



Technical note on
**Guide on governance
and risk culture**

ECB - Draft version

- 
1. General overview
 2. Importance of governance and risk culture for banks
 3. Functioning and effectiveness of the management bodies
 4. Internal control functions
 5. Risk appetite framework
 6. Supervisory approach
 7. Why Management Solutions?

1

General overview Executive summary

The new ECB's Guide on Governance and Risk Culture will help to address one of the prioritized vulnerabilities for 2024-2026 by the Supervisor, complementing 2021 EBA GL on internal governance



Context

- In **June 2016**, the ECB published the **SSM supervisory statement on governance and risk appetite** as part of the ongoing efforts of the SSM to enhance the governance frameworks of significant financial institutions in the euro area. In **July 2021**, the EBA published the **GL on internal governance**.
- In addition, in **Supervisory Priorities for 2024-2026** the ECB identified as a prioritized vulnerability the need of addressing the deficiencies in management bodies' functioning and steering capabilities (Priority 2).
- In this context, the ECB has published the **Draft Guide on Governance and Risk Culture** aimed at enhancing the governance structures and risk cultures within banks operating in the EU. The Guidance replaces the 2016 SSM Statement on Governance and Risk Appetite and complements the 2021 EBA GL on internal governance.



Objective

- Setting out key **ECB supervisory expectations** when assessing the **governance and risk culture** of supervised banks based on the ECB's interpretation of the current regulatory framework.
- Guiding banks towards a **more effective internal governance and risk culture**, taking into consideration their own governance arrangements, culture and behavioural patterns.



Next Steps

- The public consultation on the Governance and Risk Culture Guide ends on **October 16, 2024**.
- Subsequently, the ECB will publish the comments received, together with a feedback statement and the final version of the Guide.

Main content



Importance of Governance and risk culture

- Defining culture, including their values and code of conduct, as well as measuring adherence
- MB must regularly discuss the bank's culture, ensuring that it is aligned with prudent risk-taking

Functioning and effectiveness of the MB

- Role
- Structure
- Composition and related policies
- Functioning and effectiveness
- Relevant committees

Internal control functions

- Banks to identify, monitor and report risks and adequate internal control mechanisms are based on a three lines of defense model

Risk Appetite Framework

- RAF should be integrated and documented within a bank's decision-making processes, including strategic decisions and key strategic processes

Supervisory approach

- Holistic approach, using a range of supervisory tools and techniques, to assess governance and risk culture in banks, including ongoing supervision, on-site inspections, and thematic reviews



2 Importance of Governance and risk culture for banks

Main aspects



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

A strong governance framework...

... is grounded on the **suitability of MB members and key function holders** to carry out their roles.

... provide MB 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.

Risk culture dimensions...

... must be considered in order to have a **holistic view of potential areas of attention** related to institution's governance:

- **Tone from the top** and leadership
- Culture of **effective communication and challenge**
- Ensuring **accountability**: robust escalation and whistleblowing processes.
- Aligning **incentives** with the institution's risk culture and values.

Importance of risk culture

- Own **culture, values, and code of conduct** ensure that all actions and decisions align with the bank's core principles.
- The MB should **regularly discuss** the bank's culture to ensure it aligns with prudent risk-taking.
- **Monitoring and measuring adherence to risk culture** ensures that the stated values are reflected in the actions of both management and employees.
- Effective tools should be in place to **mitigate culture risk**. Regular reporting and discussion of these findings are crucial.
- The MB and senior management should define and communicate **desired behaviors** in line with the bank's values and act as **role models**.
- The way a bank defines its culture plays a key role in ensuring **prudent risk-taking and risk management**. Governance arrangements, culture, and behaviors should be aligned with prudent risk-taking, supported by concrete actions.
- Banks should **communicate** their aspired risk culture to all staff via multiple channels, including mission statements, values, and lessons learned.
- The **remuneration framework** should promote desired behaviors aligned with the long-term interests and risk profile of the bank. This discourages excessive risk-taking and ensures accountability for risks across the bank.
- Relevant **digital transformation** initiatives should be in place and regularly updated to ensure effective processes.
- Internal policies should ensure a **clear allocation of tasks and responsibilities** across different functions, at all levels, and across the three lines of defense. This ensures accountability and a transparent
- The ECB has identified **governance and behavioral/cultural red flags** as early warning signals of potential issues. These need to be assessed holistically and on a case-by-case basis to address any deficiencies effectively.

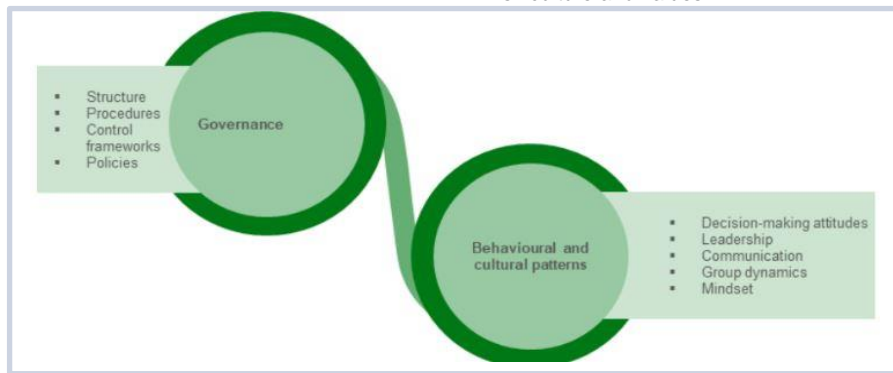
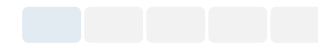


Figure 1: Link between risk culture components

2 | Importance of Governance and risk culture for banks

Red flags

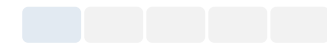


The ECB has identified a number of governance and behavioural/cultural red flags¹ that need to be assessed in a holistic and case-by-case manner, as any deficiency may not be due to risk culture or to risk culture alone

Dimension	Governance red flags	Behavioural and cultural red flags
Tone from the top and leadership	<ul style="list-style-type: none"> • Insufficient MB oversight of internal control functions and the MB in its management function • Low number of formally independent members • Insufficient subsidiary oversight • Inadequate escalation and consequence management framework • Inadequate conflict of interest policy and ethics framework 	<ul style="list-style-type: none"> • Insufficient ownership of and responsibility for conduct risk. • Unsatisfactory promotion of good behaviors among staff • Dismissive attitude among staff towards compliance, regulation and supervision • Inadequate tone from the top on the balance of risk and rewards • Concentration of power in a few members of the management • Unethical behaviors not sufficiently sanctioned by the bank
Culture of effective communication and challenge and diversity	<ul style="list-style-type: none"> • Deficiencies in the whistleblowing process • Governance arrangements, including, committee structure and escalation process not facilitating debate • Inadequate diversity framework. 	<ul style="list-style-type: none"> • Lack of challenge and debate within the MB • Insufficient challenge to the main variable remuneration assumptions • Insufficient challenge from and independence of internal control functions • A culture of fear leading to an unwillingness to report mistakes, risk breaches or material concerns • Lack of diversity (skills, gender, background) • Lack of meetings and training to raise awareness and promote proper risk culture and conduct
Incentives	<ul style="list-style-type: none"> • Documentation underpinning the variable remuneration framework • Lack of interplay between strategy and risk appetite • Lack of link between variable remuneration framework and RAF • Impaired consequence management (e.g. malus and clawback clauses exist only as a formality) • Lack of individual accountability 	<ul style="list-style-type: none"> • Incentive system does not incentivise desired behaviours • Promotion process does not reflect conduct, ethics and behaviour • Applied metrics and limits not commensurate with risk profile and appetite • Imbalanced deployment of financial performance criteria versus non-financial criteria • Wrong incentives, e.g. remuneration of the CRO linked predominately to commercial objectives
Accountability	<ul style="list-style-type: none"> • Low stature and understaffing of internal control functions • RAF not comprehensive or well implemented • Weak IT and data aggregation framework • Lack of a comprehensive “lessons learned” process to identify and address similar risks 	<ul style="list-style-type: none"> • Unbalanced application of the third line of defense • Insufficient transparency in reporting • Risk management seen as a barrier to achieving business objectives

2 | Importance of Governance and risk culture for banks

Observed good practices



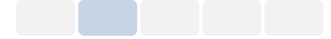
The Guide includes some observed good practices in relation to the importance of governance and risk culture for banks

Dimension	Observed good practices
Tone from the top and leadership	<ul style="list-style-type: none"> Promoting the adoption of risk-conscious behaviors (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 banks speak-up policy.
Incentives	<ul style="list-style-type: none"> The bank rewards and encourages appropriate risk-taking behavior via financial incentives. KPIs for all MB members and senior management include risk and control-related objectives that are appropriately weighted in the overall assessment of performance. Strong link between the RAF and the remuneration framework. KPIs focus on different stakeholders, including, employees, customers, regulators as well as shareholders.
Accountability	<ul style="list-style-type: none"> Implementation of 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. 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 MB 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 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 defense 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.

3

Functioning and effectiveness of the MB

Main aspects



The ECB provides its expectations on MB's role, structure, composition and related policies, functioning and effectiveness

Role and structure of MB



- The MB has ultimate and overall **responsibility** for the **institution** and defines, oversees and is accountable for the **implementation of the governance arrangements** to ensure effective and prudent management. It is expected that the MB in its **supervisory function** demonstrates a **capacity** for **constructive challenge** and **strong oversight** of the **management** and **internal control functions**.
- **Individual statements** outlining roles and duties shall be in place and available for supervisory authorities.
- MB are expected to use committees to delegate specific topics, with clear definitions of structure and mandates. Significant institutions must establish **audit, risk, nomination, and remuneration committees**, while smaller institutions may combine risk and audit committees if allowed by authorities

MB composition



- The **size** of the **MB** must be **appropriate** to allow it to effectively carry out its oversight role and other responsibilities. In this context, the MB needs to possess **adequate collective knowledge, diversity of skills and experiences** to be able to understand the institution's activities, including the main risks.
- The ECB, following EBA GL, recommends MB in its supervisory function to include a **sufficient number of formally independent members** to enhance **checks and balances** and **facilitate effective oversight of management decision-making**. Banks must manage potential conflicts of interest, distinguishing between formal independence and independence of mind. The ECB will assess independence on a case-by-case basis.
- The **chair of the MB** should be a **non-executive, preferably independent**, to foster a culture of challenge and debate. The chair should not simultaneously be the CEO to avoid conflicts of interest.
- Specific committees, like the **risk and audit committees**, should have a **majority of independent members and independent chairs**.

Functioning and effectiveness of MB



- In its supervisory function, the MB must **ensure members prepare thoroughly for meetings and dedicate sufficient time to discussions** and oversight.
- MB members should play an **active role in setting meeting agendas**.
- **Effective interaction between the MB and its committees** will reduce information asymmetries and ensure strong oversight, with periodic reports and access to committee discussions.
- Documentation for the MB and committees should be clear, contain the right balance of comprehensiveness and conciseness, and shared in advance, enabling **meaningful discussions and proper record-keeping of deliberations** and decisions.

Policies concerning the composition of MB

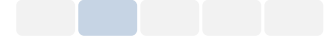


- **Suitability policies** must accurately reflect fit and proper criteria, detailing assessment methods, roles, responsibilities, and a transparent selection process for MB members and key function holders.
- **Diversity policies** should promote various aspects of diversity (e.g. educational and professional background, gender, age, and geographical provenance), and set gender targets at the management body level.
- **Succession planning processes** should include principles for selection, monitoring, and re-appointment of members, and mechanisms to mitigate potential negative effects of simultaneous departures.

3

Functioning and effectiveness of the management bodies

Observed good practices

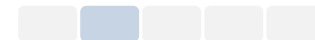


There are some observed good practices for functioning and effectiveness of the management bodies

Risk Culture Dimension		Observed good practices
MB composition	Collective suitability and diversity	<ul style="list-style-type: none"> When using the EBA suitability matrix, the questionnaires contain an objective assessment performed by the nomination committee. Clear guidance on suitability criteria (e.g. soft skills and time commitment), taking into account industry standards and available benchmarks. The MB appoints members with specific expertise 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". MB, as ultimately responsible decision-makers for the nomination process, are provided with full documentation of decision-preparers. External parties are involved at least every three years when performing MB self-assessments. When searching for candidates, institutions consult external service providers in order to have a larger pool of candidates available. A bank's diversity policy covers the entire organisation and is not limited to the MB.
MB Functioning and effectiveness	Organisation of the MB in its supervisory function	<ul style="list-style-type: none"> Assigning specific subjects to individual non-executive members ahead its meetings to facilitate the discussion. Gathering insights from the bank's different business areas (e.g., by meeting with lower-level executives and heads of internal control functions). Collecting views from outside the institution about the external environment and about the institution itself. Systematically discussing the consequences of possible decisions on strategic topics in terms of risks (e.g., budget process, IT projects). The bank appoints members with specific expertise/national backgrounds on the basis of the institution's risk profile and future development. Continuous training sessions divided into a general and a tailor-made part (based on expertise matrix), given by external providers and members of the management function. Induction programs for new members. Group-wide crisis committee established with the participation of senior and all relevant units. Clear indication of roles and responsibilities of executive and non-executive members of the MB.
	Interaction between the MB and its committees	<ul style="list-style-type: none"> One-to-one meetings between the committee chairperson and heads of internal control functions (e.g. resources, regular reporting). Clear internal rules stating that members of the MB shall be present in committee meetings for certain agenda items and upon invitation. MB agendas differentiate clearly between open committee sessions 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. The committee chair informs the whole MB 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 MB 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. Cross-participation: a member of the risk committee participates in the meetings of other committees. 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.

3 | Functioning and effectiveness of the management bodies

Observed good practices



There are some observed good practices for functioning and effectiveness of the management bodies

Risk Culture Dimension		Observed good practices
MB Functioning and effectiveness (cont.)	Nomination Committee	<ul style="list-style-type: none"> • Discussing the scrutiny of candidates during the nomination committee meetings, As part of the selection process. • 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	<ul style="list-style-type: none"> • Making concrete recommendations on executives' scorecards, e.g., recommended differentiation of the weight of KPIs for different executives. • Proposing review of KPIs for executives who have significantly changed their roles during a year.
	Audit Committee	<ul style="list-style-type: none"> • Being 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	<ul style="list-style-type: none"> • Meeting regularly and frequently, at least quarterly (for G-SIIs global systemically important banks around 11 times per year).

3

Functioning and effectiveness of the management bodies Observed good practices



There are some observed good practices for functioning and effectiveness of the management bodies

Risk Culture Dimension		Observed good practices
Functioning and effectiveness of management bodies	MB and committee documentation	<ul style="list-style-type: none"> • There is a process of agenda setting throughout the whole year 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, 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.
Policies concerning the composition and functioning of management bodies	Suitability policies	<ul style="list-style-type: none"> • 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 MB members as well as training needs. • Policies are publicly available (e.g., via the bank's website).
	Diversity policies	<ul style="list-style-type: none"> • Banks perform statistical analyses to understand the representation of gender and different age ranges in the bank. • Banks monitor the underrepresented gender within the MB and with respect to promotions and salary increases. • Banks seek to appoint a diversity manager and/or gender balance expert to the nomination committee. • 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
	Succession planning	<ul style="list-style-type: none"> • Banks identify the profile of possible future candidates in advance and maintain lists of internal successors which are reviewed and updated at least annually. • 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 MB leave at the same time.

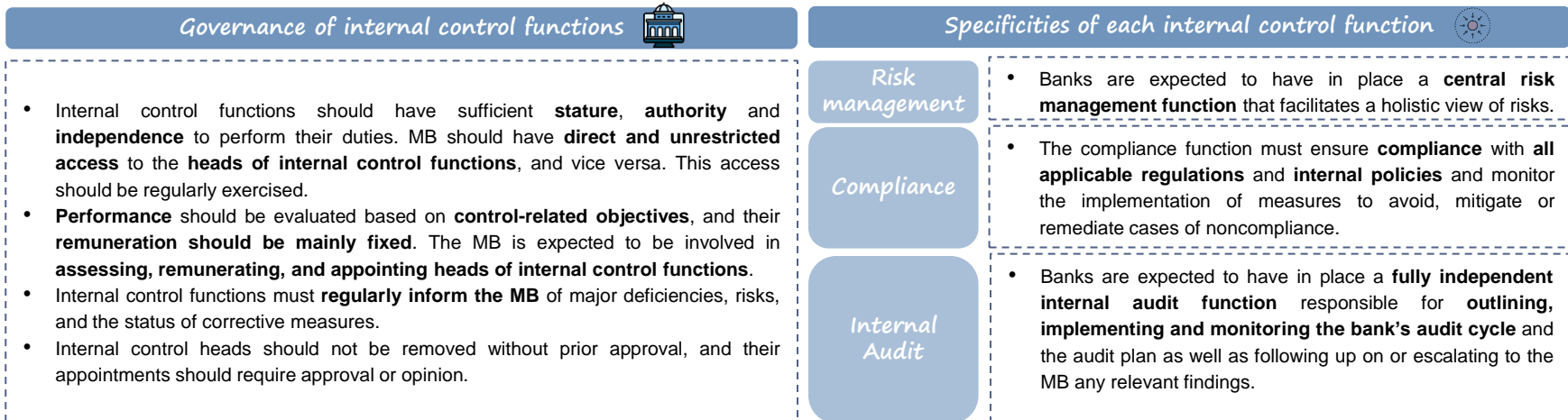
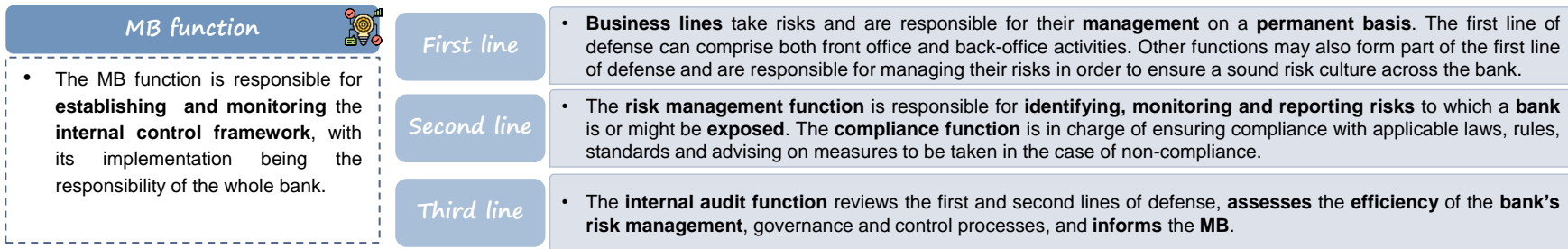
4

Internal control functions

Main aspects



To ensure the adequacy of the internal control mechanisms, the ECB expects that the processes of banks to identify, monitor and report risks and adequate internal control mechanisms are based on a three lines of defense model





There are some observed good practices for the internal control functions

Risk Culture Dimension		Observed good practices
Risk Management Function	Identification and monitoring of risks	<ul style="list-style-type: none"> Using a risk management toolkit which can be easily adjusted and adapted to any new risk developments, periods of crisis or emerging risks, using both backward and forward-looking information and adjusting the respective scenarios.
	Risk management	<ul style="list-style-type: none"> 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.
	Regular reporting to the risk reporting committee	<ul style="list-style-type: none"> CRO reports at least on a quarterly basis to the risk committee and the MB. 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). The CRO immediately informs the chair of the risk committee when a risk limit is breached. The risk committee 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
	Decision making	<ul style="list-style-type: none"> The CRO is involved in and provides an opinion on the bank's strategy-setting phase (including digital strategy) and has the power to veto for certain decisions. The CRO can also escalate any other case where the decision may entail increased risks. 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. Units within the risk management function are segregated from the units responsible for risk control activities. Internal control functions are also involved in all phases of the strategy design and roll-out. Proper appeal or escalation processes are properly documented in internal policies and implemented in practice for the final decision.



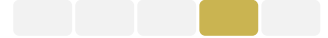
There are some observed good practices for the internal control functions

Risk Culture Dimension		Observed good practices
Compliance function		<ul style="list-style-type: none"> • CCO report at least on a quarterly basis (increased in the case of larger and more complex banks) to the MB. • The bank outlines a risk appetite which imposes a minimum standard across the banking group. • Comprehensive and harmonized risk assessment discussed at MB level implemented across the group. • Initiatives to ensure the digitalization of compliance processes. • Monitoring of the remediation of compliance function findings through a group-wide dashboard, accessed also by MB. • The group compliance function carries out compliance inspections within subsidiaries. • Quantitative metrics used in the RAF.
Internal Audit	Audit plan and cycle	<ul style="list-style-type: none"> • The audit plan acknowledges that resources may be needed for ad hoc reviews because of unexpected events, and sufficient spare capacity is readily available. • The audit plan takes into account supervisory authorities' findings (i.e. SREP recommendations).
	Follow-up on IA findings	<ul style="list-style-type: none"> • 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.
	Stature of IA during the issuing of report and findings	<ul style="list-style-type: none"> • 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

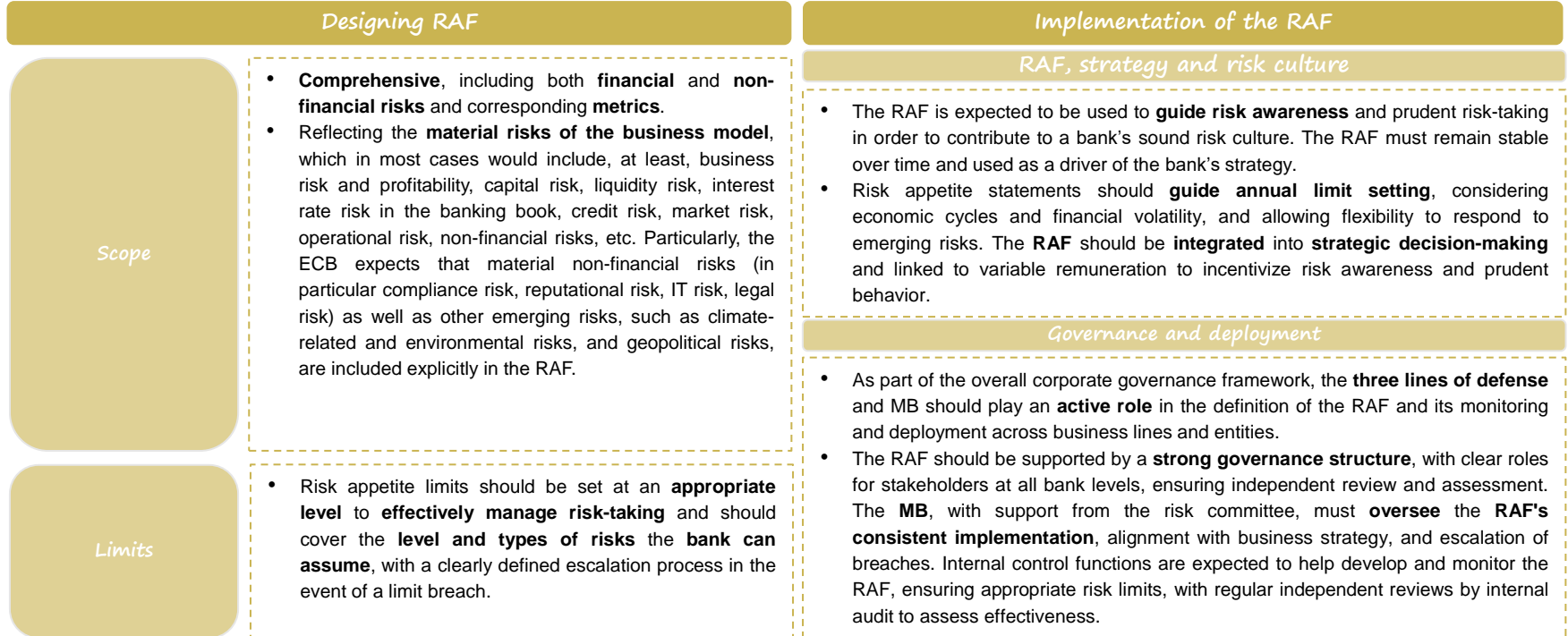
5

Risk appetite framework (RAF)

Main aspects

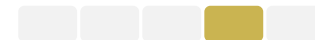


The RAF is a cornerstone of a sound governance framework. It should be integrated and documented within a bank's decision-making processes, including strategic decisions and key strategic processes



5 | Risk appetite framework (RAF)

Observed good practices



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

RAF Dimension		Observed good practices
Designing a RAF	Limits	<ul style="list-style-type: none"> The MB 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 MB is assessed relative to the complexity of the risks ((e.g. ranging from 20 to 40). 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. 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..
Implementing a RAF	Governance and deployment	<ul style="list-style-type: none"> The bank's internal policies require an opinion of the MB 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, various business units, departments responsible for risk management, and subsidiaries of the institution. 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. 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 organization. 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 tone from the top is adequately permeated cascaded throughout the bank in order to promote sound risk-taking in line with the RAF. There are training programs on risk appetite, including exams and certification, through which the management is able to monitor the employees' understanding of RAF and the organization'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

Main aspects

The ECB Banking Supervision employs a holistic approach, using a range of supervisory tools and techniques, to assess governance and risk culture in banks, including ongoing supervision, on-site inspections, and thematic reviews

ECB Banking Supervision supervisory activities and governance tools

- 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**. The ECB Banking Supervision uses a holistic approach to assess governance and risk culture components as well as a wide range of tools.
- In the course of **ongoing supervision**, the supervisory tools include the **assessment of MB 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, MB documents and minutes), as well as interviews, meetings, including bilateral meetings, and the periodic attendance of JSTs as observers at MB meetings.
- 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. **On-site inspections** provide a **complementary tool** to assess **governance and risk culture deficiencies** identified in the course of ongoing supervision. Specific deep dives, including on behavior and culture, on individual banks are also carried out on the basis of idiosyncratic risks.
- 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.

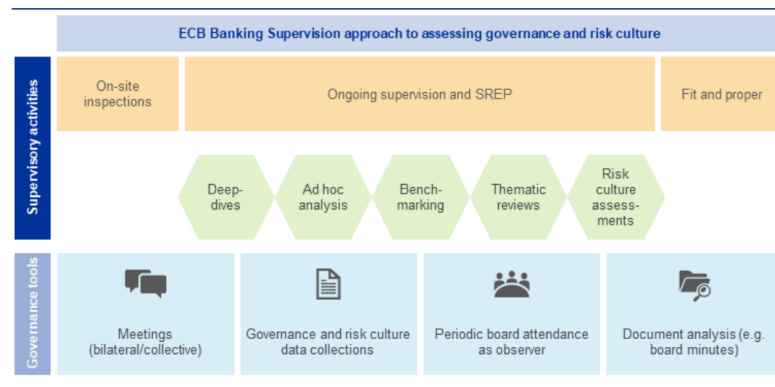


Figure 7: ECB Banking Supervision supervisory activities and governance tools

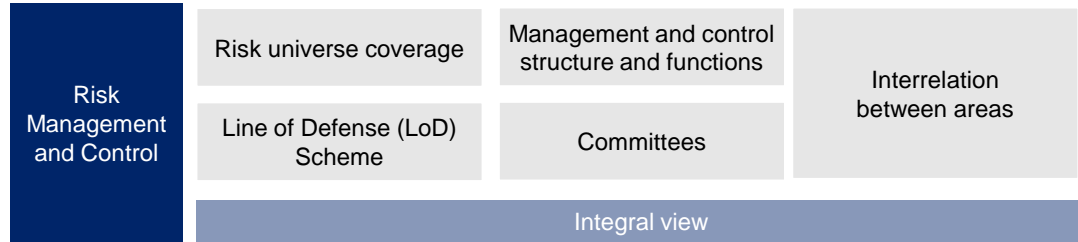
7 | Why Management Solutions?

MS value proposal

Based on MS experience in organizational structure and corporate governance review projects, a proven methodology to evolve towards best market practices while ensuring compliance with supervisory expectations has been defined

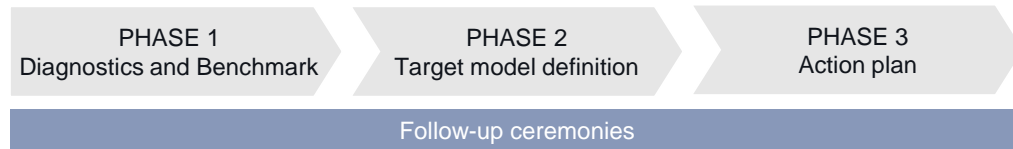
WHAT?

First, it will be given a detailed overview of main lines of analysis to be addressed in the project



HOW?

And then, considering the same axes, it will be explained how it will be carried out (Phases of the project)



7 | Why Management Solutions?

Main credentials

Projects and scope

- ▶ **Definition and implementation of Financial and Non-Financial Risk Management Frameworks** including prior **diagnosis** and subsequent **design of deployment plans** as well as support in their execution (PMO).
- ▶ **Risk appetite framework:** identification of key metrics for the different risk types, definition of calculation procedures, support in the calibration of thresholds, etc.
- ▶ **Governance and Organization:** design of **three lines of defense models for Financial and Non-Financial Risks** (participating areas, segregation of roles and responsibilities between lines, relationship model and communication flows, etc.).
- ▶ **Definition and implementation of assessment approaches (methodology):** qualitative approaches from an extensive (self-assessment) and intensive (large risk scenarios) perspective, quantitative approaches (internal/external losses), Key Risk Indicator (KRI) approaches, etc. and **specialist aspects of the different risks** (e.g. supplier assessment).
- ▶ **Risk Management policies and procedures** (risk identification and assessment, control environment, risk transfer, risk acceptance, etc.) and design of **robust control environments** for the mitigation of Financial and Non-Financial Risks (and objectification of the control environment).
- ▶ **Data and systems:**
 - ▶ **Governance, Risk and Compliance (GRC) tools:** implementation of proprietary (MIR, Gamma, SIRO) and third-party tools.
 - ▶ **Risk Reporting:** design of dashboards with 360° vision, definition of procedures to generate reporting, etc.
 - ▶ **Definition and Support in the Application of BCBS 239** in the Risk Domain

Clients

- 2 European supervisor and 1 American supervisor
- 3 European G-SIB
- Over 20 D-SIB in Europa and America
- Multiple local banks and savings banks with significant relevance in their respective regions
- Consumer credit financial institutions
- Credit cooperatives
- Asset management companies (investment funds)
- Insurance companies
- Large companies in regulated industries (Energy and Telecommunications)
- Etc.

Comparison with previous versions

The new Guidelines include some changes and new approach from the previous regulatory standards: SSM supervisory statement on governance and risk appetite and EBA GL on internal governance

Main changes from the 2016 SSM supervisory statement on governance and risk appetite

- 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 behavioral 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.



[Access to Document](#)

Main changes from the 2021 Guidelines on internal governance

- The **EBA Guidelines on Internal Governance** specify that EU banks and supervisors shall ensure that banks have strong management bodies. These bodies should be capable of challenging decision-making processes and maintaining a sound risk strategy, including appropriate risk appetite and risk management frameworks. The guidelines emphasize the importance of **governance arrangements** that promote a strong risk culture throughout all levels of an institution.
- The new guide on governance and risk culture presents a **more detailed and broader approach** compared to the 2021 guide. There is an increased **focus on risk culture**, including its link to **remuneration and accountability**, as well as behavioral aspects that were less developed in the previous guide. The current guide includes **more detailed chapters on a wider range of topics**, reflecting an evolution in supervisory expectations and observed good practices from supervisory experience.
- **Recent ECB publications, updated CRD provisions, EBA GL, and international standards have been incorporated**, providing a more contemporary and relevant framework for governance and risk culture in the banking sector.
- Additionally, the new guide sets out clear **objectives, timelines**, and **responsibilities** for responding to non-compliance, enhancing the responsiveness and **supervision capabilities**.
- These changes reflect an effort to strengthen **internal governance and risk culture in banking entities**, ensuring they are better prepared to face the challenges of the current financial environment.



[Access to Document](#)

A


Abbreviations

CCO	Chief Compliance Officer.
CRO	Chief Risk Officer
EBA	European Banking Authority
ECB	European Central Bank
GL	Guidelines
IT	Information Technologies
JST	Joint Supervisory Teams
MB	Management Body
RAF	Risk Appetite Framework
SREP	Supervisory Review and Evaluation Process
SSM	Single Supervisory Mechanism




International
One Firm


Multiscope
Team


Best practice
know-how


Proven
Experience


Maximum
Commitment

© Management Solutions, 2024

All rights reserved. Cannot be reproduced, distributed, publicly disclosed or transformed, whether totally or partially, free of charge or at no cost, in any way or by any means, without the express written authorization of Management Solutions.

The information contained in this publication is merely to be used as a guideline, is provided for general information purposes and is not intended to be used in lieu of consulting with our professionals. Management Solutions is not liable for any use that third parties may make of this information. The use of this material is not permitted without the express authorization of Management Solutions.

Antonio García
Partner at Management Solutions
antonio.garcia.perez@msspain.com

Marta Hierro
Partner at Management Solutions
marta.hierro@msspain.com

For more information please visit
www.managementsolutions.com

Or follow us at:     