EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Draft guide on governance and risk culture

July 2024

Contents

1 Introduction

Good governance is key for banks to take the right decisions. It is therefore one of the major pillars that ensures their safety and soundness and the stability of the financial system of the European Union, which are overarching goals of the Single Supervisory Mechanism (SSM), thereby contributing to the trust of the wider public in the banking sector.[1]

Both the global financial crisis and idiosyncratic bank failures have shown that deficiencies in internal governance and risk culture can often be seen as early warning signals or even a root cause of difficulties ahead. These deficiencies may then translate into poor decision-making, often resulting in imbalances between risk-taking and control. If severe, such deficiencies can materialise over time as risks to capital, also undermining banks' operational resilience. Therefore, sound governance and risk culture contribute to promoting a more sustainable business model over the full business cycle. This is especially important in an environment in which banks face economic, financial, competitive, and geopolitical headwinds.

Governance and risk culture are essential features of any well-functioning organisation, having an impact on its structure, culture, and people. Shaping the organisation of a bank and its management body, defining its values, norms, expected behaviours and collective mindset are key to ensuring the soundness of its business operations, strategic planning, and decision-making. Better strategic steering capabilities in particular help to address the challenges stemming from the constantly evolving environment in which banks operate.

Since the global financial crisis, governance and risk culture have risen to the top of the agenda of regulators and supervisors around the world. Standards and supervisory guidance have been provided at international level by the Basel Committee on Banking Supervision (BCBS).[2] At Union level, these standards and guidance are reflected in the Capital Requirements Directive (CRD)[3], which is in turn transposed into the national legislation of individual Member States. The guidelines adopted by the European Banking Authority (EBA) provide guidance concerning the internal governance arrangements, processes, and mechanisms that institutions must have in place under the CRD.[4] In addition to the legal framework, important

---

1 See recital 30 and Article 1 of Council Regulation (EU) No 1024/2013 of 15 October 2013 conferring specific tasks on the European Central Bank concerning policies relating to the prudential supervision of credit institutions (OJ L 287, 29.10.2013, p. 63) (SSM Regulation).

2 See the BCBS Guidelines on corporate governance principles for banks and the BCP Core Principles for effective banking supervision.

3 Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC (OJ L 176, 27.6.2013, p. 338).

4 See, in particular, EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04), EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05) and joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU (ESMA35-36-2319, EBA/GL/2021/06).

guidance has been published by the Financial Stability Board (FSB) and the Group of Thirty (G30).[5]

Against this background, a significant amount of work has also been carried out in relation to governance and risk culture since the inception of the SSM.[6] Internal governance and risk management is also one of the pillars of the Supervisory Review and Evaluation Process (SREP) carried out on an annual basis. As part of on-going supervision, bank-specific assessments of targeted governance areas have also been performed by supervisors on the basis of idiosyncratic features of individual banks. In addition, on-site inspections have been conducted to perform deeper assessments related to governance and controls. Furthermore, fit and proper supervision plays a strong role in ensuring that management body members and key function holders are suitable to perform their duties.

Despite this increased supervisory attention and the improvements already made by some institutions, the European Central Bank (ECB) 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.[7]

The main purpose of this ECB Guide on governance and risk culture is to set out key ECB supervisory expectations when assessing the governance and risk culture of supervised entities based on the ECB's interpretation of the current regulatory framework.[8] The Guide does not lay down legally binding requirements and it does not replace the relevant legal requirements in either Union or national law, nor should it be construed as introducing new rules or requirements compared to current Union and national law.

The information in this Guide builds on the SSM supervisory statement on governance and risk appetite of 2016, which it supersedes as of the date of its publication, and makes use of additional evidence collected through the supervisory activities described above. It also provides examples of some observed good practices, thereby connecting the dots between the applicable regulatory framework and the supervisory work done over the years. While not being exhaustive, it aims to

---

5 See in particular the FSB Principles for Sound Compensation Practices, the FSB Guidance on Supervisory Interaction with Financial Institutions on Risk Culture, the FSB toolkit on misconduct, the G30 reports on Banking Conduct and Culture: A Call for Sustained and Comprehensive Reform and Banking Conduct and Culture: A Permanent Mindset Change.

6 This area has regularly been on top of the SSM supervisory priorities, starting in 2015 with the thematic review on governance and risk appetite for all significant institutions, followed by a thematic review on governance for less significant institutions (2021) and a targeted analysis of management body effectiveness and diversity (2022-2024).

7 Article 16(2)(b) of the SSM Regulation provides that for the purposes of Article 9(1) the ECB has the power to require the reinforcement of arrangements, processes, mechanisms and strategies. See also "Supervisory measures" on the ECB's banking supervision website.

8 In this Guide, the term "supervised entity" means supervised entity as defined in Article 2(20) of Regulation (EU) No 468/2014 of the European Central Bank establishing the framework for cooperation within the Single Supervisory Mechanism between the European Central Bank and national competent authorities and with national designated authorities (SSM Framework Regulation) (OJ L 141, 14.05.2014). In the Guide, the terms "supervised entity," "bank" and "institution" are used interchangeably.

guide banks towards a more effective internal governance and risk culture, taking into consideration their governance arrangements, culture and behavioural patterns. The Guide should be read in conjunction with other ECB Banking Supervision publications, such as the Guide to fit and proper assessments, Good practices for climate related and environmental risk management, the Guide on effective risk data aggregation and risk reporting, and the ECB Guide on options and discretions available in Union law.

Good governance and risk culture are equally important for all banks, whatever their size, and the various elements of this Guide are also relevant for smaller institutions. Taking into account the principle of proportionality (in line with Article 74(2) CRD), banks' governance arrangements, processes and mechanisms are to be comprehensive and proportionate to the nature, scale and complexity of the risks inherent in the business model and the institution's activities. It is to be noted that in pursuing its supervisory approach, ECB Banking Supervision acknowledges national specificities as well as the different governance structures existing across the euro area.

Our interactions with the banking industry over the past years have been important to better understand the challenges banks are facing and to explain the ECB's high expectations in this area. This Guide aims to continue this effective and helpful dialogue between supervisors and supervised banks, working towards a common goal of improving internal governance and risk culture.

This Guide is also intended for the internal use of the various supervisory teams, with the aim of ensuring a common and consistent approach. The ECB also recommends that national competent authorities (NCAs) align with the expectations and practices set out in this Guide when assessing the governance of less significant institutions.[9] Finally, this Guide is intended as a practical tool and is not a substitute for the analysis of individual situations and the exercise of supervisory judgement.

ECB Banking Supervision will continue to develop its supervisory approach towards addressing governance and risk culture-related risks over time, taking into account regulatory developments as well as evolving practices in the industry and in the supervisory community. Therefore, the expectations set out in this Guide may be adapted over time. This Guide is applicable as of the date of its publication.

[9] This Guide is without prejudice to national law. However, where possible, the ECB and the NCAs strive to interpret national rules consistently with the expectations and practices set out in this Guide.

2 Governance and risk culture: importance for banks

ECB Banking Supervision assesses governance and risk culture in line with relevant Union law, as transposed into national law, guidelines issued by EU agencies and international standards.[10] At the level of Union law, the CRD requires banks to have robust governance arrangements in place, including in relation to the risks inherent in the institution's business model and activities.[11] Meanwhile, according to the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), EU banks and supervisors should ensure that institutions have a strong management body in its supervisory function which challenges decision-making and that a sound risk strategy. Also, risk appetite and risk management frameworks should be in place, as well as governance arrangements that effectively foster a sound risk culture at all levels of an institution. International standards provide further guidance on assessing governance and risk culture.[12]

The following section conveys ECB Banking Supervision's understanding of the components of governance and risk culture that are subject to its supervisory assessment based on the above-mentioned laws and guidelines, its approach to assessing different governance structures, and the offsite and on-site supervisory tools it uses.[13] In outlining the ECB's approach to assessing governance and risk culture, the Guide also makes use of the recommendations stemming from an external assessment of the SREP by a group of experts.[14]

To the extent possible, the Guide follows the terminology used in the CRD, the joint European Securities and Markets Authority (ESMA) and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders (EBA/GL/2021/06), and the EBA Guidelines on internal governance (EBA/GL/2021/05). For example, unless otherwise specified, the term "management

---

10 Under Article 4(3) of the SSM Regulation, for the purposes of carrying out the tasks conferred on it by the SSM Regulation, the ECB applies all relevant Union law, and where that Union law is composed of Directives, the national law transposing those directives. References to CRD provisions in this Guide also refer to such provisions as transposed into the relevant national law. In this respect, the Guide does not replace national law, nor is it intended to introduce new binding rules compared to existing national law.

11 See Article 74 of the CRD in conjunction with Article 98(7) of the CRD, which provides that "the review and evaluation conducted by competent authorities shall include governance arrangements of institutions, their corporate culture and values, and the ability of members of the management body to perform their duties".

12 See the BCBS Guidelines on corporate governance principles for banks, the BCP Core Principles for effective banking supervision and the FSB's Guidance on Supervisory Interaction with Financial Institutions on Risk Culture: A Framework for Assessing Risk Culture.

13 ECB Banking supervision does not have competence or powers in the areas of anti-money laundering and countering the financing of terrorism (AML/CFT), consumer protection or criminal matters. However, the ECB integrates AML/CFT-related matters in its prudential assessment of governance and risk culture.

14 Assessment of the European Central Bank's Supervisory Review and Evaluation Process, Report by the Expert Group to the Chair of the Supervisory Board of the ECB.

body" applies to the bodies in all governance structures that perform management and/or supervisory functions.[15]

2.1 Overview of governance and risk culture components

2.1.1 Defining governance

Governance, including internal governance, means the way in which a bank is organised and its management body conducts decision-making and risk management.[16] In line with the EU legal framework, banks are required to have robust governance arrangements, including a clear organisational structure with well-defined, transparent and consistent lines of responsibility, effective risk management processes, control mechanisms and gender-neutral remuneration policies.[17]

In this context, governance includes the allocation of the roles and responsibilities of the relevant people, functions, bodies and committees within a bank and how they interact. A strong "three lines of defence" model is another key component of a bank's internal governance framework.[18] In the view of the ECB, the internal governance framework reflects the functions responsible for taking and managing risks and ensures that issues are properly managed, monitored, mitigated, escalated and reflected in the bank's strategic plans and its risk appetite framework (RAF).

The importance of assessing a bank's governance framework centres around the need to ensure internal checks and balances, prevent weaknesses in governance, such as excessive risk-taking and misconduct, and promote sound and prudent management. 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.[19]

---

15 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 and the management body in its supervisory function.

16 Paragraph 18 of the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05) states: "Internal governance includes all standards and principles concerned with setting an institution's objectives, strategies and risk management framework; how its business is organised; how responsibilities and authority are defined and clearly allocated; how reporting lines are set up and what information they convey; and how the internal control framework is organised and implemented, including accounting procedures and remuneration policies. Internal governance also encompasses sound information technology systems, outsourcing arrangements, and business continuity management".

17 In line with Articles 74 and 88 CRD.

18 See Section 4 of this Guide, on "Supervisory Expectations regarding the internal control functions".

19 On data risk aggregation, see also the ECB Guide on effective risk data aggregation and risk reporting.

2.1.2 Defining risk culture

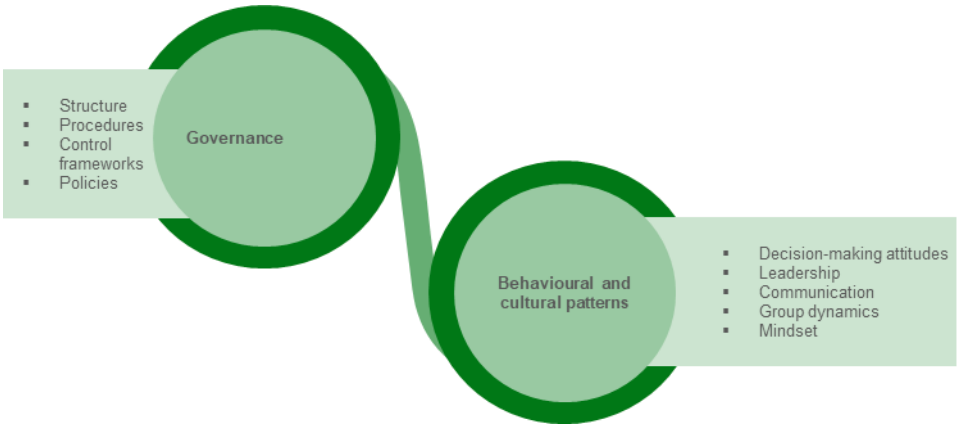
2.1.2.1 Risk culture and the link between governance and behavioural and cultural patterns

Risk culture is intrinsically linked to governance and encompasses the collective mindset and the shared set of norms, attitudes and behaviours related to the awareness, management and control of risks at all levels in a bank. It influences the day-to-day decisions of staff and management and shapes their risk-taking behaviour.[20] Risk culture is a transversal concept and intrinsically relates to other governance topics covered in the succeeding parts of this Guide.

From the perspective of ECB Banking Supervision, risk culture relates to a bank's governance and to behavioural and cultural patterns. Governance concerns the more formal aspects of risk culture, such as a bank's organisational structure and the procedures, control frameworks and policies that are in place (see Section 2.1.1), while behavioural and cultural patterns can be found in decision-making, leadership and communication styles. There are different cultural drivers for these behavioural patterns, such as group dynamics and collective mindsets, identified at all levels of the bank, including management bodies, senior management, middle management and staff.[21] These drivers can also be root causes of a bank's risk culture-related deficiencies.

Figure 1

Link between risk culture components



[20] See the definition of risk culture in paragraph 13 of the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05): "Risk culture means an institution's norms, attitudes and behaviours related to risk awareness, risk-taking and risk management, and the controls that shape decisions on risks. Risk culture influences the decisions of management and employees during the day-to-day activities and has an impact on the risks they assume."

[21] The term "group dynamics" refers to interactions between different positions and patterns within a group or between groups that affect behaviours and overall group effectiveness, e.g. group composition, cohesion and (dealing with) conflict, levels of psychological safety, status and trust. The term "collective mindset" refers to deeply held beliefs, assumptions and values that often guide group dynamics and individual behaviours, concerning, for example, the fundamental nature of risk, how to deal with risks and risk-taking behaviours, and how leaders see their own role.

2.1.2.2 Risk culture dimensions

Broadly speaking, risk culture has four dimensions: tone from the top and leadership; culture of effective communication and challenge and diversity; accountability for risks; and incentives, including remuneration.

- Tone from the top and leadership play a crucial role in creating a culture of prudent risk-taking within an institution.[22] Tone from the top includes the composition and functioning of the management body and senior management, including the management body's responsibility to define the bank's corporate culture and ensure that it is properly adhered to.[23] It also includes the management body in its supervisory function, its committees and internal control functions, as well as its capacity to oversee management decisions. Another key aspect is the consistent communication and actions from the management body on risk and compliance matters, including on ethical behaviour covered in its code of ethics or conduct covering also behaviours related to ML/TF, tax integrity and other financial related misconduct[24]. It encompasses also bank's dialogue from the top with supervisory authorities.

- A culture of effective communication and challenge and diversity should exist at all levels, especially within the management body and its committees, internal control functions and business lines, and with respect to all types of risks. It is essential that the composition of the management body provides it with the diversity of knowledge, skills and experience necessary to ensure its effectiveness, the establishment of a culture of constructive challenge, including a speak-up culture to create a safe environment in which concerns can be raised, and quality of debate, facilitating the decision-making process. At all organisational levels, the decision-making process should benefit from constructive criticism from staff, as well as from the internal control functions.

- Accountability for risks is in place in the form of assigning clear responsibilities for taking, monitoring, managing and mitigating financial and non-financial risks, including emerging risks, as well as a clear definition of the role of control functions.[25] In this context, as part of ensuring sound risk culture, it is crucial that all managers and staff members across the three lines of defence, starting

---

22 The term "culture" is used more generally than "risk culture." Specifically, in this context, "risk culture" refers to components such as culture of challenge and behaviour, while "culture" is broader, referring to the ability of the bank to manage its corporate and risk culture, and includes the bank's values and code of conduct.

23 In line with paragraph 22(k) and Section 10 of the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), the term "corporate culture" covers the corporate values, including the ethical and professional standards, which are developed, adopted and adhered to within an institution (among staff and management). Corporate culture also includes the implementation of a code of conduct or similar instrument.

24 See EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 103.

25 Member States have until 10 January 2026 to transpose CRD VI (Directive (EU) 2024/1619 of the European Parliament and of the Council of 31 May 2024 amending Directive 2013/36/EU as regards supervisory powers, sanctions, third-country branches, and environmental, social and governance risk, OJ L, 2024/1619 of 19.6.2024) by adopting and publishing the laws, regulations and administrative provisions necessary to comply with this Directive. However, the ECB encourages banks to start preparing their governance arrangements in order to be fully compliant when the national transposition measures enter into force. It is noted that CRD VI will introduce amendments regarding the mapping of roles and responsibilities of management body members.

from business lines, are familiar with all relevant aspects necessary to assume their roles and responsibilities, e.g. the ethical values, the strategic objectives, the RAF and the risk limits. Another important feature of the risk culture is the implementation of escalation and alert mechanisms for risk and control issues and findings.

- The proper setting of incentives, with ex ante and ex post risk alignment mechanisms in remuneration schemes, is another key dimension of risk culture.[26] These incentives need to be considered in connection with a bank's strategic objectives and its RAF. In this context, a bank's financial incentives should not be too closely linked to its short-term profitability but should also reflect on risk-related criteria to align risk-taking behaviour with the institution's long-term interests. In addition, it is expected that banks monitor that also other financial and non-financial incentive schemes, beyond remuneration, such as performance and talent management tools (e.g. promotions), are designed and implemented in a way which supports sound and prudent risk management. Moreover, the bank's remuneration framework should address behaviours not aligned with prudent risk-taking. In this context, in terms of bonus setting, banks should also ensure that they properly apply the limit on the ratio between variable and fixed remuneration (the bonus cap).[27] Other requirements, such as the deferral of the variable component and its payment in the form of instruments, ensure the alignment of incentives with the performance, risks and longer-term interests of the institution. In addition, the ECB recommends that institutions apply transparency in the promotion process and alignment with ethical standards. The ECB also expects banks to apply a consequence management framework for misconduct, including a disciplinary process and a sanctions regime.[28]

Banks are responsible for defining their governance arrangements and for setting their own culture. It is expected that banks consider all the risk culture dimensions in order to have a holistic view of potential areas of attention related to their governance. In this context, ECB Banking Supervision has identified a non-exhaustive list of red flags related to the different risk culture dimensions (see Table 1).[29]

---

[26] See EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04).

[27] See Article 94 CRD: variable remuneration is limited to 100% of the fixed component of the total remuneration, or 200% with the approval of shareholders.

[28] The ECB understands "consequence management framework" to mean an internal framework (set of policies and processes) establishing and ensuring the application of consequences in the case of misconduct or failure to adhere to the institution's core values (e.g. its code of conduct), risk appetite, risk culture and general internal policies, procedures, risk limits and desired risk behaviours. The ECB considers that the framework should also cover consequences in the case of non-compliance with applicable law and regulations and the bank's obligations as an authorised credit institution and should define the relevant escalation processes.

[29] Red flags may be leading indicators of underlying governance and risk culture problems.

2.2 Governance assessment of specific structures

Sound governance arrangements are crucial for all banks. Governance arrangements should be commensurate with the bank's size, complexity and risk profile to enable an adequate level of oversight by the management body. In this context, ECB Banking Supervision undertakes a forward-looking, risk- and judgement-based assessment of risks.

1. In its supervisory approach, ECB Banking Supervision acknowledges national specificities and seeks to foster a level playing field based on an interpretation of the legal requirements in line with EBA guidelines and taking into account observed good practices (as also presented in this Guide). A two-part approach is followed when assessing the different components of a bank's governance and risk culture: first, the ECB considers the national law applicable to the bank which transposes and implements the CRD; second, it interprets that law in accordance with the applicable European and international standards and applies it.

2. ECB Banking Supervision also acknowledges that there are different governance structures across the euro area, including unitary (one-tier) and dual (two-tier) management bodies as well as traditional and other models, different business models, and listed and non-listed banks. Strong governance frameworks and risk culture are essential for all banks, irrespective of their governance structure. In addition, all institutions should continue to adapt to evolving risks and challenges that may arise owing to a bank's specific risk profile and business model as well as externalities, including geopolitical developments, legislative changes, digitalisation (including artificial intelligence and crypto-assets), information and communication technology (ICT) and security risks, including cyber, and environmental, social and governance (ESG) risks.[30]

Against this backdrop, this Guide conveys some ECB's observed good practices for banks across the euro area. It sets out supervisory expectations, while acknowledging national specificities and divergences across existing governance structures.

The Guide respects the principle of proportionality, namely that banks' governance arrangements, processes and mechanisms are proportionate to the size, internal organisation and nature, and complexity of a bank's activities.[31]

2.3 The importance of risk culture for banks

Banks are expected to define their culture, including their values and code of conduct, as well as measure adherence and implementation of this culture. In

[30] On climate-related risks, see also the ECB Guide on climate-related and environmental risks.

[31] In line with the CRD and EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05).

addition, the management body is expected to regularly discuss the bank's culture, in order to ensure that it is aligned with prudent risk-taking.

It is expected that banks define their culture and values and draw up a code of conduct. It is also expected that banks are able to monitor and measure adherence to that culture. The ECB recommends that banks regularly discuss the bank's culture at management body level, as well as its implementation across the bank. Effective tools should be in place for banks to mitigate their culture risk, i.e. the risk of a misalignment between the bank's stated values and the actions of member of its management body, and the behaviour of its employees. It is recommended that findings, from the ongoing monitoring of how such culture is implemented, are reported to, and discussed by the management body and its relevant committees.

As mentioned in Section 2.1.2.2, it is also expected that banks reflect on behavioural and cultural aspects that can be drivers ensuring a sound risk culture as well as their respective root causes (e.g. related to group dynamics and collective mindsets) can be transversal across the four risk culture dimensions. It is expected that the management body and senior management define and communicate desired behaviours in line with the values of the bank and act as role models. It is expected that banks identify and act upon root causes of undesired behaviours.[32]

The ECB believes that the way a bank defines its culture plays a key role in ensuring prudent risk-taking and risk management.[33] This implies that the bank's governance arrangements, culture and behaviours should be aligned with prudent risk-taking. It is expected that this is substantiated by concrete actions through, but not limited to, the four risk culture dimensions: tone from the top and leadership; culture of effective communication and challenge and diversity; ensuring accountability (including, the bank's escalation and whistleblowing processes); and setting of incentives.[34]

---

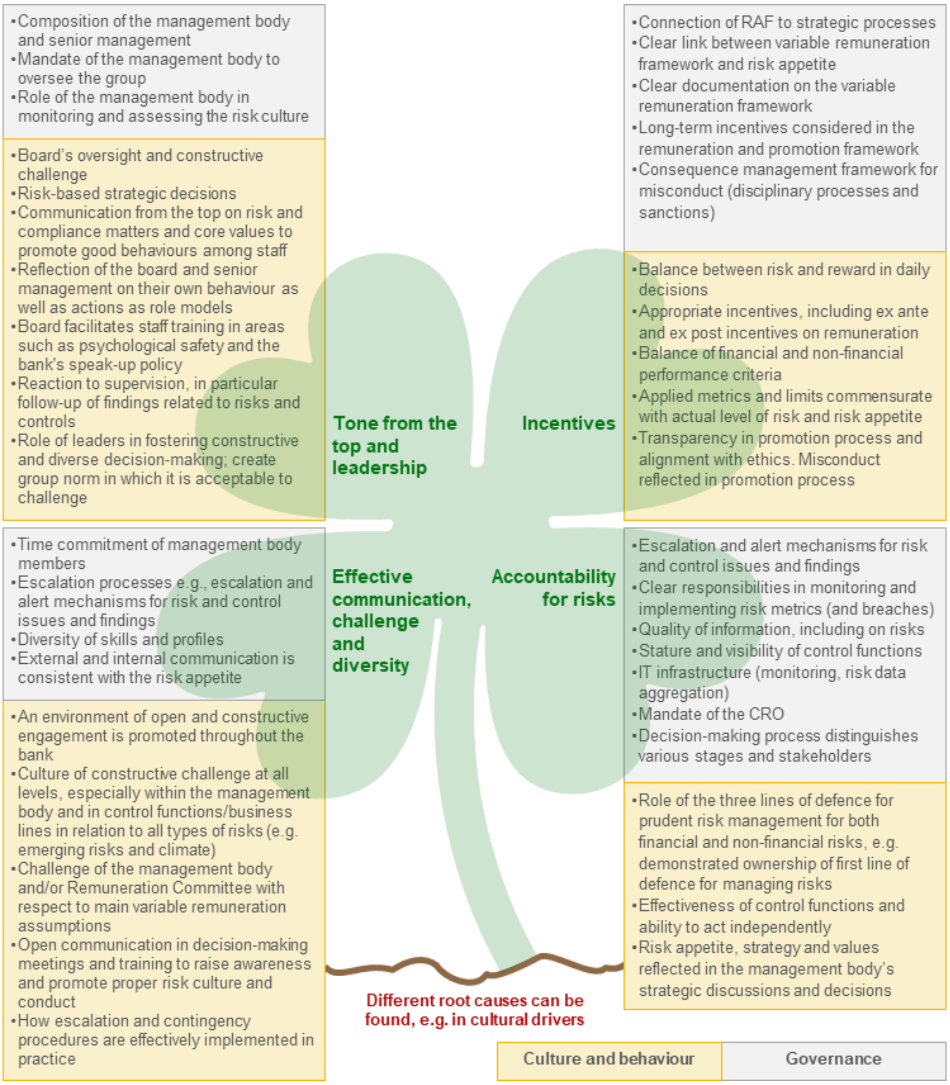
32 See FSB Guidance on Supervisory Interaction with Financial Institutions on Risk Culture, Section 3.

33 See EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 98(c).

34 See also the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), Title IV, and as well as Section Part 2.1.2. of this Guide.

Figure 2

Map of risk culture components, connecting governance, culture and behaviour



As part of the tone from the top and leadership, it is essential that a bank communicates its aspired risk culture to all staff via multiple channels, including, among other things, mission statements, values of the bank and lessons learned. The ECB expects that banks facilitate a culture of effective communication and challenge at all levels, from the management body and senior management to the staff, to strengthen the ability to openly and constructively challenge decisions.[35] It also expects that banks encourage a culture in which all staff are able to speak up and report mistakes and have in place the necessary processes and policies to facilitate this.

Regarding the setting of appropriate incentives, the bank's remuneration framework is key to ensuring the existence of an incentive system that promotes desired

[35] See EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), Ibid, paragraphs 22(k) and paragraph 98.

behaviours aligned with the long-term interests and risk profile of the bank in order to ensure a sound risk culture and discourage excessive risk-taking.[36] There should be a link between a bank's remuneration framework, its strategy and its risk appetite. An appropriate incentives and remuneration framework is also key to ensuring accountability for risks across the bank and via the internal control functions. In order to ensure effective processes, it is expected that banks have in place relevant digital transformation initiatives which are monitored and updated regularly.

In addition, in order to ensure accountability and a transparent decision-making process, banks' internal policies should ensure a clear allocation of tasks and responsibilities across the different functions, at all levels and across the three lines of defence.[37] it is also expected that banks define clear accountability of the management body to the internal control functions for the remediation of audit and supervisory findings. For this purpose, it is expected that banks set strong incentives for the management, including senior managers, and ensure there is a link between such accountability for remediation of audit and supervisory findings and the bank's performance assessment and remuneration framework, e.g. via specific key performance indicators (KPIs).[38]

Observed good practices

Tone from the top:

- Members of a bank's management body promote the adoption of risk-conscious behaviours (e.g. via speeches, blogs), building trust and psychological safety.
- Regular communication between all staff involved in delivering the bank's strategy, including project managers, internal control functions, business analysts, support functions and the business areas concerned, to discuss and obtain feedback on issues important to its successful execution.
- Dedicated training on risk culture-related topics, such as psychological safety and the bank's speak-up policy.

Incentives:

- The bank rewards and encourages appropriate risk-taking behaviour via financial incentives, including bonuses, promotions and non-financial rewards in the form of secondments, accreditations, qualifications and specialised training opportunities.
- KPIs for all management body members and senior management include risk and control-related objectives that are appropriately weighted in the overall assessment of performance.

[36] For further information on the ECB expectations regarding the remuneration framework, see Section 5.2.1 of this Guide.

[37] Articles 74 and 88 of the CRD.

[38] See also Section Part 6 of this Guide, on the Risk Appetite Framework (RAF).

- There is a strong link between the RAF and the remuneration framework, providing incentives for employees to deliver in line with the RAF and risk culture, e.g. if the actions of an employee lead to a breach of risk limits, this will have an impact on their variable remuneration.
- KPIs focus on different stakeholders, including, employees, customers, regulators as well as shareholders.

Accountability:

- The bank has implemented a risk culture dashboard that is embedded in the bank's governance framework, and which facilitates reporting, follow-up actions.
- The bank proactively works on improving risk culture, e.g. by carrying out self-assessments on risk culture and having a risk culture plan which is tracked on a semi-annual basis.
- In order to ensure individual accountability, the bank sets out the requirements for and responsibilities of specific roles, including the chair, the chief executive officer (CEO), the chief risk officer (CRO) and the heads of internal control functions.
- In their annual performance assessment and self-assessment, members of the bank's management body are also assessed on their assumption of responsibilities and accountability.
- Root cause analyses and "lessons learned" exercises are undertaken in cases where things have gone wrong, not with the aim of attributing blame or penalising staff but to identify and fix problems.
- The bank fosters awareness of compliance and non-financial risks through different channels, such as internal communications on compliance rules (e.g. emails, posters in meeting rooms) and training on compliance rules with a test at the end.
- Regular training for staff in the first line of defence on risk strategy updates.
- The responsibilities of the board members are linked to the risk taxonomy, to ensure accountability and responsibility mapping e.g. each team, topic, process is clearly allocated per risk, including where collaboration across teams is needed.

2.3.1 Risk culture red flags

Based on its supervisory experience over previous cycles, the ECB has identified a number of governance and behavioural/cultural red flags. These serve as early warning signals of potential governance and risk culture issues. They need to be assessed in a holistic and case-by-case manner, as any deficiency may not be due to risk culture or to risk culture alone.

Table 1

Risk culture red flags (non-exhaustive list)

Risk culture dimension	Governance red flags	Behavioural and cultural red flags:
Tone from the top and leadership	- Insufficient management body oversight of internal control functions and the management body in its management function - Low number of formally independent members - Insufficient subsidiary oversight - Inadequate escalation and consequence management framework in the case of risk, ethical or compliance issues - Inadequate conflict of interest policy and ethics framework	- Insufficient ownership of and responsibility for conduct risk - Unsatisfactory tone from the top from the management body to promote good behaviours among staff - Dismissive attitude among staff towards compliance, regulation and supervision - Inadequate tone from the top on the balance of risks and rewards - Concentration of power in a few members of the management - Unethical behaviours not sufficiently sanctioned by the bank and insufficient communication on these issues
Culture of effective communication and challenge and diversity	- Deficiencies in the whistleblowing process - Governance arrangements, including, committee structure and escalation process not facilitating debate - Inadequate diversity framework	- Lack of challenge and debate within the management body (discussion dominated by a few management body members) - Insufficient challenge of the management body in its supervisory function and/or its committees (e.g. remuneration committee) with respect to the main variable remuneration assumptions - Insufficient challenge from internal control functions (e.g. lack of a role for the risk management function or its head in challenging decisions) - Insufficient independence of internal control functions from the management body in its management function (e.g. filtering or review of information included in internal control function reports prior to the approval process) - A culture of fear leading to an unwillingness to report mistakes, risk breaches or material concerns - 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
Incentives	- Documentation underpinning the variable remuneration framework (e.g. KPIs) either missing or ambiguously worded - Lack of interplay between strategy and risk appetite - Framework to address behaviours not aligned with prudent risk-taking - Lack of link between variable remuneration framework and risk appetite - Impaired consequence management (e.g. malus and clawback clauses exist only as a formality) - Lack of individual accountability, including in the bank’s remuneration and/or consequence management framework	- Incentive system does not incentivise desired behaviours - Promotion process does not reflect conduct/misconduct, ethics and behaviour - Applied metrics and limits are not commensurate with the bank’s actual level of risk and its risk appetite - Imbalanced deployment of financial performance criteria versus non-financial criteria - Wrong incentives, e.g. remuneration of the CRO linked predominately to commercial objectives or connected with the performance of activities that the risk management function monitors
Accountability	- Low stature and understaffing of internal control functions - RAF not comprehensive or well implemented - Weak information technology (IT) and data aggregation framework - Lack of a comprehensive “lessons learned” process to identify and address similar risks	- Unbalanced application of the third line of defence, i.e. the first line of defence lacking a culture of accountability for risk, leaving this to the second and third lines of defence - Insufficient transparency in reporting (especially in the case of issues/concerns) - Risk management seen as a barrier to achieving business objectives

3 Functioning and effectiveness of the management bodies

3.1 Role of the management body

The management body 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. It is expected 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.

A bank's management body defines, oversees and is accountable for the implementation of the governance arrangements that ensure the effective and prudent management of the bank.[39] To achieve this, the ECB is of the view that roles must be clearly defined and distinguish between an executive management function and a non-executive supervisory function. The management function is primarily responsible for directing the bank, while the supervisory function, as the top layer of any system of control, has no executive competences.[40]

The management body in its management function steers the institution, by making decisions and overseeing the day-to-day running of the bank by senior management. It also steers the definition and implementation of the bank's strategy, the performance of which is expected to be regularly monitored. The management body in its management function also ensures that the institution has a risk management system that allows the proper identification, assessment, monitoring and control of all risks to which the institution is or might be exposed.

The management body in its supervisory function oversees and challenges the management body in its management function. It ensures and periodically assesses the effectiveness of the institution's internal governance framework and takes appropriate steps to address any identified deficiencies, in particular with regard to the effectiveness of the bank's strategy, the internal controls of the risk management system and the internal audit system. This also includes the oversight of and accountability for the remediation of audit outcomes and supervisory findings.

To this end, the ECB expects members of the management body to effectively assess and challenge the decisions of the senior management where necessary and to effectively oversee and monitor management decision-making. Constructive challenge can be described as asking the right question at the right time with the right intent, thereby providing insight and support to the executive function. Hence, the capacity of a management body in its supervisory function to independently

[39] See Article 88(1) CRD.

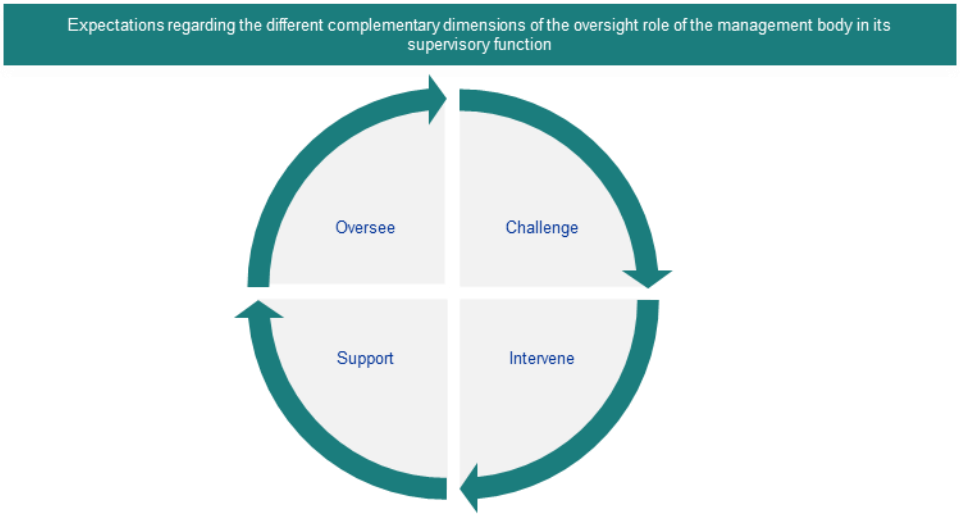
[40] EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraphs 28-31 and 32-34.

challenge the management function largely depends on the quality of debate, which is linked to, among other things, the suitability of individual members of the management body and of the management body collectively in terms of knowledge, skills and experience, diversity and other relevant factors.[41]

While constructive challenge may in practice also happen outside of management body meetings, substantial discussion and debate are expected to take place within the management body and its committees, and there is also expected to be evidence of this (in the form of meeting minutes). The ECB considers that this presupposes that all management body members are included in the discussions and have the opportunity to express their opinions.

Figure 3

Complementary dimensions of the oversight role of the management body in its supervisory function



3.1.1 Management body responsibilities

Notwithstanding the overall collegial responsibility of the management body, a clear allocation of responsibilities is important to ensure the accountability of members of the management body. In this regard, CRD VI provides that Member States are to ensure that institutions draw up, maintain and update individual statements setting out the roles and duties of each member of the management body in its management function, senior management and key function holders, and a mapping of duties, including details of the reporting lines and the lines of responsibility, and the persons who are part of the governance arrangements and their duties approved

41 See ECB Guide to fit and proper assessments, Section 3.5.

by the management body.[42] These statements should include both the details of reporting lines within the legal entity as well as at a functional level. The scope of each individual's duties is expected to be well defined, and no area of duties is expected to be left without ownership.[43]

These statements of duties and the mapping of the duties are to be made available at all times and communicated in due time, upon request, to the supervisory authorities.[44] The ECB also recommends banks to make use of these statements to define and allocate the responsibility for the remediation and follow-up of audit and supervisory findings and measures, linking them to appropriate incentives and remuneration.[45]

3.2 Structure of the management body in its supervisory function

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.

In most banks, the management body in its supervisory function delegates certain topics to specific committees.[46] In addition to an audit committee, significant institutions must establish risk, nomination and remuneration committees to advise on and prepare decisions to be taken by the full management body, which, however,

---

42 See Articles 74(1) and 88(3) of CRD VI (Directive (EU) 2024/1619 of the European Parliament and of the Council of 31 May 2024 amending Directive 2013/36/EU as regards supervisory powers, sanctions, third-country branches, and environmental, social and governance risks). Although Member States have until 10 January 2026 to transpose CRD VI by adopting and publishing the laws, regulations and administrative provisions necessary to comply with this Directive, the ECB encourages banks to start preparing their governance arrangements in order to be fully compliant when the national transposition measures enter into force. Article 3(1)(9) CRD VI defines "senior management" as those natural persons who exercise executive functions within an institution and are directly accountable to the institution's management body but are not members of that body, and who are responsible for the day-to-day management of the institution under the direction of the management body of the institution. In line with Article 3(1) (9a) CRD VI, "key function holders" means persons who have significant influence over the direction of the institution but are not members of the management body, including the heads of internal control functions and the chief financial officer (CFO), where those heads or that officer are not members of the management body. It also includes other key function holders identified on a risk-based approach by relevant institutions.

43 Recital 41 and Article 88(3) CRD VI.

44 Second subparagraph of Article 88(3) CRD VI.

45 See also Section 2.4 of this Guide.

46 For some institutions, the establishment of certain committees is obligatory, including the risk committee (Article 76(3) CRD); the nomination committee (Article 88(2) CRD); the remuneration committee (Article 95(1) CRD); and the audit committee (Article 41(1) of Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts (as amended by Article 1 no. 32 of Directive 2014/56/EU), amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87)). See the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 40. As a good practice, some institutions establish additional committees, such as a committee on ethics and compliance (see paragraphs 77-79 of the BCBS Guidelines on corporate governance principles for banks) or on ESG matters (see ECB Guide on climate-related and environmental risks, p. 22).

still retains ultimate responsibility for such decisions.[47] Under Article 76(3) CRD, competent authorities may allow institutions which are not considered significant under the CRD to combine the risk committee with the audit committee.[48] Members of the combined committee must have the knowledge, skills and expertise required for both the risk committee and the audit committee. Where, due to proportionality considerations, a specialised committee has not been established, these duties and obligations must be performed by the management body in its supervisory function.

A clearly defined and documented structure and scope of management body committees is key to fostering comprehensiveness of the topics discussed in the management body. It is expected that management body committees are designed to increase efficiency and allow a deeper focus in specific areas, and the structure and scope of committees are expected to be clearly articulated to avoid confusion resulting from possible overlaps on some topics. The ECB has the following expectations regarding the individual committees, where established.

- The risk committee should advise the management body on the institution's overall current and future risk appetite and strategy and assist the management body in overseeing the implementation of that strategy by senior management.[49]

- The audit committee has a central role in overseeing the internal audit function and in ensuring that it can perform its tasks in an independent and effective manner. Furthermore, the audit committee should at least support the management body regarding all aspects of preparing audit-related decisions and regarding matters related to external auditors, financial reporting and internal controls. Depending on the setup, the audit committee’s role can be broader than the oversight of the internal audit function.

- The nomination committee should at least support the management body in its supervisory function regarding all aspects of preparing decisions on the appointment of members of the management body and key function holders and of assessing the management body.[50] More specifically, it is expected that the nomination committee, among other things, defines the profiles needed for candidates and communicates this to stakeholders. The nomination committee is expected to play a key role in setting up and implementing the suitability policy and succession planning (see also Section 3.4.3) and the diversity policy.

---

47 Unless exempted under Article 39(2) and (3) of Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014 amending Directive 2006/43/EC on statutory audits of annual accounts and consolidated accounts (OJ L 158, 27.5.2014, p. 196).

48 In this case, the ECB expects banks to ensure at all times that the members of a combined committee possess, individually and collectively, the necessary knowledge, skills and expertise to fully understand the duties to be performed by the combined committee. The relevant topics should be well covered by the committee and the full management body. The ECB understands the concept of “significant institutions” for the purpose of Chapter 2 of Title VII CRD in line with the definition in paragraph 13 of the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05). Such institutions are referred to in this Guide as “CRD-significant institutions.”

49 For CRD-significant institutions, this is a requirement under Article 76(3) CRD. See also the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 61.

50 For CRD-significant institutions, this is a requirement under Article 88(2) CRD. Where, under national law, the management body does not have any competence in the process of selecting and appointing any of its members, Article 88(2) CRD on the establishment of a nomination committee does not apply.

In particular, the nomination committee should decide on a target for the representation of the underrepresented gender in the management body and set out how to achieve it.

- The remuneration committee should at least support the management body in its supervisory function regarding all aspects of preparing remuneration-related decisions.[51] To this end, the remuneration committee is expected, among other things, to provide its support and advice to the management body on the design of the institution's remuneration policy and to be involved in the preparation of decisions on the remuneration of members of the management function and other material risk takers. The remuneration committee should also ensure that incentives to take risks are balanced by incentives to manage risk and that remuneration is gender neutral in line with the EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04).

The committees are also expected to interact with each other where this is required for the subject under discussion.

3.3 Management body composition

3.3.1 Size of the management body in its supervisory function

It is expected that the size of the management body is appropriate to allow it to effectively carry out its oversight role and other responsibilities.

The size of a management body should not adversely affect its functioning. Indeed, it can have an impact on the quality of debate and hence on its effectiveness. While large management bodies can potentially hamper interactive discussions, small ones, conversely, sometimes face issues of limited discussion, challenges in the composition of their committees and potential concerns about the continuity of activities in the event of simultaneous departures of multiple members. Among significant institutions, in one-tier board structures management bodies have on average 11 non-executive directors and, in most cases, between one and three executive directors, while in two-tier board structures management bodies in their supervisory function have an average of 12 non-executive directors.[52] It is to be noted that the range is quite big, depending also on the governance structure and, potentially, on national specificities (such as the inclusion of employee representatives).

[51] For CRD-significant institutions, this is a requirement under Article 95(2) CRD.

[52] Based on 2023 data.

3.3.2 Collective suitability and diversity

In order to provide efficient and effective oversight, the management body needs to possess adequate collective knowledge, diversity of skills and experiences to be able to understand the institution's activities, including the main risks.

Management bodies need to have the right composition of members, having regard to the need for diverse perspectives, experience and knowledge. Although each member of the management body is not expected to know everything, each should have a basic knowledge in every area, and collectively they should have expert knowledge covering all areas. To this end, two main elements of the fit and proper assessment need to be determined.[53]

- First, is each member of the management body individually suitable? The criteria applied include reputation, knowledge, skills and experience, time commitment, and independence of mind.
- Second, is the management body as a whole collectively suitable? This requires an assessment of whether the management body's members are individually and collectively in a position to understand the institution's activities and the environment in which it operates, including the main risks proportionate to the size, complexity and risk profile of the bank.[54]

For this, the nomination committee must check the individual and collective suitability of the management body.[55] The outcome should be discussed within the management body in its supervisory function, also covering the composition and suitability of management body committees. These self-assessments should make use of the suitability matrix template provided by the EBA, or the institution's own appropriate methodology, and consider the needs of the management body according to the succession plan and role definitions.[56] The methodology is expected to be reviewed on a regular basis.

The ECB also believes that diverse management bodies make better business decisions.[57] Diversity includes inter alia aspects like educational and professional background, gender, age and geographical provenance, and in a broader sense can also include several other dimensions.[58] Management bodies that create a safe space to enable diversity of thought and continuous learning tend to develop a broader range of views and opinions based on different experiences, perceptions

---

53 Article 91 CRD. See also the ECB Guide to fit and proper assessments, p. 40.

54 See also Chapter 3.1 of the ECB Guide on effective risk data aggregation and risk reporting.

55 Assessments should be repeated annually for CRD-significant institutions (Article 88(2)(c) CRD) and every two years for other institutions (joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU (ESMA35-36-2319, EBA/GL/2021/06), paragraph 156).

56 Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU (ESMA35-36-2319, EBA/GL/2021/06), paragraph 150.

57 See recital 60 of Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013.

58 In line with the EBA Guidelines on benchmarking of diversity practices, including diversity policies and gender pay gap, under Directive 2013/36/EU and Directive (EU) 2019/2034 (EBA/GL/2023/08).

and values. This is crucial to avoid groupthink and for the management body to remain on top of the various topics it oversees in a rapidly changing environment.

Observed good practices

- 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.
- 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.
- In the nomination process, a candidate's misalignment with the bank's culture and values is a "showstopper" regarding the appointment.
- 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.
- CRD-significant institutions involve an external party at least every three years when performing management body self-assessments.
- When searching for candidates, institutions consult external service providers in order to have a larger pool of candidates available.
- To harness the benefits of diversity and create an inclusive environment, a bank's diversity policy covers the entire organisation and is not limited to the management body.

3.3.3 Independence and conflicts of interest

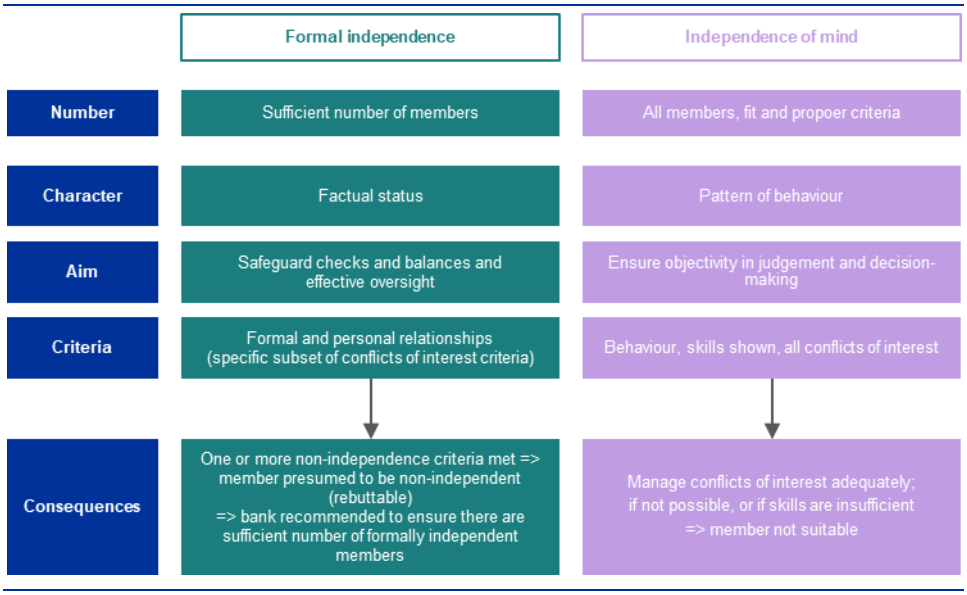
Subject to the requirement that all management body members must act with independence of mind, the ECB recommends that the management bodies in their supervisory function include a sufficient number of formally independent members to enhance checks and balances and facilitate effective oversight of management decision-making. Furthermore, banks need to have an adequate framework to properly manage potential conflicts of interest on an ongoing basis.

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 (see below), potentially limits its oversight capacity. Insufficient independence may adversely affect the sound management and coverage of risks of banks.

Figure 4

Formal independence and independence of mind



Concerning formal independence, the ECB follows the approach in the EBA guidelines.[59] According to the joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders, larger (CRD-significant) and listed banks should have a management body in its

[59] The requirement of "formal independence" for some members of the management body in its supervisory function is laid down in the national legislation of some Member States, which also determines in different ways how this criterion is defined. This is also envisaged in the joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU (ESMA35-36-2319, EBA/GL/2021/06). However, while the joint ESMA and EBA Guidelines distinguish between being independent and having independence of mind, this Guide uses the term "formal independence" instead of "being independent," clarifying that formal criteria apply.

supervisory function that includes a sufficient number of independent members.[60] While acknowledging the limits stemming from national law and noting different national approaches with regard to the joint ESMA and EBA Guidelines, the ECB strongly believes that a sufficient number of formally independent members is paramount to facilitate effective oversight of senior management. Indeed, in practice, ECB Banking Supervision has often observed more concerns around insufficient oversight and insufficient capacity to challenge in banks with a very low number of formally independent members of the management body in its supervisory function. Having a very low number of formally independent members is therefore not considered good practice, and the ECB carefully evaluates this element as part of its assessment of banks' governance arrangements.

The criteria to assess a member of the management body in its supervisory function as not formally independent include, for instance, any present or past relationships or links of any nature with the institution concerned or its management that could influence the member's objective and balanced judgement and reduce the member's ability to make decisions independently, the number of years spent on the management body of another entity within the scope of prudential consolidation, or possible family ties with members of the management body in its management function. However, meeting one of the criteria for non-independence does not automatically prevent a member from qualifying as independent. Rather, the supervised entity could justify why the management body member should still be considered to be formally independent.[61] In general, all independence criteria need to be assessed on a case-by-case basis subject to any provisions of national law.[62]

According to the joint ESMA and EBA Guidelines EBA/GL/2021/06), banks should have a sufficient number of formally independent members.[63] However, the Guidelines do not specify what constitutes a "sufficient number". Therefore, subject to the provisions of national law, the ECB assesses whether the management body of a bank has a "sufficient number" of formally independent members on a case-by-case basis, taking into account the impact that the level of formal independence has on the quality of debate and on the management body's capacity to challenge, as well as the size, complexity and characteristics of the bank, in line with the principle of proportionality. At the end of 2023, in significant banks, around 60% of non-executive members of management bodies in their supervisory function were regarded as being formally independent. In line with the EBA Guidelines, employee representatives are not counted towards the overall assessment of whether there are a "sufficient number" of independent members.

Regarding "independence of mind", no member of the management body, whether in its supervisory function or in its management function, can have any potential or

---

60 The joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU (ESMA35-36-2319, EBA/GL/2021/06) also outline a number of situations in which a management body member is presumed not to be "formally independent".

61 ibid., paragraphs 89 and 90.

62 For a non-exhaustive list of typical scenarios, see the joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU (ESMA35-36-2319, EBA/GL/2021/06), paragraph 89.

63 See paragraphs 87 and 88 of the guidelines.

perceived conflict of interest that may impede their ability to perform their duties independently and objectively without influence from other persons or due to other positions held.

To this end, it is expected that banks have an adequate conflicts of interest framework to properly manage potential conflicts of interest on an ongoing basis. While acknowledging that, in some countries, members of the management body in its supervisory function may be allowed by national law to have executive functions (in the same management body), the ECB is of the opinion that this is not best practice and exposes the management body members concerned to clear conflicts of interest, since both roles, executive and non-executive, are exercised by the same individual. Accordingly, the ECB recommends that banks review existing cases to ensure alignment with the principle of separation of executive and non-executive functions (see Section 3.1 above). The ECB also recommends that, in situations where the CEO of a bank moves to the position of chair of the management body in the same entity, adequate mitigating measures are put in place to ensure the independence of mind of the newly appointed chair, especially in view of possible conflicts of interests owing to the previously held position of CEO in the same entity.

3.3.4 Chair of the management body in its supervisory function

The role of the chair of the management body is key to fostering a culture of challenge and debate and to setting the tone from the top, which then cascades down throughout the whole organisation. To promote checks and balances, and as the main person responsible for the effective functioning of the management body, the chair should, as a general principle, be a non-executive member, and the ECB recommends that it is an independent member.

The chair of the management body in its supervisory function provides leadership to the management body and is responsible for its effective overall functioning, including maintaining a relationship of trust with its members. This role is key to maintaining the focus on core strategic issues, while entrusting the day-to-day management of the bank to the management body in its management function and to senior management. It is the chair's responsibility to create a strong link with them, foster a culture of challenge and debate within the management body, and set the tone from the top, which then cascades down the whole organisation. To this end, the decision-making process in the management body should not be dominated by the CEO in a manner that could be detrimental to the interests of the institution.

The ECB is of the view that, as a general principle, the chair of the management body in its supervisory function should be a non-executive member, and the ECB recommends as best practice that it is also an independent member.[64] The chair of

[64] EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 37; and BCBS Guidelines on corporate governance principles for banks (2015), paragraph 62.

the management body in its supervisory function must not simultaneously exercise the functions of a CEO within the same institution.[65]

The tasks and responsibilities of the chair include, inter alia, leading the management body, contributing to an efficient flow of information within it and vis-à-vis its committees, and being responsible for the effective overall functioning of the management body, including contributing to a clear allocation of duties among its members and the existence of an efficient flow of information between them.

The ECB strongly advocates a separation of executive and non-executive functions within the management body, meaning that the chair should be a non-executive member without any executive powers. While acknowledging that, in some countries, the chair may be allowed by national law to have executive functions, the ECB is of the opinion that this is not best practice and recommends that existing cases be reviewed. Where the chair has executive functions, it is recommended that mitigating measures be put in place to address inter alia (i) the unclear allocation of roles between the executive chair and the CEO, blurring the lines between management and supervisory functions; (ii) the concentration of powers in the executive chair; and (iii) the impact on checks and balances and the oversight role of the management body in its supervisory function.

3.3.5 Committee composition

The composition of management body committees should facilitate their oversight function. They should be composed of members with knowledge of the areas covered by the committee as well as a sufficient number of independent members.

According to the EBA Guidelines on internal governance (EBA/GL/2021/05), committees of the management body in its supervisory function should be composed of at least three members and should not be composed of the same group of members which form another committee.[66] When looking at committee compositions, banks need to consider whether current committee members have adequate expertise and can devote sufficient time to giving advice and challenging the proposals and information of all committees of which they are members, and whether committees have independent and strong chairs.

In line with the applicable EBA Guidelines, more specific expectations for individual committees include the following.

- In global systemically important institutions (G-SIIs) and other systemically important institutions (O-SIIs), the risk committee should include a majority of members who are formally independent, and the chair of the risk committee should be an independent member. In other significant institutions, as determined by competent authorities or national law, the risk committee should

[65] According to Article 88(1)(e) CRD. Under CRD VI, a former waiver under which institutions could justify a deviation subject to the approval of the authorities has been discontinued.

[66] See paragraphs 48 and 49.

include a sufficient number of members who are independent and should be chaired, where possible, by an independent member. In all institutions, the chair of the risk committee should be neither the chair of the management body nor the chair of any other committee.[67]

- In the audit committee, the majority of members should be formally independent, including the chair, who should be appointed by its members or by the management body. At least one member of the audit committee must have competence in accounting and/or auditing.[68]

- In G-SIIs and O-SIIs, the nomination committee should include a majority of members who are formally independent and should be chaired by an independent member.[69] Members of the nomination committee should have, individually and collectively, appropriate knowledge, skills and expertise concerning the selection process and suitability requirements as set out in the CRD.[70]

- In G-SIIs and O-SIIs, the remuneration committee should include a majority of members who are independent and should be chaired by an independent member. In other CRD-significant institutions, the remuneration committee should include a sufficient number of formally independent members, including the chair. The remuneration committee should collectively possess appropriate knowledge, expertise and professional experience concerning remuneration policies and practices as well as risk management and controls.[71]

---

67 See EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 54. For ECB expectations on formal independence, please see Section 3.3.3 of this Guide.

68 Article 39(1) of Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts (as amended by Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014), amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (OJ L 157, 9.6.2006, p. 87) National law may be stricter.

69 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 52.

70 ibid., paragraph 53.

71 EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04), paragraphs 55 and 56.

Figure 5
Committee composition

Specific expectations for individual committees based on the applicable regulatory framework					
		Risk committee*	Audit committee**	Nomination committee*	Remuneration committee***
Formal independence of chair		✓ (neither chair of the management body nor chair of any other committee)	✓	✓	✓
Formally independent members	G-SIIs/O-SIIs	majority	majority	majority	majority
	Other CRD-significant institutions	sufficient number	majority	sufficient number	sufficient number

* Paras. 46 ff. of EBA/GL/2021/05.
** Paras. 46 ff. of EBA/GL/2021/05 and Article 39(1) of Directive 2006/43/EC (as amended by Directive 2014/56/EU of the European Parliament and of the Council of 16 April 2014).
*** Paras. 55 of EBA/GL/2021/04.

3.4 Functioning and effectiveness of management bodies

3.4.1 Organisation of the management body in its supervisory function

The management body is expected to define appropriate practices for its organisation and define the means for such practices to be followed and periodically reviewed.

The practices and organisation of management bodies play a critical role in their functioning and effectiveness, both in their management and in their supervisory function. Specifically, for the supervisory function, the ECB expects management body members to prepare thoroughly for meetings and thus be able to identify areas in which they can challenge the management function; this includes collecting information from other sources. The ECB considers that the proper exercise of the task of approving and overseeing the implementation of the institution's strategic objectives, risk strategy and internal governance supposes that the management body and its respective committees devote sufficient time to debate.[72] It is therefore essential that individual members dedicate sufficient time for adequate preparation and that the full management body in its supervisory function and its main committees meet frequently and for a sufficient length of time. To ensure sufficient time, banks should verify whether the proposed time commitment of the members of the management body reflects adequately the frequency and duration of its meetings as well as the number and complexity of the items on the agenda.

[72] Article 88(1)(a) CRD.

It is expected that members of the management body have a proactive role in shaping meeting agendas and suggesting topics to be discussed rather than leaving it to senior management alone to set the agenda through the proposals submitted for decision. Furthermore, the ECB expects the management body to regularly ensure that agendas cover a comprehensive range of topics, reflecting the size, complexity, business model and risks of the institution, while not being overloaded. Most importantly, it is expected that institutions define practices to allow open and critical debate in the management body, ensuring that dissenting views can be expressed and discussed.

Observed good practices

- The management body assigns specific subjects to individual non-executive members ahead its meetings to facilitate the discussion.
- To increase their capacity to challenge, management body members gather insights and knowledge from the bank's different business areas, for example by meeting with lower-level executives and heads of internal control functions.
- The management body collects views from outside the institution about the external environment and about the institution itself.
- The consequences of possible decisions on strategic topics (e.g. budget process, asset transfers, IT projects, etc.) in terms of risks are systematically discussed within the management body.
- The bank appoints members with specific expertise/national backgrounds on the basis of the institution's risk profile and future business development, depending on its business model and geographical footprint.
- Continuous training sessions for management body members are divided into a general and a tailor-made part (structured on the basis of an expertise matrix); training is given by external providers and members of the management function.
- In a crisis situation or emergency, a group-wide crisis committee is established with the participation of senior executives (e.g. CRO, CEO, CFO, chief information officer) and all relevant units, such as the head of human resources (HR), representatives of the marketing, communication and IT departments and internal control functions, with daily meetings. The management body increases the frequency of committee meetings for the most affected risks.
- The bank provides a clear indication of roles and responsibilities of executive and non-executive members of the management body, allowing sufficient time for meaningful preparation of management body meetings to ensure their effective functioning.
- Induction programmes are provided for new members of the management body in its supervisory function informing them about the institution's internal organisation and key contact persons in the most relevant departments from whom they may directly request information needed in the performance of their roles.

3.4.2 Interaction between the management body and its committees

It is expected that management bodies develop practices to facilitate interaction between the management body and its committees to ensure the proper flow of information and strong oversight.

In view of the management body's overall responsibility for the institution, the ECB considers it essential to have in place practices to facilitate interaction between the management body in its supervisory function and its committees as well as among the different committees.[73] This allows committees to have more focused discussions, keeping in mind that the ultimate responsibility for outcomes lies with the management body. Therefore, these practices should be aimed at reducing information asymmetries among members.

During full management body meetings, all members should be informed about the outcomes of discussions in the committees and be given the opportunity to provide any additional input or views, including on those items for which decision proposals were prepared in one of the committees. Furthermore, the chair of each committee should report periodically to the management body, and its members should have access to the information discussed in all management body committees.

In particular, interaction is expected between the risk and remuneration committees regarding the risk alignment of variable remuneration, and between the remuneration and audit committees regarding the design, implementation and effects of the institution's remuneration policies.

Members of the management body in its management function can join committee meetings and must do so for specific agenda items to present proposals and answer questions, enabling and facilitating the work of the oversight function. Nevertheless, the ECB is of the view that the systematic presence of the management function, and in particular the CEO, during entire committee meetings might hamper discussions among members of the management body in its supervisory function and therefore limit constructive challenging. This is particularly relevant for risk and audit committee meetings, where it is expected that executives step out of nomination and remuneration committee meetings when their own position, performance or remuneration are being discussed.

Banks are expected to maintain and periodically update their organisational procedure or other similar document setting out their organisation, responsibilities and key activities.

Observed good practices

- One-to-one meetings are organised between the committee chairperson and heads of internal control functions are organised to discuss relevant topics (e.g. resources, regular reporting, performance assessment, discussion of the agenda before each meeting, etc.), the content and outcome of which are reported back to the full management body.

[73] Article 88(1)(a) CRD.

- Banks have clear internal rules stating that members of the management body in its management function shall be present in committee meetings for certain agenda items and upon invitation (in some Member States this is laid down in national law).
- The management body agendas differentiate clearly between ‘open’ committee sessions (open to all management body members) and ‘closed’ sessions (only open to for non-executive members).
- The audit and risk committees are responsible for conducting appraisals of the heads of the internal control functions, and remuneration decisions are taken in collaboration with the remuneration committee (such decisions may be based on proposals presented by the CEO to the committees or the management body, which then can sufficiently challenge the proposals, leading to adjustments where necessary).
- The committee chair informs the whole management body after each committee meeting, also providing briefing notes, summary/action points from meetings.
- Internal charters lay down the frequency and minimum content of reporting to the management body by the head of the internal audit function.
- The risk management function regularly provides to the remuneration committee the subset of KPIs to be included for the risk-adjusted evaluation of the bonus pool.
- Joint committee meetings take place, e.g., between the audit or remuneration committee and the risk committee on internal control function-related items.
- Cross-participation: a member of the risk committee participates in the meetings of other committees (e.g., the chairperson of the audit committee is a member of the risk committee, ensuring a link between the two bodies; a remuneration committee member is also a member of the risk committee).
- Banks internal organisational procedures include inter alia rules for including items on agendas of meetings, timelines for sharing documentation with members ahead of meetings, and rules on the participation of observers.

Observed good practices

Nomination Committee:

- As part of the selection process, the scrutiny of candidates is discussed during the nomination committee meetings. The discussion is based on a candidates list provided internally or by an external company and involves the capabilities for the specific roles and the time commitment and making concrete recommendations to the management body/shareholders’ meeting.

Remuneration Committee:

- The remuneration committee makes concrete recommendations on executives’ scorecards, e.g., recommended differentiation of the weight of KPIs for different executives.

- The remuneration committee proposes a review of KPIs for executives who have significantly changed their roles during a year.

Audit Committee:

- The audit committee is regularly informed about the ongoing implementation of the audit plan with the use of KPIs (audits completion, quality of audit reports, etc.) as well as other aspects of internal audit functions effectiveness (follow-up of findings and backlog, staff turnover and rotation).
- The audit committee chairperson asks to receive final audit reports with a poor rating.
- The escalation of audit reports with high-risk findings from the local audit committee is clearly described in internal policies and adhered to in practice (group-wide oversight).
- The head of the internal audit function and members of the audit committee hold a private session without the presence of management to discuss issues of interest at the end of each committee meeting or ask observing members of the management body in its management function to leave the room for certain agenda items.

Risk Committee:

- The risk committee meets regularly and frequently, at least quarterly (for G-SIIs global systemically important banks around 11 times per year).

3.4.3 Management body and committee documentation

It is expected that the management body and committees' documentation is clear and contain the right balance of comprehensiveness and conciseness, enabling meaningful discussions at management body level. Agendas and documentation should be shared sufficiently far in advance of meetings and the management body should maintain appropriate records of its deliberations and decisions.

It is expected that the management body and committees' documentation is clear and contain the right balance of comprehensiveness and conciseness, enabling meaningful discussions at management body level. Agendas and documentation should be shared sufficiently far in advance of meetings and the management body should maintain appropriate records of its deliberations and decisions.

The ECB considers it essential for the proper performance of the tasks of the management body and its committees that its members are provided with clear and concise documentation, enabling meaningful discussions at management body level. Agendas and documentation should be shared sufficiently early before meetings to allow members to familiarise themselves with the topics and prepare. Even on technical topics, supporting documentation should be tailor-made for the needs of the management body and its committees, including, for example, executive

summaries and highlighting the risks, opportunities, costs and benefits of the various items on which decisions are expected to be taken or a committee's advice is sought. Moreover, the management body and its committees should maintain appropriate records of their deliberations and decisions, providing an adequate summary of matters reviewed, recommendations made, decisions taken and dissenting opinions.

Observed good practices

- There is a process of agenda setting throughout the whole year (which can be adjusted) to ensure a comprehensive coverage of all risks and material processes.
- A written policy provides that agendas and documentation are shared sufficiently early before the meetings (at least five working days in advance).
- The minutes describe the time and date of meetings, their duration, the members present and absent and their respective functions/roles, and state whether any conflicts of interest exist. They allow an understanding of different views brought up when topics are discussed, and when decisions are taken, and of the nature of challenge provided by non-executive members and include follow-up points, actions, or requests.

3.5 Policies concerning the composition and functioning of management bodies

3.5.1 Suitability policies

A bank's suitability policy should accurately reflect all five fit and proper criteria. It should clearly outline the criteria applied to determine the suitability of management body members, guidance on how these are assessed and a transparent selection process to ensure that only suitable candidates are put forward to become management body members.

Banks themselves have primary responsibility for the initial and ongoing assessment of the suitability of the members of the management body and key function holders.

The suitability policy should state clearly how the fit and proper criteria are assessed and assign roles and responsibilities linked to concrete steps in the internal procedure for the suitability assessment.[74] Furthermore, the policy should be reviewed regularly, both in its design and in its implementation, and should reflect any findings or feedback from the nomination and audit committees.

[74] The fit and proper criteria are: (i) experience; (ii) reputation; (iii) conflicts of interest and independence of mind; (iv) time commitment; and (v) collective suitability. See also the ECB Guide to fit and proper assessments.

Observed good practices

- Specific suitability criteria that are relevant for the bank and go beyond standard fit and proper criteria are included, such as on soft skills.
- Policies include sections on the start-up and onboarding of new management body members as well as training needs.
- Policies are publicly available (e.g. via the bank's website).

3.5.2 Diversity policies

Banks' diversity policies are expected to outline the institution's approach to promoting diversity in its various aspects (e.g. educational and professional background, gender, age, and geographical provenance). Regarding gender diversity, the ECB expects that banks' policies include provisions on gender targets at management body level and monitoring of compliance with targets as well as provisions on the monitoring of gender pay gaps.

When it comes to gender targets, ECB Banking Supervision takes all applicable legal requirements, at both EU and national level, into account.[75] Gender diversity considerations have also been added to the ECB's Guide to fit and proper assessments.

All institutions are required to put in place a policy promoting diversity in the management body.[76] In addition, CRD-significant institutions have to set targets and policies relating to gender diversity and disclose them.[77] This policy needs to explain how the targets can be credibly achieved within a set timeframe.

Observed good practices

- Banks perform statistical analyses to understand the representation of gender and different age ranges in the bank.
- Banks monitor the underrepresented gender within the management bodies and with respect to promotions and salary increases.
- Banks seek to appoint a diversity manager and/or gender balance expert to the nomination committee.

[75] The ECB also takes into account the provisions of Directive (EU) 2022/2381 of the European Parliament and of the Council of 23 November 2022 on improving the gender balance among directors of listed companies and related measures (OJ L 315, 7.12.2022, p. 44).

[76] Article 91(10) CRD; see also the joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU (ESMA35-36-2319, EBA/GL/2021/06), paragraphs 104 to 108.

[77] Article 88(2)(a) CRD.

- The compliance function assesses the compliance of the diversity policy with regulations and internal policies.
- The internal audit function carries out an independent review of the implementation of the diversity policy.

3.5.3 Succession planning

Institutions should establish a succession planning process which describes the way in which the bank ensures an adequate transition and the continuity of activity of management body members.

A smooth and well-defined transition process from one position holder to the next can be of substantial importance for the well-functioning of a management body. This applies to planned departures but even more so in cases where the need for a new appointment occurs suddenly and unexpectedly. If succession planning is not well formalised, this can jeopardise the continuity of activity on the management body, especially if some members represent key areas of expertise as part of the collective knowledge of the management body, or if there is a concentration of departures within a short period of time.

The ECB therefore expects that institutions establish a succession planning policy and process which describes the way in which the bank ensures an adequate transition and the continuity of activity of key function holders and management body members, including members of the management body in both its management and its supervisory function and, in particular, the chair and the CEO. This can be set out in the charter of the management body, in the policy for the selection and appointment of management body members and key function holders (suitability policy) or in a separate document. It should include principles on the selection (as defined in the suitability policy), monitoring and succession planning of members and on the re-appointment of existing members.

Where several members of the management body leave at the same time, the ECB expects institutions to develop and implement mechanisms to avoid and mitigate any resulting negative effects.[78] Succession planning should also take into account the objectives and targets set out in the institution's diversity policy.[79]

Observed good practices

- Banks identify the profile of possible future candidates in advance and maintain lists of internal successors which are reviewed and updated at least annually.

[78] Joint ESMA and EBA Guidelines on the assessment of the suitability of members of the management body and key function holders under Directive 2013/36/EU and Directive 2014/65/EU (ESMA35-36-2319, EBA/GL/2021/06), paragraph 133.

[79] ibid.

- Banks draw up and regularly maintain a list of potential candidates as a precautionary measure to address situations in which it might be difficult for the institution to find potential successors.
- Banks use specific tools for succession planning like talent pool heatmaps or succession planning maturity indices (which anticipate upcoming appointment needs).
- Banks adhere to diversity policy targets in the context of succession planning.
- Banks have mechanisms in place to avoid and mitigate negative effects in the event that several members of the management body leave at the same time.

4 Internal control functions

The CRD requires banks to have in place robust governance arrangements which include, among other things, effective processes to identify, monitor and report risks and adequate internal control mechanisms.[80] The EBA Guidelines on internal governance (EBA/GL/2021/05) describe the practices to be followed by banks to develop and maintain a culture that encourages a positive attitude towards risk control and compliance within the bank and a sound and comprehensive internal control framework.[81] The management body function is responsible for establishing and monitoring the internal control framework, with its implementation being the responsibility of the whole bank, through the three lines of defence.

To ensure the adequacy of the internal control mechanisms, the ECB expects they are based on a three lines of defence model.[82]

- 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.[83] The business lines ensure prudent risk-taking, risk management and compliance in order to ensure a sound risk culture across the bank.

- Second line of defence: The risk management function is responsible for further identifying, measuring, monitoring and reporting risks to which a bank 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.[84]

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

---

80 Article 74 CRD.

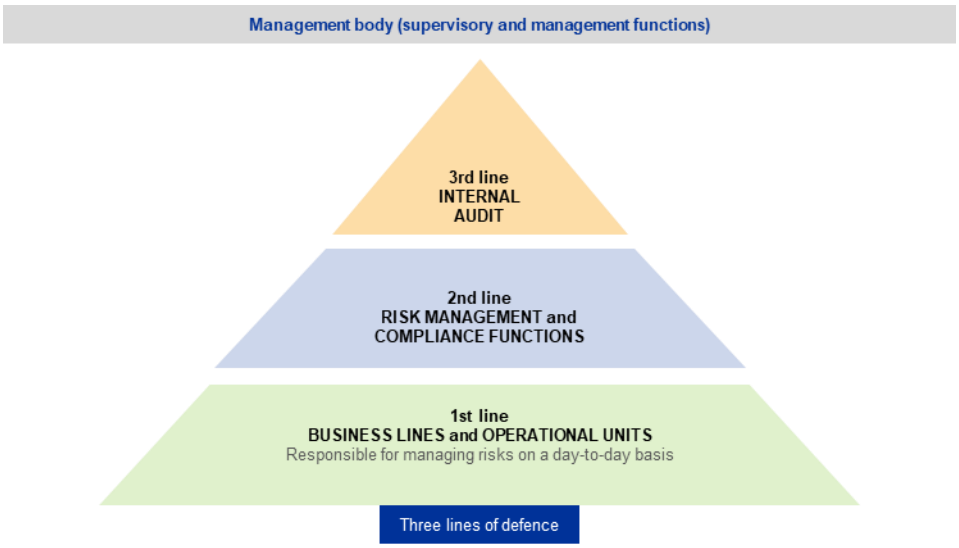
81 See Title V of the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05). On the internal control functions, see paragraphs 169-224 of these guidelines.

82 ibid. See also the BCBS Guidelines on corporate governance principles for banks, paragraph 13.

83 See EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 32 under "Background and rationale".

84 See EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 33 under "Background and rationale": as part of the second line of defence, banks may set up additional specific control functions (e.g. IT security control or AML compliance function).

Figure 6:
The three lines of defence model



The ECB expects that banks have in place well-functioning and independent internal control functions (risk management, compliance and audit) that have sufficient authority, stature, reporting lines and resources to perform their functions. The internal control functions and the business lines are pivotal in ensuring a coherent risk culture in a bank by assuming accountability for risks (see also Section 2 of this Guide).

4.1 Governance of internal control functions

4.1.1 Stature, authority and independence

The internal control functions should have sufficient stature and authority to perform their duties, as well as independence from the business activities they monitor and control. It is also expected that the internal control functions' opinion on the bank's business and activities is duly considered by the management body.

In line with the EBA Guidelines on internal governance (EBA/GL/2021/05), the internal control functions should have appropriate and sufficient authority, stature and access to the management body to fulfil their mission.[85]

The management body should ensure that the internal control functions are independent of the business lines they control.[86] The EBA Guidelines outline criteria

[85] Article 76(5) CRD as amended by CRD VI; EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 141.

[86] EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 68.

for the adequate functioning of control functions, including ensuring the independence of the internal control functions in terms of their reporting lines and keeping the internal control functions separate from the activities they are assigned to monitor and control.[87] While it is expected that banks ensure that the head of an internal control function stays independent, this should not impede their ability to access the person who has the exclusive role of managing the activities that the internal control function monitors and controls.

With regard to the heads of internal control functions, the ECB is of the view that they should be senior managers at an adequate hierarchical level to provide them with the appropriate authority, benefitting from clear management support as well as having the stature and authority needed to fulfil their responsibilities.[88] Members of the management body may also be responsible for an internal control function, provided they do not have other mandates (e.g. responsibility for a specific operational business line or revenue-generating function) that could give rise to conflicts of interest and would compromise their internal control activities and the independence of the internal control function.[89]

In order to ensure the functioning and stature of the internal control functions, banks need to allow them unhindered access to the management body, including to the relevant committees, and this access is expected to be utilised in practice and properly documented. It is expected that the management body, or its relevant committee, assess and reinforce the stature and independence of the bank's internal control functions at least annually.

4.1.1.1 Access to the management body in its supervisory function

The ECB is of the view that the management body should have unhindered and direct access to the heads of the internal control functions and vice-versa in order to support them fulfilling their duties.

As outlined in the BCBS Guidelines on corporate governance principles for banks and the EBA Guidelines on internal governance (EBA/GL/2021/05), the management body should have full and direct access to the heads of the internal control functions and this access should be frequently exercised.[90] Equally, it is expected that the

---

87 ibid., paragraph 175.

88 In line with the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), "heads of internal control functions" means the persons at the highest hierarchical level in charge of effectively managing the day-to-day operation of the independent risk management, compliance and internal audit functions. Under Article 76(5) CRD as amended by CRD VI, Member States shall, in accordance with the proportionality requirement laid down in Article 7(2) of Commission Directive 2006/73/EC, ensure that institutions have internal control functions independent of the operational functions and which shall have sufficient authority, stature, resources and access to the management body. Under Article 76(6) as introduced by CRD VI, internal control functions shall, in particular, be able to raise concerns and warn the management body in its supervisory function where appropriate or where specific risk developments affect or may affect the institution.

89 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraphs 26 and 107(a).

90 See the revised BCBS Guidelines on corporate governance principles for banks, paragraphs 110,137 and 142; and the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 173.

heads of the internal control functions report regularly to the management body in both its supervisory and management functions and to its relevant committees and to have direct access to the management body in its supervisory function where necessary.[91] The heads of the internal control functions are also expected to be able to meet with the management body or its committees without members of the management body in its management function being present. In this respect, the ECB recommends that the heads of internal control functions hold bilateral periodic meetings with the chair of the management body and the chairs of the relevant management body committees (e.g. the risk, remuneration or audit committees). This also means that the heads should have the ability to present reports and findings via regular and ad hoc access to the management body and its committees, without any impediment and without management filtering. [92] It is recommended that the bank's internal policies define the frequency of such regular reports and the underlying process for ad hoc reporting.

4.1.1.2 Performance assessment, remuneration and appointment

The ECB expects the management body in its supervisory function and/or specialised management body committees to be involved in the performance assessment, remuneration and appointment of the heads of the internal control functions.

It is expected that a bank’s specialised management body committees and/or the management body in its supervisory function are involved and have a key role in the assessment of the performance of the heads of the internal control functions and to approve, or recommend to the management body for its approval, the annual remuneration of the internal control functions as a whole, including the KPIs.[93] The criteria used for the assessment of performance and risks for variable remuneration purposes should be determined separately from the business units that the internal control functions control and be predominantly based on control-related objectives, while it is also expected that their remuneration is predominately fixed.[94]

In order to preserve the independence and objectivity of the internal control functions, the remuneration of senior officers in these functions should be directly overseen by the remuneration committee or, in its absence, the management body in its supervisory function.[95] The heads of the internal control functions should also not

---

91 See Article 76(5) CRD as amended by CRD VI. Under Article 76(6) as introduced by CRD VI, internal control functions shall, in particular, be able to raise concerns and warn the management body in its supervisory function where appropriate or where specific risk developments affect or may affect the institution.

92 For further information on the management body and on reporting to the management body committees, see Section 3 of this Guide.

93 The criteria used for assessing performance and risks should predominantly be based on the objectives of the internal control functions. Variable remuneration for control functions should predominantly follow from control objectives, e.g. the Tier 1 ratio, the non-performing loan ratio, the non-performing loan recovery rate or, in the case of the internal audit function, audit findings. See EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04), paragraph 233.

94 ibid., paragraphs 196 and 232-234.

95 ibid., paragraphs 37 and 58.

be removed without the prior approval of the management body in its supervisory function, and the reasons for any such removal should be given.[96] Moreover, appointments should be subject to the prior approval or opinion of the management body in its supervisory function and/or the relevant specialised management body committee. Institutions should also have documented processes in place to assign the position of head of an internal control function and for withdrawing his or her responsibilities.[97]

4.1.2 Combining of functions

A separation of internal control functions is expected as well as a division of duties in order to avoid "dual-hatting," prevent conflicts of interest and preserve the independence of the control functions.

On the combining of functions, taking into account the proportionality criteria, the risk management function and compliance function may be combined. However, in principle, a separation of internal control functions would be expected.[98] In this respect, the separation of functions means that functions should be performed by different units, with a dedicated head allocated to each unit. There may, however, be exceptions, also taking into account the proportionality criteria and different practices regarding the reporting lines. Nevertheless, in all cases, reporting lines of internal control functions need to ensure their independence and that there are no conflicts of interest between the combined internal control functions.[99] Moreover, the internal audit function should not be combined with any other internal control function.[100]

The governance arrangements to be defined by the management body must ensure, among other things, the segregation of duties in the organisation.[101] The ECB expects such segregation to preclude "dual-hatting" of roles across different lines of defence in order to preserve independence and prevent conflicts of interests.[102] It is expected that this will apply both to the heads of the internal control functions and to the members of the management body in its management function with direct responsibility for an internal control function.

For example, the role of the CRO or head of the risk management function must be filled by an independent senior manager with distinct responsibility for the risk management function, except where proportionality is applied and there are no

---

96 See Article 76(6) CRD as introduced by CRD VI and EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 174.

97 See EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 174.

98 Particularly in the case of significant institutions.

99 See also EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 201.

100 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 176. CRD VI adds a new paragraph 6 to Article 76, clarifying that the internal audit function shall not be combined with any other business line or control function of the credit institution.

101 In accordance with Article 88(1) CRD.

102 Article 88 CRD. For further information on the management body, see Section 3 of this Guide.

conflicts of interest.[103] In order to ensure the CRO's independence, the CRO should not have management or financial responsibility related to any operational business lines or revenue-generating functions, and there should be no "dual-hatting" (i.e. the chief operating officer, CFO, chief auditor or other senior manager should in principle not also serve as the CRO).[104]

4.1.3 Resources and staffing of the internal control functions

The ECB expects that the internal control functions are sufficiently staffed, with qualified employees who are knowledgeable of both financial and non-financial risks.

In line with the EBA Guidelines on internal governance (EBA/GL/2021/05), the ECB expects the management body of a bank to ensure that the internal control functions have appropriate financial and human resources to fulfil their tasks.[105] In practice, banks are recommended to monitor the adequacy of resources on a regular basis, define the training needs at least annually, and devise a plan to remediate identified gaps. In addition to financial and human resources, it is expected that banks ensure the availability of technical resources for the fulfilment of the tasks and responsibilities of internal control functions. In this context, it is essential that banks ensure that their internal control functions have appropriate tools and processes, including IT systems and tools to assist data analysis and communication.[106]

In addition, it is expected that banks ensure that the internal control functions have an adequate number of qualified staff, at both parent and subsidiary level, possessing sufficient knowledge, skills and experience. It is expected that the members of the internal control functions, including their heads, have a sufficient understanding of financial and non-financial risks, new emerging risks, and data and reporting requirements.[107] It is essential that a bank's internal control function staff remain qualified and receive relevant training.

If heads of internal control functions are subject to fit and proper assessments pursuant to national law as key function holders, or if they are also management body members, it is expected that they have an up-to-date understanding of the

---

103 See Article 76(6) CRD and EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 201. In this Guide, the terms "CRO" and "head of the risk management function" are used interchangeably to refer to the head of the risk management function as per Article 76 CRD. When the head of the risk management function is one level below the management body in its management function and reports to one of its members, that member should not also be responsible for business lines or other activities subject to monitoring by the risk management function.

104 BCBS Guidelines on corporate governance principles for banks, paragraph 110. For further information on the role of the CRO, see Section 4.2.1 of this Guide.

105 Article 76(5) CRD as amended by CRD VI and EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraphs 177 and 178. In addition, in line with the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), Section 18 on new products and significant changes, banks should not initiate new business (or products, services, distribution channels, markets) if they have not yet verified that the existing capabilities of the internal control functions are commensurate with the emerging risks.

106 The EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 178, outline that internal control functions should have appropriate IT systems and support at their disposal, with access to the internal and external information necessary to meet their responsibilities.

107 ECB Guide on effective risk data aggregation and risk reporting, p. 6.

business of the bank and of the risks the bank may be exposed to.[108] If a bank intends to outsource operational tasks of the internal control functions or any activities, it should do this in line with the EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02)[109] and its own outsourcing policy. This notwithstanding, where a bank outsources any operational tasks, it should duly take into account the proportionality criteria.[110]

4.1.4 Roles, responsibilities and processes

It is expected that internal control functions have clearly defined roles and tasks as well as a clear allocation of responsibilities.

It is expected that banks ensure that internal policies define the roles and tasks of the internal control functions and ensure a clear allocation of responsibilities across the three lines of defence (as further expanded on in Section 4.2. of this Guide). This clear allocation of roles and responsibilities is critical to ensure strong accountability for proper risk management as an indispensable element of a sound risk culture. It is also recommended that internal policies include expected interactions between internal control functions, namely the compliance and risk management functions, to ensure that the latter has a holistic view of all the risks the bank is or might be exposed to.

The management body should also be properly informed by the control functions of major identified deficiencies and risks, the recommendations and corrective measures to be taken, as well as the deadlines for their implementation.[111] It is key that the management body is regularly informed of the overall status and functioning of the internal control functions and receives relevant information concerning the bank's subsidiaries and branches. It is expected that the management body is periodically informed on the performance of the operational tasks of the outsourced internal control functions, and the frequency of the updates is expected to be commensurate with the materiality of the functions outsourced.[112] The management body is also responsible for approving the bank's strategy to comply with restrictive measures and ensure its proper implementation.[113] It is expected that the management body is expected to form, on an annual basis, a comprehensive view on the functioning of the control functions and have a clear opinion on strengths and areas for improvement.

In view of the oversight function of the management body and the requirement that banks periodically assess the effectiveness of their governance arrangements, it is

---

[108] See ibid, p. 13.

[109] See EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02).

[110] On proportionality, see EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), Title I, paragraph 18.

[111] EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 151.

[112] See EBA Guidelines on outsourcing arrangements (EBA/GL/2019/02), paragraph 102.

[113] See Consultation paper on draft EBA Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures (EBA/CP/2023/42).

the ECB's understanding that the internal policies and processes of the bank ensure that the management body in its supervisory function and, where established, the specialised management body committees have a formal and active role in this annual assessment of the effectiveness of internal control functions and oversee the follow-up of any measures taken to address identified weaknesses.[114]

Similarly, in the case of consolidation, the timely integration of a bank's internal control and risk management framework is expected, in line with its consolidation plan, in order to ensure that execution risks are appropriately mitigated.[115]

4.2 Specificities of each internal control function

4.2.1 Risk management function

The ECB expects that banks have in place a central risk management function that facilitates a holistic view of and involvement in all risks, both financial and non-financial.

The main responsibility of the risk management function is to ensure that all risks are identified, assessed, measured, monitored, managed and properly reported by the relevant units in the institution.[116] It should be actively involved at an early stage in setting the institution's risk strategy, in ensuring the bank has effective risk management processes in place, and the risk appetite is appropriately translated into specific risk limits that are properly applied throughout the group.[117] The ECB expects banks to have in place a central risk management function that facilitates a group-wide holistic view across financial and non-financial risks.[118]

In line with the EBA Guidelines on internal governance (EBA/GL/2021/05), the risk management function's involvement in decision-making processes should ensure that relevant risk considerations are taken into account appropriately.[119] However, to preserve the independence of the risk management function and ensure a proper risk culture, the ECB considers that accountability for the decisions taken remains with the business units, and ultimately the management body. Against this background, it is expected that an appropriate escalation process is defined.[120] In the case of certain decisions (e.g. decisions to grant new loans, or certain investment

---

114 See Article 88(1) CRD.

115 The term "consolidation" means any combining of pre-existing independent legal entities that is relevant from the perspective of prudential supervision of institutions by European banking supervision, including mergers of institutions and acquisitions of one institution by another, but excluding intra-group transactions. See the ECB Guide on the supervisory approach to consolidation in the banking sector.

116 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 191.

117 ibid., paragraph 187. For expectations regarding the RAF, see Section 5 of this Guide.

118 ibid., paragraph 185. In the case of groups, this is also expected at a consolidated level in view of the level of application of the requirements in accordance with Article 109 CRD.

119 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 188.

120 In line with the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 188.

decisions), a sufficient balance is expected between the independence of the risk management function and its involvement in the decision-making process. To ensure that the independence of the risk management function is preserved at all times, the ECB expects it to be verified periodically.[121] Ideally, such verifications also encompass the application of mitigation measures, if needed.[122] In any case, the ECB is of the view that the risk management function should not have the power to initiate business decisions.[123]

A CRO or a senior risk officer should be in place as head of the risk management function with exclusive responsibility for that function, for monitoring the institution's risk management framework across the entire organisation, and for providing comprehensive and understandable information on risks and advising the management body.[124] The CRO should be a senior manager with sufficient expertise, independence and seniority to challenge decisions that affect an institution's exposure to risks.[125] It is expected that the CRO participates in senior management meetings at which the risk profile of the institution is discussed and strategic risk decisions are made. In this respect, the CRO should have all risks, both financial and non-financial, in their portfolio and monitor the full life cycle of these risks. With regard to the CRO's incentives, in order to ensure a sound risk culture and accountability and to facilitate prudent risk-taking, the CRO's remuneration should be based predominantly on the objectives of the internal control functions but may also be based to some extent on the performance of the institution as a whole.[126] It is therefore the ECB's understanding that the weight of risk/control-related KPIs should be higher for the CRO than for other senior managers. In this context, the CRO should be able to challenge decisions taken by the institution's management and its management body and speak up if the CRO considers that risk considerations are not well taken into account, and any grounds for objections should be formally documented.[127]

---

121 Article 76(5) CRD. See also the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 175.

122 Article 76(5) of the CRD. See also the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraphs 175, 183.

123 However, the CRO (or other risk management function representatives in credit decision-making bodies) may be granted a veto power over decision-making (e.g. for credit or investment decisions), accompanied by proper escalation/appeal procedures. See also EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 202, and EBA Guidelines on loan origination and monitoring (EBA/GL/2020/06), paragraph 69.

124 In line with the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraphs 200 and 201.

125 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 201.

126 See EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04), paragraphs 232-234.

127 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 202.

Observed good practices

On the identification and monitoring of risks (including emerging risks):

- The risk management function uses a risk management toolkit which can be easily adjusted and adapted to any new risk developments, periods of crisis or emerging risks, e.g. by enhancing the frequency of monitoring tools (RAF, recovery plan indicators) and reporting to the management body, using both backward and forward-looking information and adjusting the respective scenarios.

On the management of risks (including emerging risks):

- In the case of near breaches of risk limits, regular risk management function meetings take place to consolidate all information received, including in coordination also with the compliance function.
- Certain employees are designed as horizontal points of contact for specific risks (e.g. climate) so that these risks are integrated appropriately into the risk management function's working procedures (ECB Guide on climate-related and environmental risks).

On the regular reporting to the risk committee:

- The CRO reports at least on a quarterly basis to the risk committee and the management body. Internal policies clearly define a minimum of what is covered by this internal reporting (e.g. key risk developments, monitoring of the bank's risk profile, developments regarding risk strategy and risk appetite, cases where of the risk management function's objects objection to material decisions), and also leave room to communicate any other key risk issue.
- The CRO immediately informs the chair of the risk committee when a risk limit is breached, also irrespective of the timing of the next risk committee meeting.
- The risk committee (and the audit committee with respect to the outsourcing of the internal audit and/or the compliance functions) is informed at least quarterly on the performance of all critical and important outsourced activities and functions. For non-critical outsourced activities, the reporting takes place at least semi-annually.

The risk management function's involvement in decision-making:

- The CRO is involved in and provides an opinion on the bank's strategy-setting phase (including, digital strategy). Internal control functions are also involved in all phases of the strategy design and roll-out.
- The CRO has the power to veto for certain decisions, e.g. loans decided in the highest credit committee, material investment decisions, setting or changes of limits. Proper appeal or escalation processes (e.g. to the full management body) are properly documented in internal policies and implemented in practice for the final decision.

- The CRO can also escalate, upon discretion, any other case where the decision may entail increased risks. Such veto cases, and their grounds, are documented (e.g. in minutes) and reported regularly to the management body in its supervisory function and/or the risk committee.
- Units within the risk management function that prepare and provide an opinion, veto or vote on in a business decision-making process are segregated from the units responsible for risk control activities with regard to this process.
- If the CRO is not a member of the top risk decision-making bodies, the bank ensures that a procedure is in place to obtain receive their opinion on whether those proposals are consistent with the institution's risk strategy and risk appetite.

4.2.2 Compliance function

It is expected that the compliance function ensures compliance with all applicable regulations and internal policies and proposes and monitors the implementation of measures to avoid, mitigate or remediate cases of non-compliance, including misconduct and money laundering, as applicable.

The compliance function is a key component of a bank's second line of defence to ensure the sound and effective management of compliance risks. Its role is to ensure that banks operate with integrity and comply with applicable laws, regulations and internal policies.[128] In this context, it is expected that the compliance function assesses the possible impact of any changes in the legal or regulatory environment on the institution's activities and compliance framework and to monitor compliance with applicable rules across all organisational units of the credit institution, as well as to remediate cases of non-compliance.[129]

The compliance function is also involved in the approval of new products and processes, providing a systematic prior assessment and opinion. A strong, independent compliance function can steer mitigation of risks related to misconduct, money laundering and other forms of non-compliance. For this purpose, it is necessary to have in place an adequate exchange of information between the business lines and the compliance function (and the AML/CFT compliance function where it is a separate internal control function)[130] both at the group level and between the heads of the internal control functions and the bank's management

[128] See also EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 204-213. It should be noted that ECB Banking Supervision does not have competence or powers in relation to AML/CFT matters. However, it integrates AML/CFT-related matters into its prudential assessment of governance and risk culture. In this context, AML/CFT-related topics will only be covered insofar as they relate to ECB Banking Supervision.

[129] See also EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 209.

[130] If the national law does not prohibit AML/CFT being a separate internal control function.

body.[131] To ensure that the independence of the compliance function is preserved at all times, its independence is expected to be verified periodically.[132]

It is expected that the head of compliance or CCO is independent and has stature within the bank. The ECB therefore recommends that the CCO is dedicated to the role on a full-time basis. As in the case of other heads of internal control functions, the management body reviews the CCO's performance, with the involvement of the head of the relevant management body committee (see also Section 4.1.1.2 above).

It is expected that the compliance function ensures that compliance monitoring is carried out through a structured and well-defined compliance monitoring programme. In addition, it is key that banks develop a well-documented compliance policy and communicate it to all staff.[133] In line with the principle of proportionality, it is expected that the policy is adapted on an individual basis to the specificities of its business, its complexity and the associated risks, also taking into account the group context. At the same time, when identifying and measuring or assessing compliance risks, it is expected that a bank develops appropriate methodologies, including both forward-looking and backward-looking tools. In this context, adequate data quality, aggregation and IT systems allow the aggregation of risk exposures across business lines and support the monitoring and supervision of compliance risks across the group.[134] It is essential that compliance risks are sufficiently and appropriately reflected in the bank's risk appetite statement.[135]

Banks should ensure the ability of the compliance function to assess and report on all relevant compliance risks, including the risks related to restrictive measures and their implications on the bank's business[136]. The ECB is of the view that sufficient harmonisation and integration of compliance processes and methodologies is required within the group (particularly relating to subsidiaries and branches and entities located outside the home country).[137] In particular, it is expected that banks ensure that their subsidiaries and branches take steps to check that their operations are compliant with local laws and regulations in addition to implementing group policies. If local laws and regulations hamper the application of stricter procedures and compliance systems implemented by the group, especially if they prevent the disclosure and exchange of necessary information between entities within the group, subsidiaries and branches should inform the head of compliance or the CCO of the consolidating institution.[138] In this context, it is expected that banks belonging to a

---

131 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 142.

132 See also EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 175.

133 ibid., paragraph 208.

134 See the ECB Guide on effective risk data aggregation and risk reporting, p. 1.

135 See also Section 5 of this Guide.

136 See Consultation paper on draft EBA Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures (EBA/CP/2023/42).

137 Notably, in view of the level of application of the requirements, also on a consolidated level in accordance with Article 109 CRD. See also the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 85.

138 ibid., paragraph 213.

group have in place a central compliance function with a group-wide and holistic view of all compliance risks to which the group is or might be exposed.

The ECB expects that banks formalise and document the division of tasks between the compliance and risk management functions. Although the allocation of responsibilities may vary from one bank to another, some key principles are expected be observed: the two functions remain independent from the business side and have direct access to the management body in its supervisory function; the joint work of both internal control functions ensures comprehensive coverage of all relevant material risks (financial and non-financial risks).

Responsibility for ensuring compliance with all regulations might be shared across several control functions depending on the type of regulation and the financial or non-financial risks. Where such sharing occurs, it is expected that the compliance function, as a minimum, keeps and regularly maintains an overview of applicable regulations, indicating which units are charge of ensuring compliance with them. In this context, close cooperation and regular exchanges of information between the risk management and compliance functions is necessary for the fulfilment of their respective tasks, e.g. with regard to the approval process for new products.

Observed good practices

- The CCO reports on at least a quarterly basis to the relevant committee (e.g. the risk committee or, if established, the compliance committee) and/or management body. The frequency of reporting is increased in the case of larger and more complex banks.
- In order to comply with all applicable sanctions and embargo laws and regulations, and to manage the sanctions compliance risk in an effective and consistent manner, the bank outlines a risk appetite which imposes a minimum standard across the banking group.
- A comprehensive and harmonised risk assessment is discussed at management body level and then implemented across the group.
- Initiatives exist to ensure the digitalisation of compliance processes, including tools for monitoring and supervising compliance risks across the group, such as AI, reducing reliance on manual processes and increasing productivity.
- The second line of defence monitors the remediation of compliance function findings through a group-wide dashboard, which can also be accessed by the management body.
- The group compliance function carries out compliance inspections within subsidiaries.
- The different quantitative metrics used in the risk appetite framework include, among others, the number of regulatory compliance breach incidents, the number of sanctions failures, the number of clients with high or medium AML/CTF risks, the number of customer complaints and the number of high severity compliance findings.

4.2.3 Internal audit function

The ECB expects that banks have in place a fully independent internal audit function responsible for outlining, implementing and monitoring the bank's audit cycle and the audit plan as well as following up on or escalating to the management body any relevant audit findings.

The ECB considers that a strong internal audit function is crucial to ensure that banks have in place robust governance arrangements and adequate internal control mechanisms promoting sound and effective risk management, governance and internal control processes.[139] The internal audit function should, following a risk-based approach, independently review and provide objective assurance of the compliance of all activities and units of a bank, including outsourced activities, with the institution's policies and procedures and with regulatory requirements. Each entity within the group should fall within the scope of the internal audit function.[140] The internal audit function, as the third line of defence, is fully independent of the business lines and units they monitor. In this context, the ECB considers that an appropriate reporting line from the head of the internal audit function to the full management body and relevant committees is key to ensuring independence, as it is the case for all three lines of defence.[141] In addition, a bank's internal audit function is also expected to be subject to periodic independent external assessment.[142]

Turning to the audit cycle, the ECB recommends that there is a clear link between the outcome of risk assessments and the audit plan as regards frequency and depth of audit coverage and that activities and processes are audited at appropriate intervals depending on their risk classification. Thus, the exact duration of the audit cycle depends on the outcome of the risk-based methodology, and it is expected that all relevant activities and risks of the bank – including outsourced activities – are covered within a reasonable timeframe. Overall, it is expected that the audit cycle is not longer than five years, subject to national legal requirements which may impose a different timeframe.

The audit universe is expected to cover the whole spectrum of an institution's activities, including outsourced activities, processes, systems, business and control lines as well as all group entities and branches.[143] In particular, it is essential that banks ensure adequate attention to the RAF (e.g. ensuring that the RAF and its

---

139 The internal audit function is also expected to assess the effectiveness of a bank's internal controls related to AML and sanctions compliance programmes so that gaps or weaknesses can be remediated. While ECB Banking Supervision does not have competence or powers in AML/CFT matters, it takes into account the effectiveness of such internal controls in its assessment of supervised entities' internal governance arrangements.

140 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 216.

141 ibid., paragraph 172. See also Section 4.1.1.1 of this Guide.

142 See the internal audit function in banks, BCBS, June 2012, paragraph 48; and Global Internal Audit Standards, Institute of Internal Auditors, Standard 8.4.

143 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 216.

implementation are regularly audited).[144] In general, it is expected that banks ensure that each audit cycle covers all activities within the audit universe.

It is expected that the internal audits are performed in accordance with an audit plan and a detailed audit programme following a risk-based approach.[145] It is expected that the internal audit plan is based on a robust and properly documented risk assessment (with input from senior management and the management body), approved by the management body after prior input from the audit committee, and updated at least annually to enable an ongoing real-time assessment of where significant risks lie.[146] Any interim changes to the internal audit plan are to be brought to the attention of the management body in its supervisory function and the audit committee (where established). In addition, the internal audit function is expected to consider in its reviews the extent to which the bank is equipped to manage all risks, including, in particular, non-financial (ICT and security risks, including cyber), emerging risks (e.g. climate-related and environmental risks) and geopolitical risks.[147] In this context, the internal audit function needs to adapt to a changing environment.

In addition, the ECB expects the weaknesses identified by supervisors and the respective supervisory findings to feed into the risk assessment performed by the internal audit function as well as its audit plan in order to directly link the overall risk control framework of banks with their vulnerabilities. Furthermore, the ECB expects that the internal audit function has an active, independent role in the monitoring of the implementation of the relevant supervisory measures and their reporting to the management body to ensure informed decision-making.

It is essential that the internal audit function has appropriate stature within the whole bank with a view to having proper follow-up and closure of relevant audit findings, including escalation mechanisms.

- Follow-up, closure and escalation: all audit recommendations are to be subject to a formal follow-up procedure by the appropriate levels of management to ensure and report on their effective and timely resolution following a risk-based approach.[148] It is also expected that a bank's internal policies include proper escalation procedures that preserve the internal audit's stature in the case of high-risk findings, past due findings and disagreements between auditors and auditees.

- The role of the management body in its supervisory function, supported by the audit committee, where established: these oversee and are accountable for the follow-up process, while ultimate responsibility lies with the management body.

144 See also Section 5 of this Guide.

145 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 222. The annual internal audit plan can also be part of a multi-year plan. See The internal audit function in banks, op. cit., paragraph 31.

146 The internal audit function in banks, op. cit., paragraph 31. For further information on the management body's role, see also Section 3.2 of this Guide.

147 See ECB Guide on climate-related and environmental risks, expectation 5.6; EBA Guidelines on ICT and security risk management (EBA/GL/2019/04), paragraph 11.

148 EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 224.

This includes ensuring that senior management is taking necessary corrective actions, in a timely manner, to address findings and recommendations, including past due findings, and deficiencies identified by supervisory authorities.[149]

A sufficient level of resources and appropriately qualified internal audit staff are essential for executing audit plans and missions. it is expected that the qualifications of the internal audit function's staff members and its resources, in particular its auditing tools and risk analysis methods, are adequate for the institution's size and locations, and the nature, scale and complexity of the risks associated with the institution's business model, activities, risk culture and risk appetite.[150] A bank's internal audit function is also expected to retain staff with sufficient knowledge, skills and expertise concerning governance, systems and processes related to ICT and security risks, as well as other emerging risks, such as ESG risks.[151]

In addition, it is key that banks further formalise their internal audit function's rotation processes. The continuous performance of similar tasks may negatively affect an individual internal auditor's capacity for critical judgement owing to a potential loss of objectivity. It is expected that staff rotation within the internal audit function and between the audit function and other areas is expected to be governed by and conducted in accordance with a sound documented policy. It is recommended that the policy is designed to avoid conflicts of interest, including the observance of an appropriate "cooling-off" period between an individual's return to the internal audit function and participation in the audit of activities in which the individual has been involved.[152]

In cases where the internal audit function provides advisory or consulting services for certain strategic projects, its independence as the third line of defence is expected to be preserved. It is expected that specific mitigations are in place, including, but not limited to: (i) a clear definition of the scope of the function's advisory services in the audit charter and internal policies; (ii) the establishment of distinct auditing and advising roles; and (iii) non-participation in direct management functions, such as voting in project committees.

Observed good practices

On the audit plan and cycle:

- The audit plan acknowledges that resources may be needed for ad hoc reviews because of unexpected events, and sufficient spare capacity is readily available.

[149] The internal audit function in banks, op. cit., Annex 2(z)-(bb). For further information on the management body, see Section 3 of this Guide.

[150] EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 214.

[151] EBA Guidelines on ICT and security risk management, paragraph 25.

[152] The internal audit function in banks, op. cit., paragraph 15.

- The audit plan takes into account supervisory authorities' findings (i.e. SREP recommendations).

On the process of following-up on internal audit findings:

- During audit fieldwork, as soon as a potential finding becomes clear to the internal audit function, this is shared and discussed with the auditee, which allows timely remediation.
- Audit reports elaborate on root causes of findings, provide clear recommendations with clear deadlines to rectify findings, indicate the area(s) responsible for remediation and contain closure criteria.
- Any delays in the implementation of remedial actions, including their root cause, and any high-risk findings, "risk accepted" findings and recommendations are presented to the audit committee by the respective unit. This process is also reflected in the bank's internal policies.
- KPIs regarding timely implementation of audit findings and the respective backlog are used in the assessment of the performance and effectiveness of the audited areas.
- Extensions of deadlines attached to internal audit recommendations are only approved by the internal audit function in exceptional cases and reported for information and discussion to the senior manager and the management body in its supervisory function.
- When findings have an impact on controls, internal control functions are involved in the follow-up process by receiving the audit reports and being invited to the meetings with auditees.
- Periodic review of all findings by internal audit to identify cultural root causes.

On the stature of internal audit function during the issuing of reports and findings:

- In the case of discarded findings or changed deadlines or where further supporting documentation is requested, the approval of the head of the internal audit function is required.
- In the case of disagreement between the business area and the internal audit function, the internal audit assessment and rating prevails, while the disagreement is noted in the report.

5 Risk appetite framework

The ECB considers a well-developed RAF, articulated through the risk appetite statement, to be a cornerstone of a sound governance framework, alongside a strong risk culture and well-defined responsibilities for the risk management and control functions.[153] It is expected that the RAF is fully incorporated and documented as part of a bank's decision-making process, including being used in strategic decisions and in connection with the bank's strategic processes, such as those related to the internal liquidity adequacy assessment process (ILAAP), the internal capital adequacy assessment process (ICAAP), budget and remuneration.[154]

5.1 Designing a RAF

Even if a bank's RAF is composed of a set of existing risk policies, the ECB is of the view that a bank should formalise a summary statement to ensure consistency in its risk management procedural framework so that the management body obtains a holistic view of the bank's risks.[155] It is expected that the management body is adequately involved and plays a key role in setting and approving the RAF. Members of the management body oversee its regular review and its proper implementation and challenge whether it is taking place in compliance with the bank's policy and strategy.[156] In addition, it is expected that the RAF documentation describes the responsibilities of all stakeholders involved in accordance with the organisation of the bank. It is expected that the RAF is aligned with other strategic processes, such as the budget, ICAAP, ILAAP, recovery plan and remuneration framework, and this interplay is expected to be formalised.

It is expected that the management body of the bank, which is responsible for validating the RAF in the first place, is regularly updated about the bank's risk profile relative to its risk appetite in order to be in a position to take appropriate decisions.[157] Specifically, it is expected that banks develop internal monitoring, such as an aggregated and consolidated risk appetite dashboard, comparing the risk exposure and risk limits to the appetite for both financial and non-financial risks.[158] The ECB is of the view that this dashboard should be presented to and discussed by the management body in its supervisory and management functions and by the specialised management body committees (e.g. the risk committee and the audit

---

153 See FSB Principles for An Effective Risk Appetite Framework.

154 See also EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing under Directive 2013/36/EU (EBA/GL/2022/03), Section 5.7.

155 For further information on the risk appetite statement, see also the FSB Principles for An Effective Risk Appetite Framework, pages 5-6.

156 In line with Article 76 and Article 88(1) CRD.

157 See EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraphs 22(b), 34(e) and 71; and EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing under Directive 2013/36/EU (EBA/GL/2022/03), paragraph 115(a).

158 See also the ECB Guide on effective risk data aggregation and risk reporting.

committee, where applicable) on a regular basis. The ECB considers that at least a quarterly frequency is a good practice for larger institutions, to support the review, oversight and monitoring of the risk profile of the bank.[159]

5.1.1 Scope

The ECB expects that the scope of the risks included in the RAF is comprehensive, including both financial and non-financial risks and corresponding metrics.

In order to ensure sound and effective risk management, it is expected that the risks included in the RAF reflect the outcome of the regular risk identification exercise carried out by the institution (the ECB has observed that in practice this is usually done on an annual basis). It is expected that banks reflect the material risks of the business model of the institution, which in most cases would include, at least, business risk and profitability, capital risk, liquidity risk, interest rate risk in the banking book, credit risk, market risk, operational risk, non-financial risks, etc.[160] It is expected that material non-financial risks (in particular compliance risk, reputational risk, IT risk, legal risk) as well as other emerging risks, such as climate-related and environmental risks, and geopolitical risks, are included explicitly in the RAF.[161] It is expected that banks understand, monitor and assess these risks and their potential financial impact, using qualitative and/or quantitative indicators at sufficient granularity also with a forward-looking perspective (taking also into account the impact of second round effects on the business model, profitability, liquidity and capital position of the bank). It is also recommended that the RAF addresses risks that are more difficult to quantify, such as reputational, conduct risks, risks associated with tax offences, risks of non-compliance with restrictive measures and of circumvention of sanctions[162], as well as money laundering and terrorist financing and unethical practices, in order to ensure sound and effective risk management.[163]

Once the various risks have been identified, it is essential that banks define corresponding metrics. It is recommended that metrics presented to the management body reflect the business model, size and complexity of the institution. It is expected that any changes and developments in the business model and strategy of the institution are properly reflected in the RAF by covering all financial and non-financial risks pertinent to any such new activities (e.g. digital transformation, crypto-assets, etc.). As part of this, the ECB recommends that, where

---

159 Regarding the bank's responsibility for an appropriate risk appetite framework/statement, see also the FSB Principles for An Effective Risk Appetite Framework, page 1.

160 See also EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing under Directive 2013/36/EU (EBA/GL/2022/03), paragraph 115(b).

161 On risk appetite expectations and good practices relating to climate risk, see also of the ECB Guide on climate-related and environmental risks, Chapter 5.2, and Good practices for climate-related and environmental risk management, ECB Banking Supervision, November 2022.

162 See Consultation paper on draft EBA Guidelines on internal policies, procedures and controls to ensure the implementation of Union and national restrictive measures (EBA/CP/2023/42).

163 See FSB Principles for An Effective Risk Appetite Framework, page 6, including the example in footnote 9.

relevant, the bank assesses whether the RAF defines risks pertinent to crypto-assets (both financial and non-financial) and sets out risk indicators and corresponding risk appetite thresholds/limits. In addition, it is recommended that there is a proper balance between static metrics and forward-looking ones, including results of stress tests.

Last, but not least, it is recommended that the number of metrics presented to the management body is appropriate, meaning there is a sufficient number of metrics to cover all the risk dimensions and to properly capture the complexity of the business model of the institution. It is expected that this number will not be too high to ensure the clarity of the dashboard and the proper steering of risks which are more significant in terms of capital absorption. Although the total number of metrics reported to the management body may vary depending on the business model, risk profile and complexity of the bank, a very high or a very low number may not allow meaningful discussions within management body.

5.1.2 Limits

The ECB is of the view that 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 bank can assume, with a clearly defined escalation process in the event of a limit breach.

It is recommended that risk appetite limits are adapted to the risk profile of the group and set such that they would be hit before any regulatory requirement is breached.[164] It is expected that risk limits are set at an adequate level and not so high that there is no real possibility of breaching them. In addition, the ECB recommends that the risk limits are not adjusted too often in order to avoid breaches.

It is expected that risk appetite limits establish the level and types of risk that the bank is willing to assume in advance of its business activities in order to conduct them within its risk capacity. It is also recommended that the banks define and implement a process for regularly monitoring and reviewing their risk appetite limits, including an escalation process in the event of limit breaches, clarifying the roles of the various stakeholders.[165] Limits may be recalibrated outside of the regular review cycle on an exceptional basis (when required by specific circumstances, e.g. in the case of a change in a bank's business activity), but it is recommended that this is still discussed and approved by the relevant management body, and that it is always aligned with prudent management of risks. In any case, it is essential that institutions have effective management information systems to be able to report any limit breach adequately and in a timely manner. If limits are breached, it is expected that internal control functions ensure that breaches are properly handled and that corrective actions are taken.[166] In the case of a breach, there is expected to be an action plan

[164] For further information on risk limits, see also the FSB Principles for An Effective Risk Appetite Framework, pages 6-7.

[165] ibid. See also pages 7-12 on the roles and responsibilities of different stakeholders.

[166] Ultimate overall responsibility for risk lies with the management body in accordance with Article 76(3) CRD.

with clear objectives, timelines and responsibilities on how to react to the breach, including a clear process to monitor the execution of the action plan.

The RAF has also proven to be a strong tool for ensuring enhanced risk monitoring in periods of crisis. In particular, banks that have an adequate RAF in place, are able to manage their risks and are better prepared to face a variety of adverse circumstances, as their risk appetite is subject to closer scrutiny and control at all levels of the organisation. At all times, and particularly in times of crisis, it is expected that banks ensure that the RAF is sufficiently well defined (in terms of indicators and limits) to allow, when necessary, monitoring that is more frequent than normal with appropriate escalation processes that allow timely reporting of any limit breaches.

Observed good practices

- The management body in its supervisory function, supported by its committees, engages in robust inquiry into the causes and consequences of material or persistent breaches of risk appetite and risk limits.
- The appropriate number of metrics presented to the management body is assessed relative to the complexity of the risks (e.g. ranging from 20 to 40, or more, subject to the complexity of the risks, and depending on the bank's size, business model and overall complexity).
- On metrics to measure non-financial and/or emerging risks, these include, e.g. in the case of climate-related and environmental risks, quantitative metrics for physical and transition risks (see also Chapter 5.2. of the ECB Guide on climate-related and environmental risks).
- Banks allocate limits to business lines as well as to per the bank's entities and countries, and these local limits are consistent with the limits at consolidated level.
- Metrics capture the downside risk for the bank as a whole, such as stressed losses, which can then be allocated to businesses, risks and legal entities.

5.2 Implementation of the RAF

5.2.1 RAF, strategy and risk culture

The ECB expects that the RAF is used to guide risk awareness and prudent risk-taking in order to contribute to a bank's sound risk culture. The ECB recommends that the RAF remains stable over time and is used as a driver of the bank's strategy, rather than the strategy dictating the RAF.

ECB Banking Supervision considers the establishment of an effective RAF, with an underlying risk appetite statement, as a strategic tool to reinforce a strong risk culture in banks, which in turn is critical for sound risk management.[167]

It is expected that banks ensure that risk appetite statements remain fairly stable across time and are used as drivers of the strategy of the institution, rather than the strategy dictating the risk appetite. It is expected that risk appetite statements outline all levels and types of risk that the bank is willing to assume within its risk capacity to achieve its strategic objectives and business plan. Therefore, the risk appetite statements govern the annual limit setting (in line with Section 5.1.2 of this Guide), with due consideration given to economic cycles and financial volatility, ensuring that at all times there is sufficient headroom to risk appetite thresholds if a limit is breached, consistent with the bank's overall risk appetite. This will facilitate the taking of corrective steps to remain within the overall risk appetite.

It is expected that the RAF allows for flexibility in order to respond to emerging risks, e.g. risks coming from environmental changes and at times of crisis. However, it is crucial that the risk appetite statements are also definitive and consistent enough to avoid strategic drift.[168] In view of this, it is not expected that a bank's RAF functions on a standalone basis but is rather part of a bank's strategic decision-making, including its long-term planning.

Furthermore, it is recommended that RAFs are used to guide behaviour towards risk awareness. In particular, it is essential that variable remuneration is linked to and conditional on some risk factors, both ex ante and ex post:

- Ex ante adjustments: This includes key risk-related performance indicators used as an input to calculate variable remuneration.[169] Ex ante adjustments are carried out via the bonus pool setting, which takes into account all the risks the bank is and could be exposed to cascaded down to business unit objectives and individual KPIs, which it is recommended should be linked to the RAF.[170] Both quantitative and qualitative criteria should be used, including financial and non-financial metrics, in order to reflect a sustainable and risk-adjusted performance. In this context, the ECB recommends, as best practice, that KPIs cover the remediation of audit and supervisory findings (e.g. stemming from the SREP, on-site inspections, etc.), especially for the management body members responsible for the proper remediation of those findings.

---

167 See also EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), Title IV, Part 9; and FSB Principles for An Effective Risk Appetite Framework.

168 Observations on Developments in Risk Appetite Frameworks and IT Infrastructure, Senior Supervisors Group, December 2010, p. 5.

169 In line with the EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04), paragraph 45 under "Background and rationale", ex ante risk adjustments are applied when the remuneration is awarded to take into account current and future risks and have an immediate effect on the variable remuneration awarded and on risk-taking behaviour.

170 In line with the definition in the EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04), "bonus pool" means the maximum amount of variable remuneration which can be awarded in the award process set at the level of the institution or an institution's business unit. See also Section 14.2.1 of those guidelines.

- Ex post adjustments and consequence management: With respect to ex post adjustments, it is expected that “malus” or “clawback” provisions are used in the event of non-compliance with key risk indicators.[171] In addition, the ECB expects that an effective consequence management framework, including a disciplinary process and sanctions, is in place to address cases of misconduct and inappropriate risk-taking behaviour and to ensure individual accountability for risks as well as remediation of audit and supervisory findings.

It is expected that banks put in place a clear linkage between the remuneration framework and the RAF to ensure that continuous long-standing non-compliance with the RAF has consequences for performance assessments and variable remuneration. It is also essential to strengthen the link between risk and remuneration, improving the implementation of risk indicators in the calculation of remuneration, the transparency of the remuneration system and its ability to be understood by the employees.[172]

In this context, the implementation of the RAF is a key component of a sound risk culture. For this reason, it is expected to form an inherent part of the internal processes for the banks’ employees. In order to ensure that this is the case, it is expected that banks put their risk strategy and risk appetite statement in writing and communicate them to the staff of the institution through a formal process in order to explain to them how their job affects the risk appetite of the bank.[173] This would heighten employees’ awareness on risk matters and give them a greater incentive to undertake prudent risk-taking and risk management in order to facilitate the sound risk culture of the bank.

5.2.2 Governance and deployment

The ECB expects that, as part of the overall corporate governance framework, the three lines of defence and management bodies should play an active role in the definition of the RAF and its monitoring and deployment across business lines and entities.

The ECB considers it essential that the RAF is supported by a strong governance framework, with clear roles for all the stakeholders involved at all levels of the bank (management body, senior management, internal control functions, business lines, legal entities, etc.). The independent review and assessment of the RAF should also be clearly allocated and described, taking into account the organisational structure and independence across the three lines of defence. It is also expected that risk appetite statements are to be used to promote robust discussions on risk and

---

171 In line with the EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04), paragraph 46, ex post risk adjustment should ensure that staff are rewarded in line with the sustainability of the performance in the long term, which is the result of decisions taken in the past. For definitions of “malus” and “clawback”, see the list of definitions in the EBA Guidelines on sound remuneration policies under Directive 2013/36/EU (EBA/GL/2021/04), page 23.

172 In line with Article 94 CRD.

173 See EBA Guidelines on common procedures and methodologies for the supervisory review and evaluation process (SREP) and supervisory stress testing under Directive 2013/36/EU (EBA/GL/2022/03), paragraph 115(f).

strategic issues, not only with the management body but also with the internal control functions.

In particular, it is expected that the management body in its supervisory function, with the support of the risk committee, plays an active role in overseeing the consistent implementation of the RAF, its alignment with the business strategy and objectives, and the escalation of breaches.[174] Where the management body in either its supervisory function or its management function is not directly involved in the approval of the specific metrics and limits of the RAF, it is expected to have, at least, the opportunity to challenge and review the specific metrics and limits, via the risk committee (or equivalent committee), on the basis of information on the bank's risk situation, having itself determined the nature, amount, format and frequency of such information.

It is expected that banks' internal control functions help to develop and monitor the implementation of the RAF, checking whether the risk limits imposed on specific business activities or on specific risks are appropriate.[175] The ECB expects that an independent review of the RAF is performed regularly by the internal audit function to assess its effectiveness.[176] Banks which perform such reviews generally do so on an annual basis, including an assessment of the overall framework and of the adequacy of the identification, escalation and reporting of limit breaches.

It is also expected that the RAF is deployed within banks. This means that risk appetite statements are established for business lines and entities in order to ensure that their strategy and risk limits, where relevant, align with the bank-wide risk appetite statement.

Furthermore, in order to facilitate risk monitoring at consolidated or sub-consolidated levels, it is also expected that banks develop risk appetite dashboards for material business lines and entities, derived from the approach developed at group level.

Observed good practices

- The bank's internal policies require an opinion of the management body in its supervisory function and the risk committee as a prerequisite for the final approval of the RAF.
- The RAF is used as a basis for discussions between senior management, the various business units, the departments responsible for risk management, and the subsidiaries of the institution (e.g. on topics related to budget).
- Alignment of metrics and limits used for variable remuneration purposes with respective risk appetite metrics and limits, and adherence to the RAF being considered in the setting of the bonus pool setting (e.g. as part of gateway clauses).

174 On the management body's oversight role, see also Section 3 of this Guide.

175 On the risk management function, see also Section 4 of this Guide and the EBA Guidelines on internal governance under Directive 2013/36/EU (EBA/GL/2021/05), paragraph 187.

176 EBA Guidelines on internal governance under Directive 2013/36/EU, paragraphs 81 and 218(b).

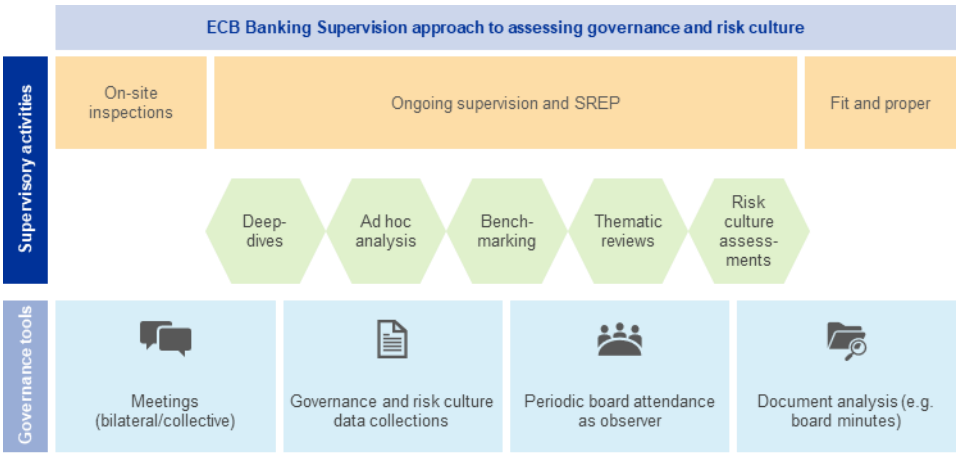
- Banks use risk appetite limits as a tool to monitor their risk profiles, keep risks in check and set the right incentives for the whole of the organisation.
- Defined early warning signals, enabling the bank to detect deteriorations in its risk profile even before risk limits are actually breached.
- A sound infrastructure for risk data aggregation to ensure monitoring of breaches.
- The tone from the top is adequately permeated cascaded throughout the bank in order to promote sound risk-taking in line with the RAF. The management body and the senior management define values and set expectations for the bank's risk culture. The management body in particular challenges the senior management and thereby so ensures that each strategic decision is based on a sound risk analysis, in line with the bank's risk appetite.
- There are training programmes on risk appetite, including exams and certification, through which the management is able to monitor the employees' understanding of RAF and the organisation's risk culture.
- Third- party risks are included in the RAF and resulting in adjusted risk tolerance in consumer credit and distribution channels.

6 Supervisory approach

In line with the SSM Regulation and the SSM Framework Regulation, ECB Banking Supervision uses different supervisory tools to ensure a holistic approach when carrying out its supervisory activities. These supervisory tools include both offsite and on-site supervision of governance and risk culture components.[177]

The ECB Banking Supervision uses a holistic approach to assess governance and risk culture components as well as a wide range of tools.

Figure 7
ECB Banking Supervision supervisory activities and governance tools



In the course of ongoing supervision, the supervisory tools include the assessment of management body members, individually and as a whole, and key function holders via fit and proper assessments, the ongoing assessment by Joint Supervisory Teams (JSTs) of a bank's governance documentation (e.g. group policies, by-laws, governance manuals, code of conduct, risk and remuneration policies, management body documents and minutes), as well as interviews, meetings, including bilateral meetings, and the periodic attendance of JSTs as observers at management body meetings.[178] The JST's findings from ongoing supervision feed into the ECB's annual SREP and might also be included in fit and proper assessments whenever there is a link to suitability criteria.[179]

On-site inspections provide a complementary tool to assess governance and risk culture deficiencies identified in the course of ongoing supervision.[180] Specific deep dives, including on behaviour and culture, on individual banks are also carried out on the basis of idiosyncratic risks. In the case of non-compliance with prudential

177 For more information, see the Supervisory Manual, ECB Banking Supervision, January 2024.
178 For further information, see the ECB Guide to fit and proper assessments.
179 For more information, see the ECB webpage on the supervisory methodology of the SREP.
180 For further information, see the ECB Guide to on-site inspections and internal model investigations.

requirements (or with supervisory measures adopted in an ECB decision), the escalation process may include the activation of supervisory powers, as well as the imposition of administrative penalties and, if the suitability of members of the management body might also be deemed to be affected, the triggering of fit and proper re-assessments.[181]

ECB Banking Supervision also performs thematic reviews and targeted analyses related to internal governance following its supervisory priorities, as well as other ad hoc assessments. These analyses provide a peer perspective, benchmarking and examples of observed good practices.

Governance and risk culture dimensions manifest themselves in different ways across a bank. The ECB assesses governance and risk culture from different perspectives, connecting the dots across different areas of ongoing on-site and offsite supervision to identify potential risks. In summary, supervisors, gather insights via different channels in order to construct a holistic picture. In this regard, supervisors use different supervisory tools and sources of information to provide banks with additional insights and peer perspectives on the different risk culture dimensions, including behavioural patterns of the bank. In the case of deficiencies, the ECB will use all measures in the supervisory toolkit and, if needed, step up the supervisory escalation to ensure timely alignment with the applicable requirements, as interpreted in the ECB's supervisory expectations set out in this Guide.

ECB Banking Supervision will continue to develop its supervisory approach towards addressing governance and risk culture-related risks over time, taking into account regulatory developments as well as evolving practices in the industry and in the supervisory community.

[181] For further information on administrative penalties, see the ECB Guide to the method of setting administrative pecuniary penalties pursuant to Article 18(1) and (7) of Council Regulation (EU) No 1024/2013.

Annex
Changes versus the supervisory statement on governance and risk appetite of 2016

Main changes in the Guide versus the 2016 supervisory statement on governance and risk appetite[182]

- Building on the 2016 statement, inclusion of more detailed chapters on a wider range and number of topics. Heightened focus on the topic of risk culture, including the link with remuneration and accountability as well as behavioural aspects.
- Part on risk culture, internal control functions and SSM supervisory tools now included – no dedicated sections on these topics in the supervisory statement of 2016.
- Enhancement of the 2016 statement's substance, with clearer supervisory expectations and a list of observed good practices per topic based on supervisory experience.
- Reflection of more recent ECB publications as well as updated CRD provisions, EBA Guidelines and international standards.

182 SSM supervisory statement on governance and risk appetite, ECB Banking Supervision, June 2016.

Postal address 60640 Frankfurt am Main, Germany
Telephone +49 69 1344 0
Website www.bankingsupervision.europa.eu

For specific terminology please refer to the SSM glossary (available in English only).