the GFC, and in fact supervisors did encourage their use. Nonetheless, OR management only emerged as an important type of risk at the beginning of this millennium[5] and naturally financial institutions developed various approaches to OR management. Consequently, the early forms of the 3LoD model varied in terms of staffing, roles and responsibilities, degree of independence and separation of lines[6].

In short, the traditional 3LoD model separates a financial institution into the following three lines with their own unique role and responsibilities[7]:

- **First Line of Defense (1LoD)** – the line that owns and manages the risk. Traditionally, it includes the business lines, but every function is a risk owner for the risks it produces;
- **Second Line of Defense (2LoD)** – functions responsible for risk control and risk management. Normally, it includes functions such as Risk, Compliance, HR, Legal, etc.
- **Third Line of Defense (3LoD)** – provides independent assurance and internal audit.

Although the 3LoD model is already fairly standardized, certain aspects of the overall framework remain open to interpretation and debate. For instance, if the 3rd Line of Defense (i.e. internal audit) identifies control deficiencies in the 1st LoD (i.e. the business), does that only reflect issues within the said line or does it also showcase a weak 2nd Line of Defense? On 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.

As many of the critics of the 3LoD model have argued, there is 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

5 The Basel Committee on Banking Supervision (**BCBS**) initiated its work on OR in 1998, noting that managing OR is becoming an important feature of sound risk management. For further information see: Basle Committee on Banking Supervision, *Operational Risk Management*, Basle Committee Publications, September 1998.

6 For example, the FSA has noted, as part of its 2003 OR observations publication, that where firms had a centralised OR function, they would always involve that function in developing OR strategy & policy, but less than half of those functions will be involved in managing OR events and only 11% would include the OR function in reviews or management of information security. For further information see: Financial Services Authority, *Building a framework for operational risk management: the FSA's observations, Annex 1 Detailed Findings,* FSA, 2003. pg. 10.

7 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. For further see: Institute of Internal Auditors. *IIA Position Paper: The Three Lines of Defence in Effective Risk Management and Control.* January 2013.

2LoD and the 3LoD can pick up the slack as they are primarily tasked with identifying the 1LoD gaps and issues. 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 extend 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).

Overly zealous control functions, however, are equally challenging. In a perfect world, the control frameworks would be ideal and there would rarely be risk events. 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, especially if they are only emerging Furthermore, imposing 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.

With the evolving of the 3LoD model and the intensified post-GFC supervisory oversight, however, a new "line" has emerged, prompting certain authors[8] to question whether it is time for a 4LoD model to be created. The so-called "fourth line of defense" 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[9] 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[10] also inform senior management about the risks and issues faced by the organization and the progress made in addressing them.

Supervisors further engage with financial institutions and their risk frameworks when discharging their supervisory mandate; namely through the various off-/on-site inspections, reviews, reports and other binding legal decisions and instructions. Consequently, supervisors have an impact on an institution's control environment that may go beyond what is the traditional supervisory exchange. For instance, supervisors can and often do mandate how certain issues should be remediated, influencing the control environment design (i.e. something that is traditionally performed by the 2LoD); supervisors further review, validate and issue findings in relation to risks identified across the organization (i.e. the traditional task of internal audit).

Last but not least, with the creation of the Banking Union's Single Supervisory Mechanism (**SSM**) and with the tone set by the European Central Bank

8 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.

9 s.166 and s.166a skilled persons review as envisaged in the UK's Financial Services and Markets Act 2000.

10 Traditionally the s.166 Skilled Person Review does not include follow-up status reports and feedback. Remediation programs relating to an ECB Supervisory Decision, however, are often followed up on via the so-called "Follow-up Letters", which are non-legislative acts, that, inter alia, are used for providing the ECB's view on the progress made on specific issues. For further information see: ECB. *Gide to on-site inspections and internal model investigations*. September 2018

(**ECB**), Joint Supervisory Teams (**JSTs**)[11] have been engaging more actively in a supervisory dialogue with the relevant financial institutions. This, however, is sometimes challenging as JSTs are composed of supervisors that come from (sometimes very) different supervisory cultures — ranging from a more advisory-style open dialogue to prescriptive formal communications. Even if this is set for continued change as the Banking Union and indeed the European Supervisory Authorities (**ESA**s) (notably EBA, ESMA and EIOPA) strive to build a more unified supervisory culture underpinning the EU's Single Rulebook for financial services, their understanding of the 3LoD itself is often different. Irrespective of these efforts, a financial institution may receive two competing instructions pertaining to the same issue (e.g. two on-site inspections identify similar compliance issues but provide different requirements as to how these should be addressed). Furthermore, supervisors may have different views as to what the role of the 2LoD and the 3LoD should be in a firm – notably whether a 1LoD deficiency is also reflective of a 2LoD problem or not, who should address it and how invasive should the internal audit be.

Despite its challenges, the increased supervisory dialogue is, nevertheless, a welcome development, as it enables firms to address certain supervisory concerns proactively (as opposed to reactively). This is particularly true in the situation of an ongoing crisis, such as the current COVID-19 pandemic. Consequently, firms are able to discuss certain concerns or issues they face with their supervisors, and find acceptable solutions that are in keeping with the respective regulatory rules but also supervisory expectations of various members of the European System of Financial Supervisors (**ESFS**), comprised of ESAs and national competent authorities (**NCA**s), both in the EU-27 as well as those (currently) 19 Member States that comprise the Banking Union.

11 Joint Supervisory Teams are responsible for the supervision of Eurozone-19 significant financial institutions that are directly supervised by the ECB. They are comprised of ECB employees and staff members of the various national competent authorities of the Eurozone-19 member states. For further information regarding the JSTs and their tasks, please see: *Ibid.*

COVID-19 risk challenges

In addition to the outlined challenges, the 3LoD model is currently under a completely different test, as financial institutions and ESAs[12] are confronted by the all-encompassing socio-economic crisis caused by the COVID-19 pandemic. All of the ESAs have provided 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, 3LoD model) of the financial sector. Most notably, the European Banking Authority (**EBA**) has 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[13].

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.[14] *T*his 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. Consequently, the COVID-19 crisis has also put the 3LoD model to the test, with financial institutions meant to provide smooth operations (i.e. business as usual), but at a time when business has suddenly become a lot riskier.

Risk owners (i.e. traditional business lines) are now under pressure to continue generating profit at times of financial stagnation. This could lead to riskier market behavior 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. This is a very new and fast-changing environment for business units, their counterparties, clients and the communities they serve, but also for control functions of those firms. It also poses risks beyond just financial crime but also regulatory, reputation and legal risk in the event of (or certainly perception of) misselling and/or deteriorating advice standards.

Moreover, it is unclear whether business lines understand what their actual risk tolerance is. 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. Thus, the control environment is arguably weakened, whilst firms are unlikely to revisit their set risk appetite threshold, allowing the 1LoD to operate in a situation where risk is perhaps underestimated.

In addition, the EBA has emphasized 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[15]. This in practice means that control and risk officers across all lines need to rethink their traditional activities and apply them in a completely digital environment. We expect to see a number of additional rulemaking instruments

12 The ESAs are the European Banking Authority, the European Securities and Market Authority and the European Insurance and Occupational Pensions Authority.

13 EBA. *EBA statement on actions to mitigate the impact of COVID-19 on the EU banking sector.* 12 March 2020 < **https://eba.europa.eu/eba-statement-actions-mitigate-impact-covid-19-eu-banking-sector** >

14 Ibid.

15 The term is used by the EBA in relation to its supervisory measures relating to the COVID-19 crisis. For further information see: EBA. *EBA statement on additional supervisory measures in the COVID-19 pandemic.* 22 April 2020. pg. 6.

published by the EU's co-legislators, as well as new supervisory expectations of the **ESFS**.

An effective risk management framework in a digital operating model (**DOM**), however, is also subject to increased information security risks, both from traditional but also cyber-related threat factors and bad actors. These range from ensuring that all critical activities are available and functional, to having numerous employees work remotely at the same time. These cybersecurity threats have been rising, making the resilience of the DOM, reliant on remote working arrangements, ever more pressing.

Information- and cybersecurity, however, also pose additional reputational risks to both the financial institutions and their supervisors, as many contingent matters and confidential supervisory exchanges need to take place digitally. Hence, there is a reputational risk increase on both ends of the supervisory spectrum.

With regards to supervisory activities, there are also additional regulatory risks relating to the ability to carry out online supervision. Having supervisory inspections (or internal audit reviews) conducted over telephone- and videoconference is not a novelty, as most large financial institutions have key personnel in multiple locations. However, those exchanges are usually carried out from the firm's premises across the globe and/or the supervisors' own offices. In the COVID-19 DOM, however, it is likely that most individuals involved would not have access to secure lines or that confidentiality cannot be ensured (e.g. avoiding one's spouse in a shared household during a lockdown may be impossible). This prompts the question whether supervisors should be pragmatic or undertake only those activities that could be maintained via secure emails or appropriately hosted platforms. This is in addition to more mundane questions around the threat factor resilience of certain collaboration and/or video-conferencing platforms, which have had known weaknesses published.

Managing compliance risks

The question of increased cybersecurity risks also relates to another prominent issue that financial institutions face in the COVID-19 crisis – managing their compliance risks. Certain aspects of the increase of compliance risks may be attributed to the human factor – not having a compliance officer walk the trade floor may be sufficiently tempting for 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.

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. 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). In this context, financial institutions need to strike a balance between the EU's 5th and 6th AML Directives[16] — which were due to be transposed and subsequently applied in all European Union (**EU**) member states (**MS**s) by January 10, 2020 and what is really achievable in terms of reporting and managing ML/TF risks in a DOM situation[17].

The EBA has reminded financial institutions to continue monitoring transactions and to pay particular attention to unusual activities. Nonetheless, the relevant financial investigation units (**FIU**s) 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.*[18] Although these examples may be appropriate under normal conditions, it is unclear whether consumers' behavior is the same during the current pandemic, and what would really constitute "unusual" behavior.

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".

16 Directive (EU) 2015/849 of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council, and repealing Directive 2005/60/EC of the European Parliament and of the Council and Commission Directive 2006/70/EC (OJ L 141, 5.6.2015).

17 Notably, the Financial Action Task Force (FATF)'s President has issued a statement related to COVID-19 measures to combat illicit funding, where it was noted that the use of digital identity as a trustworthy method to on-board clients improved the security and convenience of identifying people remotely. Nonetheless, the recently issued FATF Guideline on Digital ID (FATF. *Digital Identity.* March 2020), recognised that most countries are yet to explore the use of digital identity in the area of financial transactions and ML/TF management. For further information, see: FATF. *Statement by the FATF President: COVID-19 and measures to combat illicit funding.* 1 April 2020 <**https://www.fatf-gafi.org/publications/fatfgeneral/documents/statement-covid-19.html**>.

18 EBA. *EBA statement on actions to mitigate financial crime risks in the COVID-19 pandemic.* 31 March 2020 < **https://eba.europa.eu/sites/default/documents/files/document_library/News%20and%20Press/Press%20Room/Press%20Releases/2020/EBA%20provides%20additional%20clarity%20on%20measures%20to%20mitigate%20the%20impact%20of%20COVID-19%20on%20the%20EU%20banking%20sector/Statement%20on%20actions%20to%20mitigate%20financial%20crime%20risks%20in%20the%20COVID-19%20pandemic.pdf** >.

Thoughts for the time ahead

The past decade has seen the raise of the 3LoD model, with its ability to provide structure and accountability. Nevertheless, many have also called for its review, due to the overlapping nature of certain roles, namely in relation to risk management and control functions, which can often give a sense of diluted personal responsibility. Last but not least, the intensified supervisory engagement has further impacted the 3LoD model and its practicalities – something that will continue in the future, irrespective of whether a 4LoD model is introduced or the concept is abandoned all together.

Despite the various debates regarding the 3LoD model, what would perhaps influence its future structure the most is the COVID-19 crisis, as it forces financial institutions to operate according to a completely different model – a digital one. This might make financial institutions a lot more 'virtual-bank'-oriented, or perhaps we will see the rapid integration of FinTech/ RegTech into the traditional financial services sector. Combined offerings from RegTech providers and external counsel may assist firms in moving to a more digital enabled 3LoD model that is equally required to work remotely as well as cope with the range of challenges posed from prolonged working from home arrangements.

In the meantime, however, financial institutions need to address some pressing issues that the COVID-19 crisis has brought to bear upon their 3LoD operating model. Namely, financial institutions should reassess their policies and process and amend them, where possible, to enable sustainable corporate governance in a digital environment. This exercise might prove to be difficult to accomplish, however, as it requires careful consideration, in order to ensure that the control environment is not compromised – e.g. one can move to weekly committee meetings with shorter agendas and "lighter" decision making processes, but should never undermine controls such as four-eye checks.

As their IT infrastructures are also put to the test, financial institutions should assess its capacity on an ongoing basis, considering the systems' capabilities: (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.

As reviews of policies and procedures, as well as IT infrastructure overhauls, can be lengthy (and often costly processes), financial institutions should also focus on their corporate governance and ensure that people across all lines of defense understand what their role and responsibilities entail during a time of crisis. This could be achieved via increased senior management communications, clear guidelines, awareness and training campaigns.

In addition, financial institutions and supervisors should demonstrate readiness to be flexible to adapt to the challenges that the COVID-19 crisis presents. This includes the introduction of mechanisms to mitigate employee-related risks, such as those regarding stress management and job-redundancy concerns. Last but not least, firms should consider introducing simplified escalation processes and employee-feedback options, as many may face new challenges, and the 3LoD model is only as good as employees' ability to address issues in a timely manner (especially at times where the IT infrastructure may fail).

Considerations for financial services firms

In light of the above, what might financial services firms consider doing? While some of these questions are likely to require solutions, developed with external counsel, that are driven by firm-, business sector-, jurisdiction and TOM-specific models, there are some common considerations that may merit earlier action over the shorter-, medium- but also over the longer-term. These include firms:

1. Reviewing the fitness of design and implementation of their 3LoD model and its efficacy in preventing and/or controlling risks, as well as supporting remedial action;
2. 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 ESFS but also global regulators, as "critical economic functions";

3. Rethinking how control functions collaborate within that community but also with 2LoD and 1 LoD functions across the various business lines, jurisdictions and client types that are part of a firm's TOM;
4. Given the current set of challenges, firms may need to create additional controls from existing known areas, as well as those that arise from additional COVID-19 relief being offered by legislators and/or financial supervisory policymakers. This may also include further adaptation of internal escalation channels to emphasize clear and rapid communication, redoubling efforts on raising awareness across all levels and stakeholders (from board to individual business unit) of compliance and risk culture and values, as well as strengthening, as required by supervisors, whistleblowing channels19 to prevent malfeasance;
5. Reviewing and revising existing policies and procedures, rolling-out new ones, as well as new systems and controls, to account for findings from points 1 and 2, including the move to a new "new normal" in how firms operate and engage with clients and counterparties in the communities they serve; and
6. Setting up lines of communication bilaterally or via industry associations with contacts at peers but also competitors, to align their 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 above may be in various stages of development across financial services firms, some of the changes and improvements in adapting the 3LoD model to the new operating environment will likely require careful and coordinated engagement across a range of internal stakeholders, and also with various components of the ESFS, where external counsel can help assist an expedient design and deployment of those deliverables.

We hope the above may provide some further insight into how to approach some of the solutions needed for what are indeed extraordinary times and very much new legal and operational challenges.

Our **Eurozone Hub** and Dentons Financial Institutions Regulatory lawyers have long advised and are advising a number of financial services firms across multiple jurisdictions in respect of their various stages of design and deployment of their BCP and contingency measures, as well as their outreach measures in respect of counterparties, clients and other stakeholders (suppliers, auditors and supervisors).

The measures developed for our financial services clients translate into direct lessons learned that are deployable to the wider body of corporates that we service across the globe across various different areas. We equally have a depth of expertise in assisting clients with their applications to secure EU and national-level funding packages of various different types.

In addition to speaking to your usual Dentons' contact please **contact our global taskforce** for a fast response on any COVID-19 issue you may have. Details of full COVID-19 relevant coverage are available on our **COVID-19 (Coronavirus) Hub**.

We stand ready to support you in navigating these issues and how they apply to your business operations and those of your clients. We wish you and your families both comfort and strength during these unprecedented times.

19 See *inter alia* coverage from our Eurozone Hub available **here**.

KEY CONTACT

Dr. Michael Huertas
Partner, Co-Head Financial
Institutions Regulatory Europe
D +49 69 45 00 12 330
michael.huertas@dentons.com

ABOUT DENTONS

Dentons is the world's largest law firm, delivering quality and value to clients around the globe. Dentons is a leader on the Acritas Global Elite Brand Index, a BTI Client Service 30 Award winner and recognized by prominent business and legal publications for its innovations in client service, including founding Nextlaw Enterprise, Dentons' wholly owned subsidiary of innovation, advisory and technology operating units. Dentons' polycentric approach, commitment to inclusion and diversity and world-class talent challenge the status quo to advance client interests in the communities in which we live and work.

dentons.com

CSBrand-25304-Client alert (COVID-19) - Re-assessing the Three Lines of Defense (3LoD) -02 — 06/05/2020