RegCore Client Alert

Revisiting EMSA's 2020 Guidelines on the MiFID II compliance function and applying lessons learned

July 2023

Financial Services

Revisiting ESMA's 2020 Guidelines on the MiFID II compliance function and applying lessons learned

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas
@pwc.com

Contact RegCORE Team
de_regcore@pwc.com

QuickTake

Financial services firms (and their senior management) are required to maintain a permanent and effective compliance function that in turn is required to carry out various duties and responsibilities.[1] Various firms, notably those in-scope of the EU's Directive 2014/65/EU (**MiFID II**) have also, since 5 September 2020, had to comply with supervisory expectations on the MiFID II compliance function as set out in the "**Guidelines**"[2] published by the European Securities and Markets Authority (**ESMA**). These 2020 Guidelines replaced similar guidelines issued by ESMA in 2012 and updated principles therein to enhance clarity and foster greater convergence in the implementation and supervision of the compliance function amongst firms that are "in-scope" for the purposes of the 2020 Guidelines (**In-scope Firms**).

The Guidelines are addressed to competent authorities i.e., supervisory authorities (collectively **NCA**s) and certain financial market participants in order to establish consistent, efficient and effective supervisory practices within the European System of Financial Supervision (**ESFS**) and to ensure the common, uniform and consistent application of certain aspects of the MiFID II compliance function. In-scope Firms need to thus take into account the expectations set in the Guidelines as well as the national level frameworks into which the Guidelines have been included and any additional jurisdiction-specifics set by the respective NCAs pursuant to their own mandate, some of which may, despite the Guidelines, differ between NCAs where these fall outside of the scope of the Guidelines.

Following a continued inflow of new entrants as well as new types of In-scope Firms into the EU, whether as a result of Brexit or otherwise, coupled with a raft of legislative/regulatory compliance (along with financial crime) failings across established firms, both large and small, complex and non-complex, it should come as no surprise that EMSA and the NCAs are increasing their focus on In-scope Firms meeting the Guideline's

[1] See Article 22 of Commission Delegated Regulation (EU) 2017/565 as available, as at the time of writing hereof, in the last consolidated updated version (dated 2 August 2022) available here.
[2] Available here as (last) updated in the binding version of the Guidelines dated 6 April 2021, which updates the version first published by ESMA as a Final Report on 5 June 2020. Please also see compliance table of EU Member States NCAs as (last) updated 13 October 2022 available here.

outcomes. More importantly, the ESFS is likely to become even more strict and intrusive following relevant authorities' return to "supervision as normal" following the end of the COVID-19 pandemic. In-scope Firms will want to assess whether they are (still) doing enough to meet the baseline expectations of the Guidelines as well as the jurisdiction-specifics and individual expectations as set by the NCAs that supplement the Guidelines' outcomes.

This Client Alert revisits the contents of the Guidelines considering the lessons learned as the role and challenges of the compliance function has considerably changed since 2020. This Client Alert should be read in conjunction with other analysis from our EU RegCORE notably on changes to the three-lines of defence (**3LoD**) model following the impact of COVID-19 pandemic and the longer-term adoption of remote and/or hybrid working arrangements. This Client Alert should also be read in conjunction with developments around crypto-assets, as a number of crypto-asset service providers may well apply for authorisations that mean they become an In-scope Firm for purposes of the Guidelines.

A closer look at the Guidelines and lessons learned since 2020

ESMA uses the Guidelines to specify the common supervisory expectations applicable to the compliance functions at the following In-scope Firms:

1. Investment firms when carrying out in MiFID II/MiFIR and IFD/IFR "investment services" or "investment activities" or when selling or advising clients in relation to structured deposits;

2. Credit institutions (i.e., banks) when carrying out in MiFID II investment services or investment activities or when selling or advising clients in relation to structured deposits;

3. Undertakings for collective investment in transferable securities (**UCITS**) management companies when providing services in Art. 6(3) of the UCITS Directive i.e., portfolio management; and

4. Alternative investment fund managers (**AIFMs**) when providing services referred to in Article 6(4) of the AIFMD i.e., portfolio management.

The Guidelines are structured to focus on different aspects of the compliance function and its efficiency in its operations. It remains firms' (and senior management at those firms) individual responsibility to actively keep track on the performance of their compliance function through an internal compliance risk assessment.

As detailed below, the Guidelines are specific in their supervisory expectations however, in light of not having been updated since 2020, this may raise a number of questions in light of how the COVID-19 pandemic and the longer-term adoption of remote and/or hybrid working arrangements have had an effect on the compliance function. In particular both the ESFS and In-scope Firms may want to revisit and demonstrate that the compliance function and its target operating model (**TOM**) is performing against the expectations set in the Guidelines in particular as to what the compliance function is being tasked to do, how and where, notably where remote/hybrid working extends the 3LoD model well beyond its traditional "office-centric" set-up.

Moreover, the fact that the Guidelines have also not been updated since 2020 but major legislative reforms have been entered into force since then is also grounds to warrant In-scope Firms to revisit their arrangements. Some of these recent reforms include those affecting MiFID II (such as IFR/IFD and the introduction of both quantitative and qualitative "K-Factors") as well as those extending the scope of "financial instruments" to include certain eligible crypto-assets and respective activity (see our coverage on MiCAR) as well as a wider-reaching supervisory focus on third-party risk management and (digital) operational resilience. These considerations may be of importance for both those compliance functions at established In-scope Firms inasmuch as it is at newly licensed In-scope Firms both when setting up a permanent, effective and independent compliance function and maintaining and adjusting it according to the specific risks faced over time.

Guideline	**Summary of requirements**	**Lessons learned since 2020 - Observations from PwC Legal**
Guideline 1 (compliance risk assessments)	An In-scope Firm's compliance function must: a. conduct a formal compliance risk assessment (evaluated on a regular basis to ensure fit in design and fit for purpose) (the **CRA**) to make sure that compliance risks are thoroughly managed;	1. The various components and levels in the ESFS have continued to identify a number of compliances along with financial crime failings, shortcoming and near misses. A number of supervisory warnings, sanctions and

Guideline	Summary of requirements	Lessons learned since 2020 - Observations from PwC Legal
	b. establish a risk-based compliance monitoring programme (the **CMP**) on the basis of the CRA to determine the compliance function's priorities and the focus of the monitoring, advisory and assistance activities including the allocation of the compliance functions resources efficiently; c. when identifying the level of compliance risk that the firm faces, take into account all the areas of investment services, activities and ancillary services provided by the firm. This should include the types of financial instruments traded and distributed, the categories of a firm's clients, the firm's distribution channels, and, where applicable, the internal organisation of the group; d. ensure that the CRA encompass MiFID II, national implementing laws, and the firm's investment services and activities policies, procedures, systems, and controls. Monitoring outcomes and relevant internal or external audit findings should also be considered; and e. account for new risks (e.g., from new business fields, firm structure changes, or regulatory changes), the identified risks should be reviewed regularly and ad hoc.	enforcement measures have been directed not only to the firm but also its senior management and equally the compliance function in particular for having insufficient resources and/or competencies as well as for lack of in-depth controls. Such developments can also have wider-reaching reputational risk for the firm and adverse implications for the firm's viability in certain markets and in exceptional circumstances its solvability. 2. Not all of these issues highlighted above are perhaps as adequately reflected in the CRA or CMP or the wider obligation on identification, mitigation and management of compliance risk as comprehensively nor as frequently nor subject to sufficient granular or reliable data as might be warranted or as deemed desirable by respective supervisors. Getting this balance right is at the forefront of supervisors when assessing financial service firms' respective compliance as well as overall business TOM and the wider strategic steering of the specific firm continues to respond to various different ways of working and new ways of engaging with counterparties, clients and customers they serve.
Guideline 2 (compliance monitoring)	a. In-scope Firms must ensure that the CMP assesses whether the firm's business is conducted in compliance with its obligations and whether internal policies and procedures, organisation and control measures are effective and appropriate to monitor compliance risk. b. Where an In-scope Firm is part of a group, responsibility for the compliance function rests with each entity in that group. An In-scope Firm should therefore ensure that its compliance function remains responsible for monitoring its own compliance risk. This includes where an entity outsources compliance tasks to another entity within the group. The compliance function within each entity should, however, take into account the group of which it is a part - for example, by working closely with audit, legal, regulatory and compliance staff in other parts of the group. c. In-Scope Firms must use a risk-based approach to compliance so as to determine the compliance function's tools, methodologies, monitoring programme, and frequency of monitoring activities (recurring, ad hoc, or continuous). The compliance	1. The various components and levels in the ESFS have continued to express concerns that policies and procedures are often not seen as "living documents", both across individual entities and generally in a group setting, and that CMPs fail to challenge the risks from policies and procedures in particular where they subject to a "file and forget" approach and where they individually as well as collectively do not reflect the then current legislative and regulatory requirements along with the respective supervisory expectations as well as the actual day-to-day operation of the respective business units and control functions. 2. Some NCAs have expressed concern that the updates of policies and procedures are "pushed" to the compliance function by stakeholders who should be owners of policies and procedures of a specific area and where the compliance function's role is

Guideline	Summary of requirements	Lessons learned since 2020 - Observations from PwC Legal
	function should also conduct on-site business unit inspections to verify policy and procedural implementation. Compliance should also consider the scope of reviews to be performed. d. The CMP should reflect changes to the In-scope Firm's risk profile, which may arise, for example, from significant events such as corporate acquisitions, IT system changes, or reorganisation. It should also extend to the implementation and effectiveness of any remedial measures taken by the firm in response to breaches of MiFID II, related delegated or implementing acts and/or any national implementing provisions thereof. e. The compliance function's monitoring activities should also take account of: (1) the business area's obligation to comply with regulatory requirements; (2) the first level of controls in the firm's business areas (namely controls by the operative units, as opposed to second level controls performed by compliance); and (3) reviews by the risk management function, internal audit function or other control functions in the area of investment services and activities. f. Reviews by control functions should be coordinated with the monitoring activities performed by the compliance function while respecting the different functions' independence and mandate. g. The compliance function should have a role in monitoring the operation of the complaints process and it should consider complaints as a source of relevant information in the context of its general monitoring responsibilities. This does not require the compliance function to have a role in determining the outcome of complaints. In this regard, firms should grant the compliance function access to all customer complaints received by the firm.	to focus on the design and efficacy of controls. 3. Some NCAs have expressed concern that CMPs and a risk-based compliance approach inadequately reflects the new risk types and threat channels that arise from remote/hybrid working – in particular from a financial services compliance as well as tax and HR perspective. A version of PwC's **Remote Work Assistant** has been specifically modified for use by financial services clients, and more broadly In-scope Firm's compliance functions should consider setting up definitive remote/hybrid working policies that establish principles applicable to the overall firm's TOM and how the 3LoD model operates in a non-office centric environment. 4. Some NCAs have identified inadequacies in differentiating clear allocation of responsibilities and mandates across the various control functions and components of the 3LoD model and what this means for accountability and minimisation of near misses. 5. Further weaknesses in appropriate (regulated) complaints management continue to extend across the market. This has been accentuated by the COVID-19 pandemic and equally is set to rise further with financial service firms (not just In-scope Firms) moving to meet the EU's Retail Investment Strategy as well as individual EU Member States reviewing and reforming standards and supervisory expectations applicable to retail client facing business as well as wider-reaching risks for firms in light of the EU's collective action legislative framework.
Guideline 3 (reporting obligations)	The expectations set in Guideline 3 focus on a firm producing for the management's review "mandatory compliance reports" in respect of all business units involved in the provision of investment services, activities, and ancillary services provided by the firm. Such reports must cover at least those items highlighted in para. 28 of the Guidelines and (ideally) grouped by the headings outlined therein. Where a report does not cover all of the activities and services of the In-scope Firm it should clearly state the reasons why it does not.	As the various components of the ESFS, in particular ESMA, and its sister European Supervisory Authorities continue to advance data-driven reporting as a core tenant of its annual supervisory as well as enforcement work programmes as well as common supervisory actions, the importance of comprehensive and suitably granular regulatory reporting on compliance risks, performance of the compliance function and its tasks remains paramount.

Guideline	Summary of requirements	Lessons learned since 2020 - Observations from PwC Legal
Guideline 4 (advisory and assistance obligations of the compliance function)	a. In-Scope Firms should promote and enhance a 'compliance culture' throughout the firm, which should be supported by the senior management. The compliance function should monitor whether relevant staff have the necessary level of awareness and correctly apply the relevant policies and procedures. b. In-scope Firms should ensure that the compliance function fulfils its advisory and assistance responsibilities, including providing (i) support for staff and management training on an on-going and ad hoc basis and update training as appropriate according to needs, changes in business model and legislative/regulatory developments; and (ii) day-to-day assistance for staff and management and participating in the establishment of policies and procedures within the firm (e.g., the remuneration policy or the product governance policies and procedures). c. In-scope Firms should ensure that the compliance function is (i) involved in all significant modifications of the organisation of the firm in its regulated activity. This includes the decision-making process when new business lines or new financial products are being approved as well as the definition of staff remuneration policies; and (ii) the development of the relevant policies and procedures within the firm in the area of investment services, activities and ancillary services (for example the firm's remuneration policy or the firm's product governance policies and procedures). In this context, the compliance function should be enabled, for example, to provide compliance expertise and advice to business units about all strategic decisions or new business models, or about the launch of a new advertising strategy in the area of investment services and activities including in the product approval process. If the compliance function's advice is not followed, the compliance function should document this accordingly and present it in its compliance reports (possibly as ad-hoc reports, where necessary).	1. In addition to the comments above, a number of firms have been under the supervisory spotlight for failing to have a sufficiently developed let alone embedded compliance culture both in setting a tone from the top and building out understanding from the bottom up. This also raises questions on the suitability, fit and properness of senior management entrusted (and authorised) to conduct the strategic steering of the firm. 2. Individual focus as well as the use of thematic reviews and common supervisory actions are expected to continue to increase in assessing the adequacy of compliance as well as risk training programmes across In-scope Firms as well as other authorised financial services firms. 3. Particularly in respect of new types of regulated activities as well as specifically in new types of authorised but also established firms moving into such area, the sufficient involvement of the compliance function will remain in the spotlight. This ranges from assessing the role of compliance in new market entry strategies (advertising and client outreach efforts) but also in more strategic questions such as the degree of consultation/challenge from compliance in respect of certain post-Brexit arrangements such as the use of back-branching, reverse solicitation or tied agents, all of which have become subject to a stricter supervisory tone since 2020.
Guideline 5 (organisational requirements of the compliance function)	a. In-scope Firms are required to ensure that appropriate human and other resources (including IT) as well as budget are allocated to the compliance function in a manner that is proportionate to the scale and types of investment services, activities and ancillary services undertaken by the firm. b. In-Scope Firms are required to ensure that compliance staff have access to the relevant information for their tasks at all times, In-scope Firms should provide access to all relevant database and records (such as recordings of telephone conversations and electronic communications). c. In-scope Firms must maintain necessary arrangements to ensure an effective exchange of information between the compliance function and other control functions (for example internal audit and	1. The ESFS at both the EU level and individual NCAs have continued to emphasise a clear supervisory expectation of location of control functions in the EU when supporting EU regulated business. This fits into the wider requirements of firms having to have mind and matter in the EU and not running empty shells. Both established and newly licensed In-scope Firms that are not able to comply and explain how their compliance TOM meets those expectations, how it operates with other control functions etc., will need to take prompt and definitive remedial action.

Guideline	Summary of requirements	Lessons learned since 2020 - Observations from PwC Legal
	risk management) as well as with any internal or external auditors. d. In-scope Firms must ensure that, where relevant, the compliance officer should also be able to attend meetings of senior management or the supervisory function. Where this right is not granted (which should remain exceptional) this should be documented and explained in writing. The compliance officer should have in-depth knowledge of the firm's organisation, corporate culture and decision-making processes in order to be able to identify which meetings are important to attend.	2. Supervisory scrutiny of the degree of constructive challenge of the compliance officer to senior management and other group functions remains an area that the various components of the ESFS will continue to focus on. 3. Recent changes to the EU's fitness & proper standards, as supplemented by various national Member States' own supplemental rulemaking, for key function holders (including control functions), remains an area that may warrant In-scope Firms to conduct their own internal re-assessments of the adequacy of relevant staff ahead of the supervisor doing so.
Guideline 6 (skills, knowledge and expertise)	a. In-scope Firms' compliance staff (not just the compliance officer) must have the necessary skills, knowledge, expertise and authority (including as specifically evidenced in policies) to carry out their duties. b. Compliance staff should be regularly trained in order to maintain their knowledge. The designated compliance officer should possess a higher level of expertise. c. The compliance officer is expressly required to be able to demonstrate a high standard of professional ethics and personal integrity as well as sufficiently broad knowledge and experience and a sufficiently high level of expertise so as to be able to assume responsibility for the compliance function as a whole and ensure that it is effective. d. The Guidelines recognise (and thus permit) national divergences in that some EU Member States require that a nominated compliance officer is licensed or approved by the NCA following an assessment of qualifications (preferred by ESMA) whereas some NCAs in other EU Member States instead impose the responsibility for the assessment of the compliance officer's qualification solely on the senior management of the In-scope Firm.	1. As with comment 3 in Guideline 5 above, supervisors' focus on baseline qualifications and standards will likely continue. So too will a greater scrutiny on the appropriateness of training standards that are in place for staff across the firm as well as for control functions staff specifically. While the supervisors are not scrutinising the content of third-party provided training materials in particular, they are aware of those providers who positively standout amongst their peers. 2. In respect of point d in Guideline 6, while the EU has yet to harmonise the designations of control functions and their approval process, the standards as to assessing and evidencing the fit and proper nature of such persons is well established.
Guideline 7 (on the permanence of the compliance function)	a. In-scope Firms are required to maintain a "compliance policy" or other general policies or internal rules, which are periodically updated, that take account of the scope and nature of the investment services and activities and reflect both the CMP, the risk-based approach to monitoring and the reporting duties of the compliance function. b. In-scope Firms must ensure that the compliance function performs its tasks and responsibilities on a permanent basis. Firms must therefore establish	1. As with the comments above, supervisors continue to test whether the suite of policies and procedures governing the mandate and tasks of the compliance function are updated with a sufficient frequency and reflective of the day to day operations and priorities within the 3LoD model. 2. While the EU has not (yet) followed the footsteps of say the UK's financial

Guideline	Summary of requirements	Lessons learned since 2020 - Observations from PwC Legal
	adequate arrangements, in writing, for ensuring that the responsibilities of the compliance officer are fulfilled when the compliance officer is absent. This may include stand-in arrangements.	supervisory authorities, notably the UK Financial Conduct Authority, in the Senior Managers and Certification Regime, which requires documented handover procedures and materials (SYSC 25.9 FCA Handbook), some UK firms are extending that approach in their post-Brexit operations in the EU. Some lessons from that experience may be available to EU In-scope Firms when documenting handovers or assumptions of responsibilities in the compliance function or indeed for other "key function holders".
Guideline 8 (on the independence of the compliance function)	In-scope Firms must ensure that the compliance function holds a position in their organisational structure so that the compliance officer and staff act independently when performing their tasks, including independently from senior management and other units of the firm.	A number of recent compliance and financial crime failings have highlighted the inadequate authority and independence of the compliance function and In-scope Firms may want to review any assumptions and risks of unconscious bias that may adversely affect the compliance function's role and discharge of its duties.
Guideline 9 (on the proportionality and effectiveness of the compliance function)	In-scope Firms, in assessing whether their compliance function continues to be effective and whether the design of the compliance TOM is proportionate to the risks of the firm must take the following minimum criteria into account: a. the types of investment services, activities and ancillary services and other business activities provided by the firm (including those not related to investment services, activities and ancillary services); b. the interaction between the investment services and activities and ancillary services and other business activities carried out by the firm; c. the scope and volume of the investment services, activities and ancillary services carried out (absolute and relative to other business activities), balance sheet total and income of the firm from commissions and fees and other income in the context of the provision of investment services, activities and ancillary services; d. the types of financial instruments offered to clients; e. the types of clients targeted by the firm (professional, retail, eligible counterparties); f. staff headcount; g. whether the firm is part of a group; h. services provided through a commercial network, such as tied agents, or branches; i. cross-border activities provided by the firm; and j. organisation and sophistication of the IT systems. In-scope Firms are also reminded that while a compliance officer must always be appointed, it may be disproportionate for some firms, depending on the circumstances (for instance, small firms with limited and non-complex activities and/or limited volumes) to appoint a separate compliance officer that does not perform any other function. Where a firm makes use of the exemption (which should be assessed and justified on a case-by-case basis), conflicts of interest	Supervisors have repeatedly stated that they have identified good and bad types of behaviour that are applied by In-scope Firms (across various business models) in testing whether the compliance TOM is proportionate to the risks of the firm and whether staffing and resources allocated are in fact sufficiently adequate.

Guideline	Summary of requirements	Lessons learned since 2020 - Observations from PwC Legal
	between the tasks performed by the relevant persons should be minimised as much as possible.	
Guideline 10 (on the combination of compliance with other internal control functions)	a. In-scope Firms are required to maintain an overall organisational structure where control functions are properly separated in a 3LoD model. The combination of the compliance function with other control functions (such as, in limited circumstances the risk function) may be acceptable if this does not compromise the effectiveness and independence of the compliance function. Any such combination should be documented, including the reasons for the combination so that NCAs are able to assess whether the combination of functions is appropriate in the circumstances. However, where an internal audit function has been established and is maintained within the In-scope Firm, such function may not be combined with other control functions such as the compliance function. b. Compliance staff should generally not be involved in the activities they monitor. However, a combination of the compliance function with other control units at the same level (such as money laundering prevention but note in certain jurisdictions combination of compliance officer with risk officer may not meet the NCA's expectations) may be acceptable if this does not generate conflicts of interests or compromise the effectiveness of the compliance function. Whether or not the compliance function is combined with other control functions, the compliance function should coordinate its activities with the second-level control activities performed by other units in charge of other control functions.	Supervisors continue to publish findings that double hatting of roles and muddling of allocation of responsibilities continues to provide a number of risks for In-scope Firms both large and small regardless of their complexity.
Guideline 11 (outsourcing of the compliance function)	a. In-scope Firms must ensure that all requirements applicable to the compliance function continue to be fulfilled where all or part of the compliance function is outsourced including within a group. Such outsourcing will be material and the rules for the outsourcing for critical or important functions apply to the firm as well as the agreements with the outsourcing services provider. Accordingly, a due diligence assessment must be conducted before choosing a service provider and such assessment must be proportionate in the comprehensiveness of the nature, scale, complexity and risk of the compliance tasks and processes that are outsourced. In all circumstances In-scope firms can only outsource tasks but not responsibilities, which remain with the In-scope Firm. b. In-scope Firms (and senior management) must, on an ongoing basis, monitor whether the outsourcing service provider performs its duties adequately, including monitoring the quality and quantity of the services provided. c. Outsourcing of all or part of the tasks of the compliance function to non-EU entities is viewed as	1. Supervisors have continued to step up their scrutiny of regulated outsourcing of compliance functions and the direction of travel along this path is expected to continue as new requirements applicable to third-party risk management and (digital) operational resilience are rolled out during the 2024 supervisory cycle and beyond. 2. Further criticism is directed by supervisors to the compliance outsourcing providers themselves, in particular third-party boutique firms, given that a number of such providers may lack the sufficient staff and time commitment to allocate to the regulated financial services provider across the breadth of themes and jurisdictions that they are being tasked to assist the regulated firm's compliance function with. This runs the risk of the compliance function of the regulated

Guideline	Summary of requirements	Lessons learned since 2020 - Observations from PwC Legal
	potentially making oversight and supervision of the compliance function more difficult and should be subject to closer monitoring. d. In case the outsourcing arrangement related to the compliance function is terminated, firms should ensure the continuity of the compliance function either by transferring it back to the firm or outsourcing it to another provider.	firm being seen as an "on-paper compliance function" rather than an efficient function. This concern goes hand-in-hand with the continued supervisory focus on preventing empty shells and lack of mind and matter being based in the EU.
Guideline 12 (standards on the review of the compliance function by competent authorities)	a. NCAs should review how firms plan to meet, implement and maintain the applicable compliance function requirements. This should apply in the context of the authorisation process, as well as, following a risk-based approach, in the course of ongoing supervision. b. NCAs should assess whether a firm's compliance function is adequately resourced and organised and whether adequate reporting lines have been established. It should require, as a condition for authorisation, that any necessary amendments to the compliance function are made as a condition for authorisation. c. As part of the ongoing supervisory process, a NCA should – following a risk-based approach – assess whether the measures implemented by the firm for the compliance function are adequate, and whether the compliance function fulfils its responsibilities appropriately. d. In-scope Firms are responsible for determining whether amendments to the resources and organisation of the compliance function are required due to changes in the business model of the firm. e. NCAs should also, as part of their ongoing supervision and following a risk-based approach, assess and monitor - where and if appropriate - whether such amendments are necessary and have been implemented. The NCA should provide a reasonable timeframe for the firm to make amendments. However, firms' amendments are not necessarily subject to approval by the NCA. f. Some Member States require the compliance officer to fulfil an annual questionnaire in order to gather information on compliance of the firm. The questionnaire is an evaluation grid on how the firm's business is intended to be conducted and monitored by the firm. This evaluation grid includes questions related to all investment services the firm is authorised to perform. Some questions also relate to the monitoring and control of the activity to be performed by the firm. (e.g. how the control functions are organised, who they report to, whether some functions are outsourced, etc., as well as a number of open fields asking the firm to describe any relevant changes and developments compared to the previous years). The answers could be validated by the firm's senior	Since the 2020 publication of the standards in Guideline 12, the respective NCAs and other authorities forming the ESFS have taken steps to harmonise their "gatekeeper role" on approval of the adequacy of design and fitness of the compliance function and the TOM as well as conducting intensified post-authorisation checks for those In-scope Firms that evidence high(er) risk before handing these firms over to on-going supervision. It should be noted that the 2020 Guidelines do not mention the interaction between the compliance TOM and how that interoperates with the relevant firm's risk appetite framework and risk tolerance levels. Supervisors are however increasingly focusing their attention to ensure In-scope Firms are applying a holistic enterprise wide approach to compliance and risk management and that senior management in discharge of their "strategic duties" obligations are acutely aware of how these areas interrelate an affect the viability and performance of the relevant firm's and/or group's business.

Guideline	Summary of requirements	Lessons learned since 2020 - Observations from PwC Legal
	management and then sent to the NCA. This questionnaire could be a standardised, machine-readable report to enable data extraction, incorporate qualitative indicators and flags anomalies in a resource-efficient manner. The questionnaire could be used by competent authorities to monitor the firm and to require the firm to adopt an action plan to remediate to the issues as well as to determine the priorities of the supervision of the competent authority and to calibrate its risk-based approach.	

While the Guidelines principles and lessons learned since 2020 show that there are still areas for improvement in light of increased supervisory scrutiny, perhaps some of the most difficult problems that all financial services firms face is the fight for talent. In 2023 there remains an international shortage of high-quality professionals – especially those that combine compliance with rare technical skills. Such specialised professionals are in growing demand as the compliance function's involvement in areas such as (digital) operational resilience, crypto-assets and ESG increases. The fight for talent extends across the entire ecosystem so that traditional financial institutions, FinTechs, technology vendors and consulting as well as law firms are all competing heavily for suitably skilled staff.

Equally, financial services firms should also not expect RegTech and artificial intelligence in themselves to be an instant solution that slashes the need for expensive compliance headcount (whether internal or third-party sourced). Many technology packages have been available for years and most provide a "digital compliance framework" comprised by a range of tools, the majority of which require human input. Making compliance easier and more effective, achieving good client outcomes as well as reducing breaches, risks and more broadly financial crime at scale requires data and tools to analyse the business — and the interaction of people with the existing technology tools in the digital compliance framework is key.

Outlook

As the financial services legislative and regulatory framework in the EU as well as global risks have evolved since the publication of the Guidelines in 2020, some may require firms to reassess in their annual reviews whether existing policies, procedures and processes as well as their compliance systems, controls and monitoring framework as well as governance arrangements may need amending. Furthermore, reviewing fitness of design and purpose of CRAs, CMPs and wider-reaching compliance and other 3LoD relevant control functions may benefit from a comprehensive "health check". This may also require some financial services firms (and not just In-scope Firms) to look at the level of training standards they maintain in respect of compliance and other control functions but also to staff and notably senior management on compliance, risk and governance topics.

In summary, some financial services firms' compliance functions are being (ever more) increasingly being asked to do more with less and the fight for talent means that they risk losing long-standing expertise to higher-paying competitors. Consequently, some financial services firms are beginning to take a more strategic view and work with their third-party professional and legal advisors to secure professional-led, technology-powered "compliance as a service" support on a regulated outsourcing basis or more targeted technical support and advice to allow financial services firms, their business as well as control functions to track, triage and tackle legislative and regulatory developments so as to navigate challenges and seize opportunities.

About us

PwC Legal is assisting a number of financial services firms and market participants in forward planning for changes stemming from relevant related developments. We have assembled a multi-disciplinary and multijurisdictional team of sector experts to support clients navigate challenges and seize opportunities as well as to proactively engage with their market stakeholders and regulators.

PwC Legal and wider PwC teams are currently providing “Compliance as a Managed Solution”, where financial services firms may outsource the compliance function to PwC. This allows the companies to have full focus on strategic questions and the core business, while also securing the sufficient competences and in-depth specialists. PwC Legal and PwC conduct all relevant activities that relate to the compliance function, by performing an annual compliance risk assessment and setting annual (or multi-year) compliance plans. These may include controls, training, support and advise activities, etc. By combining different types of areas of expertise and people with different skills, financial firms can get an extended arm of different synergies in one and the same service. This enables the compliance function to have in-depth competencies within all relevant areas, which may be challenging for an internal compliance function with limited resources. PwC's broad range of services within, among other things, tax, valuation and accounting, sustainability and cyber security enables a comprehensive monitoring of industry practices as well as challenges and opportunities, which also opens up the possibility of adding extra value through advice from a strategic perspective. This is not only a service strictly linked to regulatory compliance, but also an opportunity for advice based on industry practice and wider market monitoring.

Moreover, we have developed a number of RegTech and SupTech tools for supervised firms, including PwC Legal’s Rule Scanner tool, backed by a trusted set of managed solutions from PwC Legal Business Solutions, allowing for horizon scanning and risk mapping of all legislative and regulatory developments as well as sanctions and fines from more than 750 legislative and regulatory policymakers and other industry voices in over 170 jurisdictions impacting financial services firms and their business.

Moreover, in leveraging our Rule Scanner technology, we offer a further solution for clients to digitise financial services firms’ relevant internal policies and procedures, create a comprehensive documentation inventory with an established documentation hierarchy and embedded glossary that has version control over a defined backward plus forward looking timeline to be able to ensure changes in one policy are carried through over other policy and procedure documents, map critical path dependencies and flag where legislative and regulatory developments may require actions to be taken in such policies and procedures.

If you would like to discuss any of the developments mentioned above, or how they may affect your business more generally, please contact any of our key contacts or PwC Legal’s RegCORE Team via de_regcore@pwc.com or our website.

Dr. Michael Huertas
Tel.: +49 160 973 757-60
michael.huertas@pwc.com