EU RegCore Client Alert

ECB-SSM revises its supervisory expectations on governance and risk culture

October 2024

Financial Services

ECB-SSM revises its supervisory expectations on governance and risk culture

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

Contact RegCORE Team
de_regcore@pwc.com

QuickTake

The European Central Bank (**ECB**), acting in its role at the head of the Banking Union's Single Supervisory Mechanism (**SSM**), has had a sustained focus in setting expectations on good governance and a robust risk culture amongst Banking Union supervised institutions (**BUSIs**). On 24 July 2024 as most of Europe was heading off for the summer holiday season the ECB-SSM published a consultation on its draft guide on governance and risk culture (the **Draft Guide**).[1] The consultation remains open until 16 October 2024. Following evaluation of feedback received during the consultation process, the finalised Guide (as will be covered in a separate Client Alert) will supersede and thus replace the 2016 SSM Supervisory Statement on Governance and Risk Appetite (the **2016 Statement**).[2]

This Client Alert assesses the key requirements in the current Draft Guide (including as supplemented by indications signalled in various statements from policymakers) and how this compares to the 2016 Statement as well as what this means for BUSIs in meeting their legislative and regulatory compliance obligations. This Client Alert should be read in conjunction with further analysis, including from our EU RegCORE, on the ECB-SSM's approach to national options and discretions, operations of Joint Supervisory Teams (**JST**s) and on-site inspections and thematic reviews (collectively **OSI**s) as well as rules on fit and proper requirements and internal governance guidelines as published by ECB-SSM but also the European Supervisory Authorities (**ESA**s), in particular those of the European Banking Authority (**EBA**) and the European Securities and Markets Authority (**ESMA**).

Given that the legislative and regulatory requirements as well as their interpretation by supervisory authorities have evolved considerably in the past eight years, many BUSIs and firms may want to take note,

[1] Available here.

[2] Available here. Importantly it should be noted that the ECB's Supervisory Board approved the launch of an extensive thematic review on risk governance and appetite at the SSM level as part of its 2015 supervisory priorities. That thematic review identified that the level of independence on the board could be further strengthened in several institutions, with a focus on the audit and risk committees.

review their current compliance with such expectations and possibly take pre-emptive as well as remedial action.

Key requirements of the Draft Guide

The Draft Guide, like the 2016 Statement, while stating it is "not being legally binding" does set out the ECB-SSM's supervisory expectations based on its interpretation of the current (updated) legislative and regulatory framework applicable to BUSIs. Those expectations flow into the supervisory engagement of JSTs and the BUSIs they supervise and thus like other ECB-SSM supervisory guidance publications, the contents of this Guide should be read like and complied with like rules.

The Draft Guide is addressed to (i) those BUSIs that are categorised as significant institutions (**SI**s) and thus subject to direct ECB-SSM supervision and (ii) those that are categorised as less significant institutions (**LSI**s) and thus directly supervised by national competent authorities (**NCAs**) and indirectly supervised by the ECB-SSM. The ECB-SSM therefore recommends that all JSTs and NCAs align themselves with the expectations and good practices identified by the Guide when assessing the governance SIs as well as for LSIs.

The ECB-SSM uses the Draft Guide to reiterate and expand on the following core expectations:

- **Governance and risk culture**: Governance, including internal governance, according to the ECB-SSM means the way in which a BUSI is organised and its management body conducts decision-making and risk management. The ECB-SSM notes that (our clarifications added in square brackets) "in one-tier governance structures, the management body performs both the management and supervisory functions, while in two-tier governance structures, these are two separate bodies: the management body in its management function [**MBMF**] and the management body in its supervisory function [**MBSF**]." The ECB-SSM goes on to further clarify that governance also includes the allocation of the roles and responsibilities of the relevant people, functions, bodies and committees within a BUSI and how they interact. A strong governance framework is grounded on the suitability of management body members and key function holders to carry out their roles and it should also provide management body members with access to quality data in a timely manner in order to ensure that appropriate decisions are taken in normal times and in crisis situations.

- **Functioning and effectiveness of the management body**: The management body of a BUSI has ultimate and overall responsibility for the institution and defines, oversees and is accountable for the implementation of the governance arrangements within the institution that ensure effective and prudent management of the institution. The ECB-SSM expects that the management body in its supervisory function demonstrates a capacity for constructive challenge and strong oversight of the management function and internal control functions. Institutions must clearly define roles and responsibilities within the organisation. In particular, it is expected that the management body structures itself in terms of leadership and the use of committees to effectively carry out its oversight role and other responsibilities. The structure and mandates of committees are expected to be clearly defined. The ECB-SSM therefore expects that the size of the management body is appropriate to allow it to effectively carry out its oversight role and other responsibilities. The ECB-SSM also states that the chair and the supervising committee should be structured in a way that facilitates their oversight functions.

- **Internal control functions**: To ensure the adequacy of the internal control mechanisms, the ECB expects they are based on the 'three lines of defence' (**3LoD**) model:

  - ***First line of defence***: Business lines take risks and are directly responsible for their operational management on a permanent basis. In the ECB's view, the first line of defence can comprise both "front office" and "back office" activities. In addition, other functions or units, e.g. HR, Legal or IT, may also form part of the first line of defence and are responsible for managing their risks and having appropriate controls in place. The business lines ensure prudent risk-taking, risk management and compliance in order to ensure a sound risk culture across the BUSI.

  - ***Second line of defence***: The risk management function is responsible for further identifying, measuring, monitoring and reporting risks to which a BUSI is or might be exposed, including on a group-wide basis, independently of the first line of defence. The compliance function is in charge of ensuring compliance with applicable laws, rules, standards and advising the management body on measures to be taken in the case of non-compliance.

- *Third line of defence*: The internal audit function independently reviews the first and second lines of defence, assesses the efficiency and effectiveness of the BUSI's risk management, governance and internal control processes and informs the management body about deficiencies.

- **Risk appetite framework (RAF)**: the RAF should allow the management body to obtain a holistic view of the BUSI's risks, hence the management body should play a key role in setting it up and approving it. The scope of the risks included in the RAF is comprehensive, including both financial and non-financial risks and corresponding metrics. Risk appetite limits should be set at an appropriate level to effectively manage risk-taking and should cover the level and types of risks the BUSI can assume, with a clearly defined escalation process in the event of a limit breach.

While the above should (hopefully) seem familiar to most BUSIs, the ECB-SSM's tone and emphasis in the Draft Guide as well as indications of supervisory scrutiny of BUSIs, including beyond the SSM-run supervisory review and evaluation procedure (**SREP**), may warrant some to reassess how to meet compliance with such new standards. As the ECB-SSM notes in the Draft Guide, in its view, despite increased supervisory attention and improvements made by some BUSIs in respect of compliance with the 2016 Statement, the ECB-SSM has:

> "…concluded that the progress made to date has not generally been sufficient. Therefore, banks need to continue enhancing their implementation of governance standards, while the ECB will continue to intensify its scrutiny in order to take timely action to bring about concrete improvements in this area and to escalate non-remediated supervisory findings whenever relevant."

With that in mind, it is unsurprising that the Draft Guide has gone into much further detail in communicating the ECB-SSM's expectations and approach to the legislative and regulatory framework within its supervisory mandate.

Key differences between 2016 Statement and the Draft Guide

The Draft Guide is, when compared to the 2016 Statement, significantly more comprehensive (66 v 22 pages). It also covers a broader range of topics in greater detail. It includes specific sections on the functioning and effectiveness of management bodies, internal control functions, RAF and supervisory approach. It also provides examples of good practices observed during supervisory activities.

One commonality shared by the 2016 and 2024 publications is that both acknowledge the principle of proportionality, meaning that governance arrangements should be commensurate with the size, complexity and risk profile of institutions. Smaller BUSIs (regardless of whether they are LSI or SI) will need to demonstrate that their governance practices are appropriate for their scale of operations. That being said, the Draft Guide, like the 2015 Statement and the bulk of ESA's supervisory expectations are clear that governance arrangements must ensure the segregation of duties in the organisation, precluding "dual-hatting" of roles across different lines of defence with the Draft Guide including specific examples.

Some of the wider reaching differences is the Draft Guide's emphasis on "risk culture" meaning that firms must pay closer attention to cultural drivers within their organisations. This includes fostering a culture of effective communication, challenge, accountability and appropriate incentives. In contrast, the 2016 Statement concentrated on the composition and effectiveness of boards and the design and implementation of the RAF. It provides a summary of findings from a thematic review but lacks the extensive detail found in the Draft Guide. Breaking this down further some of these changes can be summarised as follows:

- ***Governance components:***

  - **Draft Guide**: Provides an in-depth overview of governance components, including the role of management bodies, internal control functions and the importance of risk culture. It outlines specific expectations for the structure, composition and functioning of management bodies. The Draft Guide has a much clearer distinction between expectations of executive management and non-executive supervisory functions. Some important changes include:

    - Adding the RAF to the following statement: The board should include a risk perspective on strategic discussions and demonstrate effective oversight of risk and control functions, with a particular focus on the validation process and monitoring of the RAF;

    - Changing the expectation on the board composition in the 2016 Statement by revising it to: The size and structure of the board should not adversely affect its functioning. Institutions with large boards should assess how the size influences performance and identify measures to improve it;

- Expanding the need for independent[3] members by stating: the board should have a sufficient number of independent directors to enhance its capacity to challenge senior management. The need for formally independent members should apply to committees, especially the audit and risk committees;

- Refining the statement on the chair of the board being an independent **or** non-executive member so as to promote checks and balances to: The chair of the board should be a non-executive member and the ECB recommends that the chair is also an independent member;

- Changes were also made in the expectations on the nomination committee by taking a more proactive role. Specifically, this means the nomination committee should support the board in preparing decisions on the appointment of members, defining profiles for candidates and implementing the suitability and diversity policies. A more specific emphasis is applied to ensuring individual and then collective suitability of respective nominated persons, in particular the management body and encourages the use of self-assessments (as a pre-requisite to formal NCA (and/or ECB-SSM) fit and proper assessments i.e., approval. The Guide also expects the use of self-assessments, which should be regularly reviewed and use of the suitability matrix template provided by the EBA, or the institution's own appropriate methodology and consideration of the needs of the management body according to the succession plan and role definitions;

- Similarly, changes were made to the remuneration committee expectations as follows: The remuneration committee should support the board in preparing remuneration-related decisions, ensuring that remuneration is gender-neutral and balanced by incentives to manage risk.

- Finally, minor changes were made by adding reporting lines and lines of responsibility to the following principle: The board should have a clear allocation of responsibilities, with individual statements setting out the roles and duties of each member, including reporting lines and lines of responsibility.

  - **2016 Statement**: Focused on board composition, including size, structure, independence, collective knowledge, diversity and succession planning. It emphasised the need for effective oversight and independent challenge by boards. It specifically stated that: The size and structure of the board can impact the quality of debate and its effectiveness. Large boards can hamper interactive discussions, while small boards may face issues of diversity in their committees.

- ***Risk culture:***

  - **Draft Guide**: Defines risk culture comprehensively linking it to governance and behavioural patterns. It discusses cultural drivers such as group dynamics and collective mindsets and provides a detailed map of risk culture components. Firms must develop a robust risk culture that is integrated into governance structures. This includes clear guidelines for internal control functions and aligning remuneration policies with risk management objectives.

[3] The ECB-SSM clarifies that: "From a conceptual point of view, a distinction needs to be made between "formal independence" (a factual status) and "independence of mind" (as reflected in a pattern of behaviour/skills). Having formally independent members on the management body in its supervisory function is important for various reasons. First, the presence of independent members generally increases the diversity of views and can therefore help provide adequate checks and balances. Moreover, it can also bring new perspectives to the discussions and help decreasing the risk of groupthink. Second, independent members are in a better position to make objective assessments and to oversee, monitor and critically challenge management decision-making. Hence, their presence is expected to contribute to enhancing the capacity of the management body in its supervisory function to independently challenge the management body in its management function. Conversely, insufficient independence of the management body in its supervisory function or in its committees, especially the audit and risk committees, potentially limits its oversight capacity."

- 2016 Statement: Addressed risk culture primarily through the lens of the RAF, emphasising the need for a comprehensive framework that aligns with business strategy and promotes risk awareness.

- ***Internal control functions***
  - **Draft Guide**: Includes a dedicated section on internal control functions, outlining governance expectations for each function (risk management, compliance, internal audit). As set out above, it discusses the three lines of defence model in detail. Specifically, it reiterates that the risk management function should ensure that all risks are identified, assessed, measured, monitored, managed and properly reported by the relevant units in the institution. More importantly the Draft Guide however states that the focus should be on both financial and non-financial risks including consideration that:
    - Internal control functions must have sufficient authority, stature, reporting lines and resources. Heads of internal control functions should be senior managers with clear management support.
    - On the internal audit function the Draft Guide, like the 2016 Statement, expects that it should independently review and provide objective assurance of the compliance of all activities and units of a BUSI with the institution’s policies and procedures and regulatory requirements. The Draft Guide however adds that there should be a clear link between the outcome of risk assessments and the audit plan.
    - The management body should assess the independence of internal control functions annually.
    - Remuneration for senior officers in internal control functions should be predominantly fixed.
  - **2016 Statement**: Did not have a dedicated section on internal control functions. Rather, it mentioned the importance of effective oversight by boards but lacks specific guidance on internal control functions. The expectations on internal control functions were and still are set out in other legislative and supervisory texts. This includes that internal control functions should have sufficient stature and authority, with independence from business activities they monitor. Moreover, the management body should have direct access to heads of internal control functions.

- ***RAF***
  - **Draft Guide**: Provides detailed guidance on designing and implementing a RAF, including setting limits, monitoring adherence and integrating RAF with business strategy. It emphasises the need for a balance between static metrics and forward-looking indicators. Accordingly:
    - The RAF is now explicitly expected to be fully incorporated and documented as part of the BUSI's decision-making process, including strategic decisions related to ILAAP, ICAAP, budget and remuneration;
    - The management body is now expected to be regularly updated about the BUSI's risk profile relative to its risk appetite, with the development of an aggregated and consolidated risk appetite dashboard;
    - The scope of the RAF is now expected to include material non-financial risks (e.g., compliance risk, reputational risk, IT risk, legal risk, conduct risk) and emerging risks (e.g., climate-related and environmental, social and governance (ESG) risks, geopolitical risks as well as digitalisation – including but not limited to crypto-assets and artificial intelligence). The calibration and monitoring of risk limits are now expected to include early warning thresholds and a clearly defined escalation process for limit breaches;
    - The RAF is now expected to remain stable over time and be used as a driver of the BUSI's strategy, with flexibility to respond to emerging risks and crises;

- The RAF is now expected to be supported by a strong governance framework, with clear roles for all stakeholders, including the management body, senior management, internal control functions and business lines; and

- The RAF is now expected to be deployed within the BUSI, with risk appetite statements established for business lines and entities and risk appetite dashboards developed for material business lines and entities.

- **2016 Statement**: Discussed the RAF in terms of policies, design, governance and deployment within entities and business lines. It highlighted the need for alignment with business strategy but does not provide as much detail as the Draft Guide.

The above differences are important as they will likely warrant some BUSIs to revisit their current arrangements and take proactive steps to evidence increased compliance with the ECB-SSM's supervisory expectations.

Key takeaways for BUSIs

While most BUSIs will (hopefully) be quite familiar with what is set out in the Draft Guide, they will, in particular in light of the revisions (and those that will be made in the final version) and certainly in light of the more prescriptive requirements (which are easier for the SSM to police) want take note of the considerations in the paragraphs below. This is particularly the case given that since the ECB-SSM published the Guide a number of senior policymakers have published statements to the market and equally a number of BUSIs may have received supervisory communications addressed to them directly in light of perceived shortcomings.

The ECB-SSM's press release accompanying the Draft Guide signals patience is wearing thin on poor compliance performance:

> "Both the global financial crisis and idiosyncratic bank failures have shown that deficiencies in internal governance and risk culture can lead to difficulties for banks. Poor decision-making processes can result in imbalances between risk-taking and risk control, which can ultimately pose risks to capital and undermine banks' operational resilience.
>
> Despite the progress already made, banks need to continue to work on implementing governance standards, while the ECB will continue to intensify its scrutiny of banks and take timely action to ensure that they implement concrete improvements. Where relevant, the ECB will use all available supervisory tools to address supervisory findings that have not yet been remediated."

Accordingly, it is very likely that the ECB-SSM will focus on how BUSIs comply with the Guide with a stricter level of scrutiny than supervision of compliance with the 2016 Statement. Accordingly, BUSIs may want to consider the following steps:

1. **Reviewing and enhancing governance frameworks to meet the ECB-SSM's expectations.** This includes:

   a. Conducting a thorough review of existing governance arrangements to ensure they align with the ECB-SSM's expectations;

   b. Clearly defining roles and responsibilities within management bodies, ensuring a distinction between executive and non-executive functions;

   c. Establishing or enhancing management body committees (risk, audit, nomination, remuneration) with clear mandates and appropriate compositions.

2. **Strengthening internal control functions.** This includes:

   a. Ensuring that internal control functions (risk management, compliance, internal audit) have sufficient authority, independence, resources and staffing;

   b. Implement robust processes for regular reporting to the management body and its committees;

c. Periodically reviewing the effectiveness of internal control functions and address any identified deficiencies.

3. **Developing a comprehensive RAF.** This includes:

   a. Designing a RAF that includes both financial and non-financial risks, with appropriate metrics and limits;

   b. Ensuring that the RAF is integrated into strategic decision-making processes and regularly reviewed by the management body;

   c. Establish clear escalation processes for limit breaches and ensure timely corrective actions.

4. **Promoting a strong risk culture.** This includes:

   a. Fostering a culture of effective communication, challenge, accountability and appropriate incentives throughout the organisation;

   b. Implementing training programs to enhance risk awareness among staff at all levels;

   c. Regularly assessing and addressing behavioural and cultural patterns that may impact risk culture.

5. **Engaging in ongoing supervision and compliance.** The detailed supervisory approach outlined in the Draft Guide indicates that banks will face increased scrutiny from supervisors. Firms must be prepared for more frequent assessments, both off-site and on-site, fit and proper assessments and thematic reviews as well as specific supervisory tools such as peer perspectives, benchmarking and escalation processes for non-compliance. In contrast the 2016 Statement addressed internal governance and risk management primarily as part of the SREP without detailed descriptions of supervisory tools and with reference to CRD IV, EBA guidelines and other ECB-SSM publications from 2014 and 2016. For BUSIs this means:

   a. Embracing the Guide's emphasis on ongoing dialogue between supervisors and banks suggests that firms should be proactive in engaging with their supervisors to address any governance or risk culture issues promptly;

   b. Preparing for regular interactions on the Guide with JSTs, including providing access to governance documentation and participating in interviews and meetings;

   c. Staying informed about thematic reviews and targeted analyses conducted by the ECB-SSM;

   d. Ensuring timely remediation of any supervisory findings to avoid escalation measures.

The Draft Guide sets out also a number of good and bad practices (i.e. red flags) identified. These include but are not limited to:

Thematic area	**Bad practices**	**Good practices**
Tone from the Top and Leadership	• Deficiencies in the whistleblowing process. • Lack of challenge and debate within the management body (discussion dominated by a few members). • Lack of diversity (skills, gender, background) or inclusion, possibly contributing to "groupthink". • Lack of meetings and training to raise awareness and promote proper risk culture and conduct. • Insufficient independence of	• Management body members promote risk-conscious behaviours through various communication channels. • Regular communication between all staff involved in delivering the bank's strategy. • Dedicated training on risk culture-related topics, such as psychological safety and the firm's speak-up policy. • To harness the benefits of diversity and create an inclusive environment, a firm's diversity policy covers the entire organisation and is not limited to the management body.

	internal control functions from the management body in its management function. • Insufficient oversight of internal control functions by the management body. • Low number of formally independent members among staff. • Inadequate escalation and consequence management framework for risk, ethical, or compliance issues.	
Incentives	• Documentation underpinning the variable remuneration framework either missing or ambiguously worded. • Lack of interplay between strategy and risk appetite in the remuneration framework. • Imbalanced deployment of financial performance criteria versus non-financial criteria.	• Financial incentives, including bonuses and promotions, reward appropriate risk-taking behaviour. • Key Performance Indicators (KPIs) for management body members include risk and control-related objectives. • Strong link between the RAF and the remuneration framework.
Accountability	• Low stature and understaffing of internal control functions. • Weak information technology (IT) and data aggregation framework. • Lack of a comprehensive "lessons learned" process to identify and address similar risks.	• Implementation of a risk culture dashboard embedded in the governance framework. • Proactive self-assessments on risk culture and a risk culture plan tracked semi-annually. • Clear definition of roles and responsibilities for specific positions, including the chair, CEO, CRO and heads of internal control functions. • When using the EBA suitability matrix, the questionnaires are not filled in by the individual management body members themselves, but instead contain an objective assessment performed by the nomination committee. • Management bodies or shareholders, supported by the nomination committee, as ultimately responsible decision-makers for nomination processes, are provided with full documentation, including all relevant materials and the documented outcome of the assessments performed by decision-preparers. • Banks provide clear guidance on suitability criteria, e.g. soft skills or expected time commitment, taking into account industry standards and available benchmarks. • The management body appoints members with specific expertise or a specific background on the basis of the institution's risk profile or future business development.
Management Body Functioning	• Insufficient time dedicated to debate within the management body. • Agendas not covering a comprehensive range of topics reflecting the size, complexity, business model and risks of the institution. • Lack of open and critical debate within the management body.	• Assigning specific subjects to individual non-executive members ahead of meetings. • Gathering insights from different business areas to increase capacity to challenge. • Continuous training sessions for management body members.

Interaction Between Management Body and Committees	• Systematic presence of management function during entire committee meetings might hamper discussions among non-executive members. • Inadequate reporting lines between committees and the full management body.	• One-to-one meetings between committee chairpersons and heads of internal control functions. • Clear internal rules for the participation of management body members in committee meetings. • Differentiation between 'open' and 'closed' committee sessions.
Internal Control Functions	• Combining internal control functions without ensuring independence and avoiding conflicts of interest. • Insufficient resources and staffing for internal control functions. • Lack of clear allocation of roles and responsibilities across the three lines of defence.	• Regular reporting by the CRO to the risk committee and management body. • Use of a risk management toolkit adaptable to new risk developments. • Comprehensive and harmonised risk assessment implemented across the group.
RAF	• Risk appetite limits set too high or adjusted too often to avoid breaches. • RAF not used as a driver of the firm's strategy but rather dictated by it. • Lack of clear linkage between remuneration framework and RAF to ensure continuous compliance.	• Engagement of the management body in robust inquiry into material or persistent breaches of risk appetite. • Appropriate number of metrics presented to the management body relative to the complexity of risks. • Defined early warning signals to detect deteriorations in the risk profile before risk limits are breached.

These good and bad practices as set out in the Draft Guide are also supplemented by recent statements in the ECB's Supervisory Blog[4]. That blog article was published around the date of the start of the consultation period on the Draft Guide and the key policy communications can be summarised as follows:

- Different institutions have different root causes of governance weaknesses, including structure and composition of management bodies, as well as their functioning, including behavioural characteristics. Board composition deficit stems from limited diversity in geographical origin, skills, education, experience and gender. For example, 17% of banks lack management members with over five years of Information and Communication Technology (**ICT**) experience. As discussed in a separate Client Alert, the ECB-SSM has communicated its expectations on ICT and digitalisation amongst BUSIs.

- Despite official diversity policies in existence at most BUSIs, gender representation has not improved enough. Unfortunately, banking remains a male-dominated industry, with only 19% of management and 35% of supervisory roles held by women. This is not sufficient, as the EU's Women on Boards Directive requires a minimum of 33% female representation on the corporate board of a publicly listed bank for balance. EU Member States must implement this regulation into national legislation by the end of the year and listed banks must comply by June 2026.

- Lack of independent non-executive directors is a contributing factor to ineffective management bodies. In the ECB-SSM's view independent directors can offer a fresh viewpoint from outside the bank, providing constructive challenges to the board. After reviewing management body effectiveness in 38 banks, the ECB-SSM found that the percentage of independent non-executive directors has only marginally increased from 59% in 2020 to 62% currently. Nearly one-third of supervised banks have less than 50% independent non-executive directors on their boards.

- Executive attendance at control function and committee meetings can hinder debate and challenge, leading to inefficient management bodies. Today, 55% of banks in the ECB's targeted review still

[4] Available here.

practice this harmful behaviour. Some banks distinguish between "open" sessions (open to all members) and "closed" sessions (available solely to non-executive members) as a good practice. This allows non-executive directors to constructively question executives and have an impartial discourse.

- In the view of the ECB-SSM Banks should improve their culture to fit with cautious risk-taking. In certain institutions, the Chief Risk Officer's salary is by the ECB-SSM as too closely tied to commercial goals. To promote responsible risk-taking, several banks offer financial and non-financial incentives and link the risk appetite framework to reward.

Given the above, supervised firms must adapt to these revised expectations by enhancing board independence, integrating comprehensive RAFs into decision-making processes, ensuring robust internal control functions, fostering a strong risk culture, preparing for detailed supervisory assessments and staying updated with regulatory changes.

Outlook

The ECB-SSM's Draft Guide provides comprehensive supervisory expectations aimed at enhancing the governance frameworks and risk cultures of BUSIs, regardless of size and complexity, operating within the Banking Union. The more prescriptive requirements coupled with a stricter supervisory tone point to the ECB-SSM getting serious on remediating shortcomings on governance and risk culture. While aimed at the Banking Union, the ECB-SSM's expectations expressed in its Guide will likely be of relevance to all firms supervised by NCAs in particular those that are subject to the spotlight as part of the oversight and priorities set by the ESAs.

Supervised firms will want to take proactive steps to align their practices with these updated expectations, ensuring they can evidence the robustness of their existing or revised governance arrangements, effective internal control functions, a comprehensive RAF, a strong risk culture and ongoing compliance with supervisory requirements. For some firms this may warrant an inside-out as well as an outside-in 360-degree assessment of their compliance with the respective legislative requirements as well as the supervisory expectations of the ECB-SSM, ESAs and NCAs.

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.

In order to assist firms in staying ahead of their compliance obligations we have developed a number of RegTech and SupTech tools for supervised firms. This includes 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 1,500 legislative and regulatory policymakers and other industry voices in over 170 jurisdictions impacting financial services firms and their business.

Equally, 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 to other policy and procedure documents, critical path dependencies are mapped and legislative and regulatory developments are flagged where these may require actions to be taken in such policies and procedures.

The PwC Legal Team behind Rule Scanner are proud recipients of ALM Law.com's coveted "2024 Disruptive Technology of the Year Award".

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