EUROPEAN CENTRAL BANK

BANKING SUPERVISION

Internal governance and risk management SREP methodology

SREP Element 2: IGRM

The following sections provide a more detailed description of the methodology for assessing the internal governance and risk management (IGRM) of significant institutions as part of the Supervisory Review and Evaluation Process (SREP).

1 Introduction

The term “internal governance” refers to the internal organisation of an institution and the way it conducts and manages its business and its risks.

Internal governance, as part of overall corporate governance, includes the definition of the roles and responsibilities of the relevant persons, functions, bodies and committees within an institution and how they cooperate, both in terms of a governance framework and in terms of actual behaviour. This includes functions such as internal audit, risk management and compliance.

In addition, the internal governance framework encompasses all the institution’s rules and behavioural standards, including its risk culture and values, which are aimed at ensuring that the institution or group is properly managed. Among other things, adequate internal governance includes setting the institution’s performance and risk targets, introducing an effective administration and internal control system, establishing sound remuneration policies and practices, identifying and considering the interests of the institution’s stakeholders, and conducting business in line with the principles of sound, prudent management, while at the same time abiding by any legal and administrative provisions which may be applicable. If the institution is part of a group, the group dimension also needs to be assessed.

The IGRM assessment covers three main aspects:

- The internal governance framework (including the organisational structure, management body (MB)[1], risk management and compliance functions, and the internal audit function);
- The risk appetite framework (RAF) and the institution’s risk culture, as well as its remuneration policies;
- Risk data aggregation and reporting.

[1] The terms “management body in its management function” and “management body in its supervisory function” are not intended to refer to any specific governance structure, and references to the management (executive) or supervisory (non-executive) function should be understood as applying to the bodies or members of the management body responsible for that function in accordance with national law and the internal governance set-up.

The focus is on the overall governance and organisational arrangements of the institution, rather than on the controls for specific risks to capital, liquidity and funding. Such risk-specific controls are expected to be consistent with the institution-wide governance and risk management control framework and vice versa.

Supervisors follow the principle of proportionality in assessing the adequacy of the structures and processes in place, e.g. they take into account the scale and complexity of the institution.

The IGRM methodology is continuously updated in order to cover new aspects stemming from the evolving economic and regulatory environment – e.g. to reflect risks linked to the climate and environment, diversity-related deficiencies, anti-money laundering aspects, IT infrastructure, etc.

2 IGRM assessment

2.1 Assessment phases

The IGRM assessment encompasses three phases:

Table 1
IGRM assessment process

Phase 1	Information gathering and preliminary analysis, mainly based on information provided by the institution itself
Phase 2	Checks for compliance with relevant articles of the Capital Requirements Directive/guidelines of the European Banking Authority (EBA) and/or with ECB supervisory expectations and priorities related to IGRM
Phase 3	Supervisory assessment, including, but not limited to:[1)] Internal governance assessment (organisational structure, management body and the risk management, compliance, and internal audit functions) Risk management framework, remuneration and risk culture Risk infrastructure, data aggregation and reporting

1) As part of the SREP, supervisors carry out an assessment of sub-categories of internal governance and institution-wide controls as defined in the EBA Guidelines on the SREP.

IGRM is assessed from a qualitative i.e. risk control perspective.

Figure 1
The three phases of the risk control (RC) assessment for internal governance

Phase 1 Information gathering relies on various information sources, such as:

- internal documentation outlining features related to:

(a) the MB in its supervisory and management functions;

(b) sub-committees (charter, role, composition, succession planning and the skills and experience of members, relevant minutes on selected topics, etc.);

(c) the RAF; and

(d) remuneration policies, etc.

- the organisational structure:

(e) the organisational chart identifying key functions and committees;

(f) reporting lines and allocation of responsibilities, including key function holders and information on their knowledge, skills and experience, conflicts of interest, and reputation; and

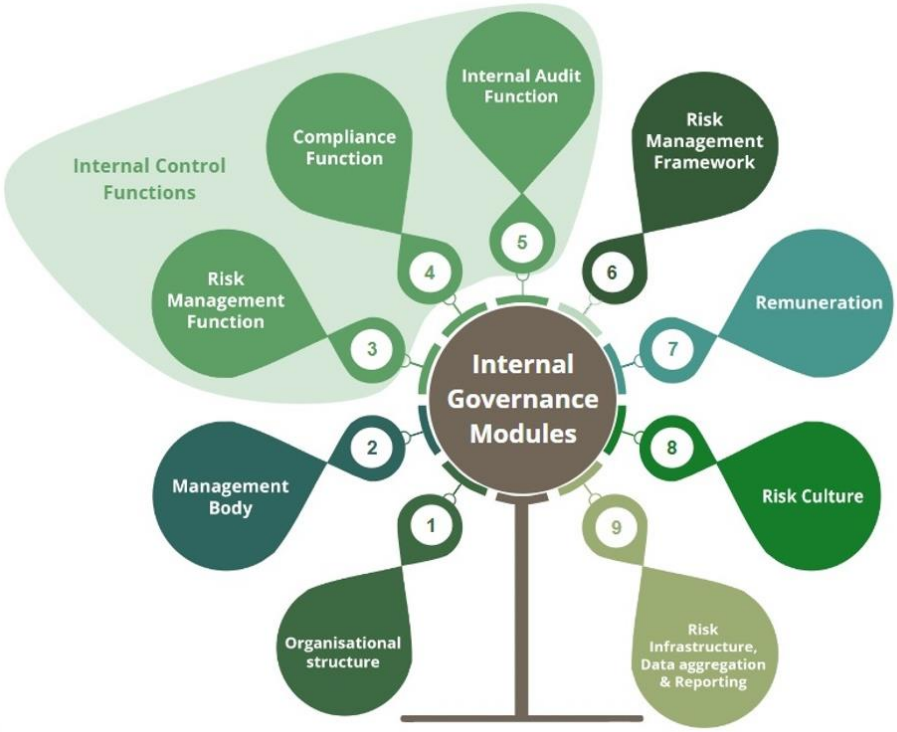
(g) relevant internal policies laying down governance-related processes and organisational arrangements, including those related to internal control functions (ICFs – such as internal audit, risk management and compliance policies, charters, assessment plans and reports on deficiencies, etc.).

Phase 2 Formal compliance checking verifies whether an institution's internal governance and risk control framework complies with key requirements arising from the applicable regulations (e.g. the Capital Requirements Directive), technical standards and key guidelines issued by the EBA or the Basel Committee on Banking Supervision, as well as ECB supervisory expectations and priorities.

In the **Phase 3 main risk control assessment** supervisors formulate their overall judgement on the quality of the internal governance framework, its current functioning and compliance with regulatory requirements. The internal governance assessment is structured into nine dedicated modules for supervisors to carry out specific in-depth assessments.

2.2 Overview of the modules

Figure 2
SREP Element 2: IGRM modules



2.2.1 Organisational structure

In this module the supervisors assess the transparency of the organisational structure, the coordination between the parent company and other entities in the group, the reporting lines, and ultimately the proper implementation of policies.

The degree of complexity of the structure may differ depending on whether the supervised institution is a stand-alone institution or a banking group. The main focus areas of this module are assessed as follows:

- **Transparency of the organisational structure** – the supervisors assess whether the bank has an appropriate, transparent and well-documented organisational structure, and whether there is a clear overview and understanding of all the activities of subsidiaries, branches, business lines, internal units and their functioning.

- **Coordination between the parent company and other entities in the group** – for banking groups, the supervisors assess the existence of clear agreements between the parent entity and the subsidiaries to ensure that the latter fulfil their obligations as separate legal entities and regulated companies. Supervisors also check whether, at the consolidated level, the

group is organised in such a way as to allow clear lines of responsibility and appropriate reporting relationships.

- **Proper implementation of policies** – supervisors assess the appropriateness of the internal governance policies in terms of organisational coverage, the business, risks, etc.

2.2.2 Management body

In this module the supervisors assess the MB's composition and collective suitability, its decision-making process and its functioning, and its oversight role. Moreover, the assessment aims to evaluate whether the MB has the ultimate and effective responsibility for setting the bank's overall strategy, determining its risk appetite, and overseeing the management and control of risk in line with that appetite.

Finally, supervisors assess the MB put in place by the bank. The proper functioning of the governing bodies is key to ensure robust decisions and proper management of the business.

The main focus areas in this module are assessed as follows:

- **Composition and collective suitability** – the supervisors assess the ability of the MB to preserve its collective suitability and an adequate composition on an on-going basis. The assessment takes into account various aspects, such as the size of the board, its knowledge, skills and experience, its reputation, its independence of mind, its time commitment, etc.

- **Decision-making process** – the supervisors assess the way decisions are taken by the MB, e.g. by verifying the quality of the internal debate (based on meeting minutes) and the quality and availability of the information prepared for the MB members ahead of meetings. The supervisors also check whether the MB is properly aware of the bank's key risks and whether adequate information on those risks is provided to the MB on a regular basis.

- **Oversight role** – the supervisors assess the oversight role of the MB in its supervisory function (MBSF). The oversight role includes reviewing the performance of the management function and the achievement of objectives, challenging the strategy, and monitoring the integrity of financial information as well as the effectiveness of ICFs, etc. To this end, the supervisors assess, among other things, whether the MB Chair facilitates open and critical discussion, enabling dissenting views to be discussed, and whether the MBSF members have fulfilled their mandate based on criteria such as independence of mind, etc.

Internal control functions (ICFs)

2.2.3 Risk management function,

2.2.4 Compliance function, and

2.2.5 Internal audit function

In these three modules the supervisors assess the organisation, status and resources of the risk management function, compliance function and internal audit function, their functioning (e.g. how their activities are carried out in practice) and their reporting to and interaction with the MB. The main focus areas in this module are assessed as follows:

- **Organisation, status and resources** – the supervisors assess whether the function operates independently and whether it has sufficient authority and stature to fulfil its duties properly. Additionally, they verify whether the ICFs have the necessary human and technical resources to carry out their work effectively and adequately.
- **Operation of the function** – the supervisors assess whether the positioning of each ICF within the organisation allows them to work independently and with sufficient authority and power, in particular, by ensuring adequate separation from the business units that these functions oversee (where applicable). Additionally, they verify how the ICFs cover all the activities and risks within their remit and the manner in which they classify the institution's functions and activities as “relevant” or “less relevant” with regard to risk and materiality.
- **Interaction with the MB** – the supervisors assess the way in which the ICFs interact with and report to the MB – i.e. they provide a critical and independent assessment on how the bank's business areas operate with regard to internal governance requirements, such as internal processes and policies, mandates, etc.

2.2.6 Risk management framework

In this module the supervisors assess the adequacy of the institution’s risk management framework.

The assessment focuses on the institution-wide implementation of the risk management framework, given that it should extend across all business lines and internal units, including ICFs, to enable the bank to make fully informed decisions

when risk-taking is involved. The assessment should also consider the components described below:

- **Risk appetite framework** – the supervisors assess the extent to which the bank's risk appetite is properly reflected in the MB's strategic discussions and decision-making process. Moreover, they assess how the RAF is approved and regularly reviewed by the MB, and whether its design and updates are adequately led by the risk management function with the support of other key functions.
- **Design of risk limits** – the supervisors assess whether the bank's governance for global and granular risk limits are closely linked to the institution's risk appetite and proportionate to its sound operation, financial strength, capital base and strategic objectives, and based on forward-looking assumptions.
- **Escalation process** – the supervisors assess the appropriateness of the escalation and contingency procedures. They verify how breaches of internal limit indicators trigger the escalation process and assess mitigating actions and the corresponding follow-up procedure.

2.2.7 Remuneration

In this module the supervisors assess the institution's overall remuneration policy and practices.

There are several dimensions and aspects to be considered, such as the internal process for setting the remuneration of the staff, in particular for employees whose professional activities have a material impact on the institution's risk profile. In addition, the supervisors verify whether the process ensures that variable remuneration does not contribute to or trigger excessive risk-taking and that it has no negative impact on the sound capital base. The main focus areas assessed in this module are:

- **Overall remuneration policy** – the supervisors assess the bank's remuneration policy and how it is implemented in practice – for instance the impact on the annual setting of the bonus pool. Furthermore, they verify whether the remuneration policy supports the achievement of the business objectives and at the same time preserves the long-term performance and long-term interests of the institution.
- **Staff identification process** – the supervisors assess the way in which the institution identifies the employees whose professional activities have a material impact on the institution's risk profile. These employees are generally known as material risk-takers or identified staff. Moreover, the supervisors check how the institution applies the qualitative and quantitative regulatory criteria in the identification process.

- **Setting of the bonus pool and variable remuneration** – the supervisors assess whether the institution has properly set the variable remuneration pool for the defined performance period as well as once the performance period is completed to check whether the envisaged variable remuneration pool can be paid out. In addition, they verify that the set-up of the bonus pool takes account of the legal ratio between fixed and variable remuneration, ex ante and ex post risk and performance adjustments, payment in the form of instruments, deferral schemes, etc.

- **Impact on the sound capital base** – the supervisors assess whether the remuneration policy and practices adequately contribute to the achievement and maintenance of a sound capital base at the consolidated group level and on an individual entity basis, with special focus on the variable remuneration that can be awarded.

2.2.8 Risk culture

In this module the supervisors assess whether institutions' risk culture ensures adequate transparency and whether it is based on clear standards, incentives and behaviours that properly inform and address risk awareness, risk-taking and risk management, as well as the adequacy of the risk control processes on which decisions are based.

Moreover, they verify whether and, if so, how the corporate risk culture influences the decisions of management and employees during their day-to-day activities as well as what impact it has on the risks they take. The main focus areas assessed in this module are:

- **Tone from the top** – the supervisors assess the internal definition and promotion of the risk culture from the top. More precisely, they verify whether the MB adequately defines and promotes a sound risk culture and checks its correct implementation (e.g. through a dedicated committee working on the risk culture and on the conflicts of interest policy, whistleblowing policy, remuneration policy, etc.).

- **Risk culture throughout the institution** – the supervisors assess how the risk culture is implemented and monitored across the bank. They verify how the key principles set in internal policies are cascaded throughout the organisation and whether they are used in practice (e.g. mandatory training sessions or workshops for all staff, or other initiatives; how potential ethics and conduct-related issues are flagged and handled within the institution, etc.).

- **Risk culture with respect to external stakeholders** – the supervisors assess the clarity and transparency of the interaction between the institution and its different stakeholders. More precisely, they verify whether the public disclosure includes key information on the institution's objectives, organisational and governance structures and policies, major

share ownership, voting rights and related party transactions, remuneration, etc.

2.2.9 Risk infrastructure, data aggregation and reporting

In this module the supervisors assess the extent to which banks are able to manage (identify/capture/monitor) and aggregate all relevant risk data across the institution, as well as generate and communicate up-to-date reports on risk data.

In addition, supervisors verify whether the IT infrastructure ensures timely, accurate and complete data and information for internal and external reporting, e.g. to respond to a wide range of requests from the MB and/or the competent authorities. The main focus areas assessed in this module are:

- **Governance and IT infrastructure** – the supervisors assess whether the bank's risk data aggregation capabilities and risk reporting practices are subject to strong governance arrangements (e.g. internal policies, etc.). The assessment focuses on several topics, such as the responsibilities of the MB, the data governance framework and its scope of application, the allocated resources and possible limitations on data quality. In addition, the supervisors assess whether the underlying IT infrastructure and data architecture fully support the bank's risk data aggregation capabilities and risk reporting practices, not only in normal times but also during times of stress or crisis.

- **Data aggregation** – the supervisors assess, among other things, whether the bank's risk data aggregation capabilities are adequate and ensure accuracy, completeness, timeliness and adaptability of risk data through effective data quality management (e.g. whether the institution relies on a highly automated environment and has effective mitigating measures in place for manual processes).

- **Reporting** – the supervisors assess whether the bank's internal, financial and regulatory/supervisory reports are accurate and distributed to the right recipients in a timely manner. In addition, the supervisors assess whether internal reports communicate clear and concise information, while remaining comprehensive enough to facilitate informed decision-making, and whether these reports are tailored to the needs of the recipients (e.g. the MB, etc.).