Consultation Paper
Application of the Supervisory Review Process under Pillar 2
(CP03 revised)

Table of contents

June 2005

Executive Summary and consultation process

This paper is a revised and expanded version of CEBS' consultation paper "The Application of the Supervisory Review Process under Pillar 2" (the first consultation on CP03), which closed for comment on 31 August 2004. These new proposals are still subject to revision, most especially if changes are made to the draft Capital Requirements Directive (CRD) before it is adopted.

CEBS has redrafted its proposals to include some of the suggestions it received in the consultation. The paper has been expanded to include guidelines on the general application of internal governance (IG) and how it applies to an institution's internal capital adequacy assessment process (ICAAP). There is also more detail on how the dialogue between the institution and its supervisor should be conducted, and how supervisors should use their internal Risk Assessment Systems (RAS) in the Supervisory Review and Evaluation Process (SREP).

CEBS recognises the increased need for supervisory co-operation, to address industry concerns that a lack of co-ordination could give rise to duplication of supervisory effort. These guidelines are designed to promote convergence of supervisory practice and consistency of approach, taking into account market trends and national practices, to achieve a sound and efficient market.

Principal aims of Pillar 2

The underlying aim of the Pillar 2 processes is to enhance the link between an institution's risk profile, its risk management and risk mitigation systems, and its capital. Institutions should themselves develop sound risk management processes that accurately monitor, measure and aggregate their risks. Institutions are expected to have an adequate assessment process that encompasses all the key elements of capital planning and management and generates an adequate amount of capital to set against those risks.

Institutions should 'own', develop and manage their risk management processes; the ICAAP belongs to the institution and supervisors should not dictate how it is applied. The task of the supervisory authority is to review and evaluate the ICAAP and the soundness of the internal processes within which it is used.

Internal governance is central to an institution's ICAAP. The guidelines now include a section explaining what supervisors will expect to find when they evaluate the adequacy of an institution's internal governance.

The dialogue between an institution and its supervisor is a key part of the supervisory review process. This paper highlights the respective involvement of supervisory authorities and institutions and the interaction between them, with the aim of making this dialogue clear and consistent. The dialogue should embrace all aspects of business risk and control risk, including risk management systems, internal control systems and internal governance. In order to ensure transparency and consistency in the dialogue, and to

promote convergence of supervisory practices, the supervisory processes have been laid out in detail.

The intensity and depth of the dialogue should be proportional to the nature scale, complexity and systemic importance of the institution. For example, a small non-complex institution would not be expected to have a sophisticated ICAAP, and its supervisor should not necessarily subject it to an intense and comprehensive dialogue. CEBS is doing further work on the concept of proportionality, which will be made available in due course.

The CRD provides supervisors with several tools for correcting weaknesses in the ICAAP, including setting a Pillar 2 capital requirement. However, capital may not always be the best mitigant of risk. Depending on the circumstances, it may be used on its own, in combination with other supervisory measures, or other measures be taken instead.

Further work

Further detail will be added in due course on the full set of Pillar 2 Building Blocks; that is, the step-by-step components that supervisors will use to perform their review and evaluation process, and the individual Pillar 2 risk buckets (i.e. specific risk factors) identified in chapter 4.

This set of guidelines will in due course be incorporated into a compendium of guidance – or handbook – for institutions and supervisory authorities on how to approach their obligations under the Banking Directive. CEBS plans to publish the final version of these guidelines in early 2006.

Request for comments

CEBS solicits comments on all aspects of this consultation paper, but is particularly interested in comments on the new elements that have been added since the initial version of this paper (CP03) was published in 2004. CEBS would especially expect to receive answers on the key questions highlighted below:

- Is there agreement on the importance of internal governance and should it be a key focus of the evaluation of the ICAAP?
- How could the proposed 'dialogue' between institutions and supervisors be made more effective?
- Would smaller, less complex institutions find additional optional guidance on the ICAAP helpful, and what might such guidance cover?
- It would also be useful to have views on the concept of proportionality, both as it relates (i) to the size and complexity of institutions and (ii) to the intensity of the dialogue between institutions and supervisors.

CEBS considers this to be a high priority project, and the timetable for completing it is tight. Nevertheless, the consultation period will be the full three months normally reserved for a first consultation, even though this is the second consultation on CP03, as new elements have been added and the

original paper has been substantially revised. An additional month has also been added because the summer months make up part of the consultation period. Comments should be submitted by Friday 21 October 2005 to CP03@C-EBS.ORG.

Comments will be published on CEBS' website (unless a respondent requests otherwise). After the consultation is closed an explanation will be published of how the major points raised were addressed. CEBS also refers readers to the separate publication of feedback to the first consultation on CP03.

CEBS' consultation papers on common reporting (CP04, 26 January 2005) and supervisory disclosure (CP05, 23 March 2005) also refer to Pillar 2. Feedback comments on these issues will be dealt with separately in the follow-up to those papers.

Chapter 1: Introduction

This paper sets forth guidance on the supervisory review process (SRP). It represents the collective views of EU supervisors on the standards (including standards on internal governance) that credit institutions and investment firms are expected to observe and the supervisory practices that supervisory authorities will apply.

The guidance elaborates on the relevant provisions of the Capital Requirements Directive (CRD): Articles 22, 123, 124 and 136.

This guidance is a key element of CEBS' programme to:

- Foster convergence of supervisory practices, which in turn should help level the playing field for institutions.
- Enable supervisors to carry out their tasks without imposing an undue supervisory burden on institutions.
- Promote a common understanding and culture among European supervisors.

In order to fully capture the implications of this guidance, it should be read in conjunction with CEBS' Home-Host and Supervisory Disclosure Consultation Papers. CEBS proposes broadening the existing mechanisms for exchanging information between EU supervisors to incorporate the routine sharing of practical experiences with the ICAAP-SREP interaction.

Key Components

SRP

The purpose of the SRP is to ensure that institutions have sufficient capital to support all the risks to which their business exposes them. Institutions are expected to develop and use sound risk management techniques in monitoring and measuring their risks.

Four internationally agreed principles underpin supervisory review:

- Institutions should have a process for assessing their overall capital adequacy in relation to their risk profile and a strategy for maintaining their capital levels.
- Supervisors should review and evaluate institutions' internal capital adequacy assessments and strategies, as well as their ability to monitor and ensure their compliance with regulatory capital ratios. Supervisors should take supervisory action if they are not satisfied with the result of this process.
- Supervisors should expect institutions to operate above the minimum regulatory capital ratios and should have the ability to require them to hold capital in excess of the minimum.
- Supervisors should seek to intervene at an early stage to prevent capital from falling below the minimum levels required to support the risk

characteristics of a particular institution and should require rapid remedial action if capital is not maintained or restored.

These principles have been incorporated into the CRD. Under the first principle, the management body (both the supervisory and management function)[1] of an institution bears primary responsibility for ensuring that processes are in place to ensure that the institution holds sufficient capital to meet both its regulatory and its internal capital targets. This principle is codified in Article 123 of the CRD and elaborated in the chapter of this paper on the internal capital adequacy assessment process (ICAAP). Sound internal governance is especially important in this context, and CEBS has developed further guidance based on Article 22 of the CRD.

The remaining principles - which require supervisors to review and evaluate the ICAAP, to perform their own assessment of the institution's risk profile, to identify any weaknesses or inadequacies, and to take supervisory measures if necessary - are codified in Articles 124 and 136 of the CRD. These are elaborated in the chapters of this paper on the supervisory review and evaluation process (SREP), risk assessment system (RAS), and Dialogue.

The SRP extends beyond the ICAAP and SREP to include ongoing supervisory monitoring of the institution's compliance with:

- The terms and conditions in the CRD for being granted approval to use the IRB and AMA (adequacy of risk evaluation systems).
- The conditions laid out under Article 145 for ongoing use of these models.
- Large exposures and an evaluation of disclosure under Pillar 3.

This guidance does not cover these wider issues, although further guidance will be developed in due course.

Internal Governance

Internal Governance is codified in Article 22 of the CRD. Internal governance aims at ensuring that an institution's management body (both the supervisory and management function) is explicitly and transparently responsible for its business strategy, organisation and internal control. Internal governance is the responsibility of the management body (both the supervisory and management function). It is concerned mainly with setting the institution's business objectives and its appetite for risk, how the business of the institution is organised, how responsibilities and authority are allocated, how reporting lines are set up and what information they convey, and how internal control (including risk control, compliance, and internal

[1] As explained more fully in the annex (definitions and acronyms), the term 'management body' is used in this paper to refer to both one-tier and two-tier management structures, and to both their 'supervisory' and 'management' functions. When reference is made to the management body, the text will note in brackets whether the reference is to the supervisory function, the management function, or both.

audit) is organised. The guidelines in Chapter 2 set forth European supervisors' expectations for the internal governance of institutions. Some of the guidelines are specifically directed at the ICAAP, while others have a broader application.

ICAAP

The ICAAP is codified in Article 123 of the CRD. Within the institution's internal governance framework, the ICAAP is a process to ensure that the management body (both supervisory and management functions):

- Adequately identify and measure the institution's risks.
- Hold adequate internal capital in relation to the institution's risk profile.
- Use sound risk management systems and develop them further.

Institutions have developed various methodologies for assessing their risk exposure and setting capital against it. The introduction of the ICAAP is not meant to suggest that existing methods, which have met the needs of institutions over the years, necessarily need to be replaced. However, all institutions should have adequate processes in place.

The ICAAP should be embedded in the institution's business and organisational processes, and not simply regarded as an add-on that permits the management body (both supervisory and management functions) to 'tick a box' and indicate that supervisory expectations nominally have been met.

SREP

The SREP is codified in Article 124 of the CRD. A key aim of the SRP is to reinforce the link between risk and capital, so that the institution's risk management strategy, approaches and systems are integrated with its capital planning. In order to evaluate the adequacy of capital held by an institution, the supervisory authority must review the institution's exposure to risks (its risk profile), the adequacy and reliability of its internal governance and ICAAP, the adequacy of its own funds and the internal capital mitigants it has set against its risks. The supervisor must also assess whether capital is the correct means of addressing the institution's vulnerabilities.

RAS

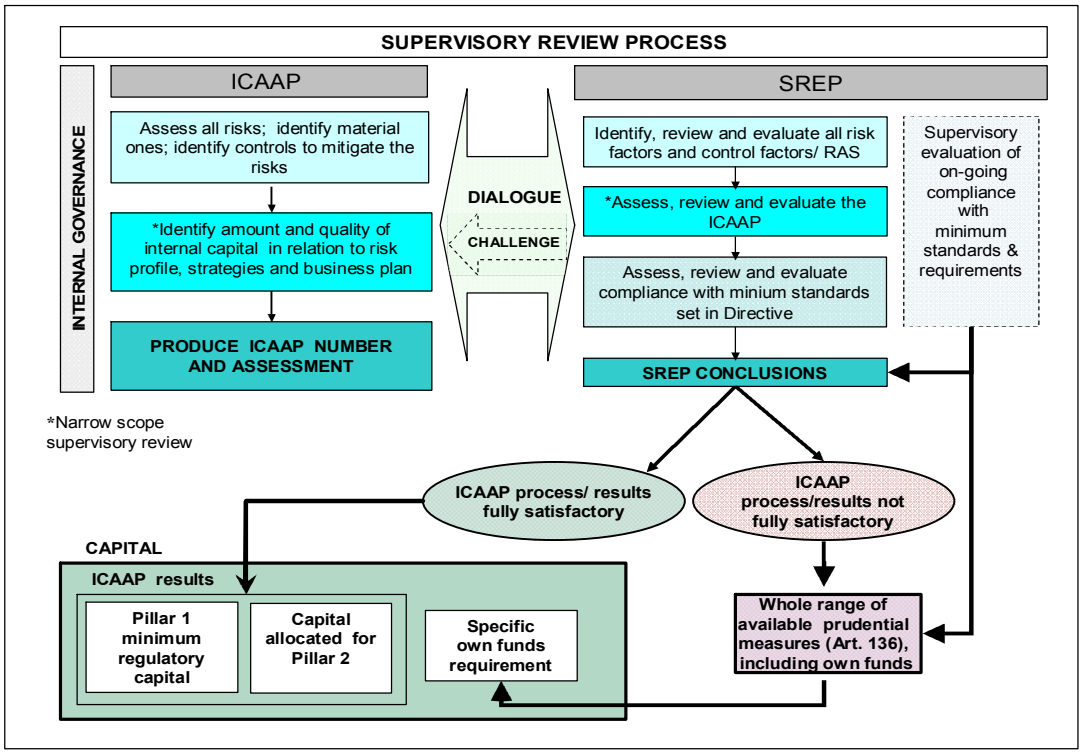
The RAS is the supervisor's tool for organising (i.e. planning, prioritising and allocating) the use of supervisory resources, and performing and managing the supervisory risk assessment. It provides structure and a practical step-by-step guide to the first phase of the SREP. It is therefore fundamentally a tool for internal supervisory purposes. The guidelines set forth in this paper should lead to greater commonality of approach among authorities. This in turn should facilitate more effective communication between supervisors, especially between home and host competent authorities.

ICAAP-SREP interaction

In the process of interaction and dialogue between supervisors and institutions concerning ICAAP supervisors question institutions on how they have assessed the risks they take and how they set their overall risk-bearing capacity. Supervisors use a 'building block' approach to break down the risks into discrete individual elements. The dialogue covers risk management, internal controls, the organisation of the institution's business, and how the institution allocate capital against risk. Such discussions are without prejudice to the institution's responsibility to design and implement an ICAAP which is appropriate for its own business.

While the guidance on interaction and dialogue is directed mainly at supervisory authorities, it will also be of relevance to institutions because (i) they must meet requirements on internal governance and the ICAAP, and (ii) they have a clear interest in knowing how supervisors intend to approach the interaction between the SREP and ICAAP, how the dialogue will be structured, and how this may influence supervisory judgements and actions. This process is illustrated in diagram 1.

Diagram 1: the Supervisory Review Process



Key considerations

Supervisors understand that the interaction of the ICAAP and SREP must be a balanced process, with each performing valuable functions and reinforcing the other.

Proportionality

The concept of proportionality is central to both the ICAAP and SREP, and also to the interaction between the two. It is laid down in the recitals of the CRD as well as in the provisions of the recast Directive on Pillar 2. It is important to note that, although the notion of proportionality is not repeated for each individual guideline, it applies consistently in this paper to all of them.

Proportionality covers two related concepts: (i) the ICAAP should be proportional to the nature, scale and complexity of the activities of the institution; and (ii) similarly, the depth, frequency and intensity of the SREP will be determined by the potential risk that the institution poses to the supervisor's objectives. Supervisors therefore need to adopt a graduated approach to the dialogue; this will have the additional advantage of optimising the use of supervisory resources.

Supervisors recognise that they will have to deal with a broad spectrum of institutions, ranging from the largest and most complex (which may elect to adopt advanced approaches based on economic capital models), to the many smaller and less complex institutions for which a relatively simple process is entirely acceptable. Indeed, one possibility for small and less complex institutions might be to base their ICAAP primarily on the Pillar 1 methodology, supplemented as necessary for any other generic factors which have a particular bearing on their risk profile (for example in terms of size, sector or products).

Relation to Pillar 1

The Pillar 1 capital requirement is based on uniform rules and is a minimum for regulatory capital requirements. However, no set of uniform rules can capture all aspects of an institution's overall risk profile. For institutions and supervisors alike, judgements on risk and capital adequacy are based on the institution’s overall risk profile, and therefore require more than a simple assessment of compliance with Pillar 1 minimum capital requirements.

Moreover, institutions are expected to operate above the minimum capital requirements set under Pillar 1. Requiring regulatory capital over and above Pillar 1 requirements is one of several regulatory tools that can be used by supervisors in the supervisory review process to address identified risks, after carefully considering other supervisory measures and other mitigating actions. Supervisors will place emphasis on the institution's own risk management process.

It should also be noted that while institutions may refer to internal capital or economic capital in their ICAAPs, these differ in meaning and composition from own funds. To maximise clarity, supervisory authorities will focus on (regulatory) own funds in the ICAAP-SREP dialogue.

Scope of application

The SRP applies to all institutions, consistent with the legal responsibility of supervisory authorities to carry out supervision at the level of individual institutions. However, the scope of application to institutions that are part of a group that is subject to consolidated or sub-consolidated supervision in the EU will depend on the final text of the CRD. As presently drafted, the CRD provides for some flexibility in application at the national level. CEBS' proposed guidelines for Home-Host co-operation aim to streamline the supervisory process.

Chapter 2. Guidance for institutions

This Chapter provides guidance on what supervisory authorities expect of institutions under the Pillar 2 framework. It sets forth how an institution can comply with:

- Guidelines on Internal Governance.
- Guidelines on the ICAAP.

2.1 Guidelines on Internal Governance

A Corporate Structure and Organisation

IG 1: Institutions should have a corporate structure that is transparent and organised in a way that promotes and demonstrates the effective and prudent management of the institution both on a solo basis and at group level.

The structure of an institution (and, where applicable, the structures and management lines of institutions within a group) should be clear and transparent both to the institution's own staff and to the relevant supervisory authorities. This is essential for supervisory oversight and for ensuring the effective and prudent management of the institution. Where appropriate, the supervisory authority may assess the legal organisation and the position of an institution within a group on a case-by-case basis.

IG 2: The reporting lines and the allocation of responsibilities and authority within an institution should be clear, precise, well-defined, transparent, coherent, and enforced.

a. There should be clear, precise and well-defined reporting lines and a clear and precise allocation of responsibilities and authority within an institution. Opaque or 'shadow' structures within an institution damage the ability of the management body (both supervisory and management functions) to conduct business in a prudent fashion.

b. The management body (both supervisory and management functions) should set and enforce clear lines of responsibility and authority within the institution. It is important that staff understand and adhere to policies and procedures concerning their authority and responsibilities. Staff receiving the information must be given adequate powers and authority to act.

c. Internal reporting has a dual function: (i) it is used by the management function as a tool for its oversight of management, and by senior management as a tool for their oversight of the entire institution; and (ii) staff use the information they receive from internal reports to carry out the responsibilities they have been given.

d. In cases where the business reporting lines do not match the legal structure of the institution or the group (e.g. operational structures where

there is no coincidence between business areas and legal units), the management body (both supervisory and management functions) should ensure that areas of responsibility and authority are sufficiently clear and transparent. Reporting lines that deviate from the institution's legal structure could result from a matrix organisation, a functional organisation, or a geographically widespread organisation.

IG 3: Institutions should ensure that the risk management function is organised in a way that facilitates the implementation of risk policies and the management of the institution's risks.

a. The risk management function should be a central organisational feature of an institution. It should be structured in a way that permits it to achieve its objectives of implementing risk policies and managing risk within the institution. Large, complex and sophisticated institutions should establish risk management functions to cover each material business line.

b. Risk management manages the risk-bearing capacity of the institution. It typically focuses on maximising the risk/return trade-off in the institution's various business lines. Risk management includes ongoing identification, measurement and assessment of all risks that could adversely affect the achievement of the institution's goals. The procedures for risk monitoring and assessment need to be updated regularly. The management body (both supervisory and management functions) should set the risk strategy, the risk policy, and accordingly the risk-bearing capacity of the institution.

B The Management Body

IG 4: The responsibilities of the management body should be clearly defined in a written document. They should include setting the institution's business objectives, risk strategies and risk profile, and adopting the policies needed to achieve these objectives.

a. These issues are the basis for the sound and prudent conduct of business, and should be decided at the level of the management body (both supervisory and management functions).

b. Senior management is responsible for implementing the strategies and policies set by the management body (both supervisory and management functions). It is important that written guidelines, manuals, and other means that are deemed necessary, are used to facilitate the accurate implementation of the institution's overall objectives.

c. Documentation should include the essential duties and working procedures of the management body (both supervisory and management functions). These documents, along with the minutes of the meetings of the management body (both supervisory and management functions), should help the supervisor to evaluate the operation of the management body (both supervisory and management functions).

IG 5: The management body should ensure that strategies and policies are communicated to all relevant staff throughout the organisation.

The management body (management function) should inform and update the staff concerning the institution's strategies and policies, at least to the level needed to carry out their particular duties. This may be done through written guidelines, manuals or other means. It is also important that the staff understand and adhere to policies and procedures pertaining to their duties and responsibilities.

IG 6: The management body should systematically and regularly review the strategies and policies for managing the risks of the institution.

a. Every institution should have effective processes for identifying, managing, monitoring and reporting the risks that it is exposed to. The management body (both supervisory and management functions) should ensure that the relevant strategies and policies are amended when necessary to reflect changing internal and external factors. This is particularly true for the macroeconomic environment in which the institution operates and the position in the business cycle.

b. Committees within the management body (supervisory function) may be set up to address risk management and audit if this facilitates the development and maintenance of good governance practices, as outlined above.

IG 7: The management body should develop and maintain strong internal control systems.

a. Strong internal control systems are essential to the ICAAP. The management body (both supervisory and management functions) is responsible for developing and maintaining systems to ensure effective and efficient operations, adequate control of risks, prudent conduct of business, reliability of financial and non-financial information reported or disclosed both internally and externally, and compliance with laws, regulations and the institution's internal policies and procedures.

b. There are several instruments at the disposal of the management body (both supervisory and management functions) for maintaining a sufficiently high standard of internal control. These include the risk control function, the compliance function, and the internal audit function, all of which are described in the section on 'Internal Control' below.

IG 8: The management body should ensure that internal control systems provide for adequate segregation of duties, in order to prevent conflicts of interest.

In developing the internal control system, the management body (both supervisory and management functions) should ensure that there is a clear,

transparent and documented decision-making process and a clear allocation of responsibilities and authority to ensure compliance with internal decisions and procedures. The internal control mechanisms should be adequate in relation to the business performed by the institution, and should constitute sound administrative and accounting procedures.

IG 9: The management body should set effective strategies and policies to maintain, on an on-going basis, amounts, types and distribution of both internal capital and own funds adequate to cover the risks of the institution. (See ICAAP section for further details.)

a. The management body (both supervisory and management functions) should ensure that the institution's strategies and policies regarding both internal and regulatory capital are both comprehensive and proportionate. Documentation should specify what types of regulatory capital may be used. Furthermore, the distribution of regulatory capital within a group must comply with legal requirements concerning the allocation of capital to subsidiaries (i.e. capital should be allocated where the risks are).

b. For internal capital, the institution is free to use a different definition of capital from that used for regulatory purposes, but here too the supervisor will expect the institution to allocate capital where the risks are.

IG 10: The management body should monitor and periodically assess the effectiveness of the institution's internal governance structure.

a. At least once a year, the management body (both supervisory and management functions) should review and, if necessary, amend its policies for the internal governance structure of the institution. This frequency applies only to the internal governance issues covered by these guidelines. It does not transcend any legal obligations or recommendations concerning governance issues on the national level.

b. A review of the internal governance structure itself should also be performed annually. This review should focus on any changes in internal and external factors affecting the institution.

IG 11: The management body should be active and independent, and should be able to explain its decisions to the supervisory authority and other interested parties.

a. Notwithstanding their obligations towards other stakeholders as required under national law, the members of the management body (both supervisory and management functions) should be free to take decisions in the best interest of the institution. Their decisions should be clearly based on the information and should take into account all relevant factors. This is particularly important when there may be conflicts of interest with other stakeholders, or within a group.

b. The members of the management body (both supervisory and management functions) should have the necessary expertise to carry out their duties, and should be able to make their own judgements and decisions.

IG 12: The management body should have policies for selecting, compensating, monitoring and planning the succession of key executives.

a. One of the primary tasks of the management body (both supervisory and management functions) is to ensure that the institution has, and will continue to have, qualified and experienced key executives.

b. The compensation schemes of the management body (both supervisory and management functions) should not be structured in a way that encourages unhealthy risk-taking or maximisation of short term profits.

IG 13: The management body should promote high ethical and professional standards and an internal control culture.

Implementing such standards throughout the institution should help reduce the risks to which it is exposed. For example, when the reputation of an institution is called into question, the loss of trust can be difficult to rebuild and can have repercussions throughout the market. In particular, operational risk will be reduced if these standards are given high priority. The management body (both supervisory and management functions) should therefore have clear policies for how these standards should be met, and they should perform a continuing review of their implementation.

C Internal Control

IG 14: Institutions should establish, as a minimum, the following three primary functions in order to implement an effective and comprehensive system of internal control in all areas of the institution, namely (i) risk control function, (ii) compliance function, and (iii) internal audit function.

a. These internal control functions should be independent of the business lines they monitor and control.

b. A control function can generally be regarded as independent if the following conditions are met:

- The control function staff do not perform any tasks that fall within the scope of the activities that the control function is intended to monitor and control.
- The control function is organisationally separate from the activities it is intended to monitor and control. The head of the control function is subordinated to a person who has no responsibilities for the activities that are being monitored and controlled.

- The head of the control function reports directly to the management body (both supervisory and management functions) and/or the audit committee, and is present at least once a year at meetings of the body it reports to.
- The remuneration of the control function staff is not linked to the performance of the activities that the control function is intended to monitor and control.

c. These functions should also be organisationally independent from each other, since they perform different functions. The reporting lines should run directly from the above-mentioned functions to the management body (both supervisory and management functions).

IG 15: The risk control function should ensure compliance with risk policies.

a. Risk control requires an appropriate control structure. This should include the establishment of control policies and procedures as well as verification that the control policies and procedures are complied with. Control activities should be defined at every business level.

b. The risk control function is designed to address the risks that the institution identifies through its risk assessment process. In large, complex and sophisticated institutions, a risk control function should be established to monitor each of the material risks (in material business lines) to which the institution is exposed. The risk control function should report to the management body (both supervisory and management functions) and other relevant staff. Senior management should continuously evaluate the risks affecting the achievement of its goals, and should react to changing circumstances and conditions.

IG 16: The compliance function should identify and assess compliance risk.

a. The compliance function is mainly an instrument for the management body (management function). Its primary task is to report any deviation – confirmed or potential – from relevant "laws, regulations, codes and standards" to the head of the relevant business line and senior management.

b. In cases of serious violations of the rules, the compliance function should also report to the supervisory function of the management body.

c. The management body (management function) needs to be fully updated on existing and proposed laws, regulations, codes and standards that are relevant to the institution. The compliance function can assist senior management in achieving this objective. The compliance function can also assess the possible impact of any changes in the legal environment on the operations of the institution. The compliance function also has the role of verifying that new products, and new procedures are in compliance with the current and future legal environment. It is the responsibility of the entire management body (both supervisory and management functions) to ensure

that the compliance function has sufficient resources (well-qualified and experienced staff, as well as a sufficient number of staff) at its disposal.

d. In some Member States, the internal audit function also covers the tasks of the compliance function.

IG 17: The internal audit function should allow the management body to ensure that the quality of the internal controls is adequate.

a. The internal audit function should have unfettered access to the management body (both supervisory and management functions) and/or to the audit committee where applicable. Any suggestions by internal audit for material improvements in internal controls should be reported directly to the management body (both supervisory and management functions). All audit recommendations should be subject to a formal follow-up procedure by the respective level of management, in order to ensure (and report) their resolution.

b. The internal audit function should evaluate the adequacy of the internal control framework of the institution (including the risk control and compliance functions where this is a different function) and report its findings. It should also have unfettered access to relevant documents and information in all business lines. It should evaluate the compliance of all activities and divisions with the institution's policies and procedures. The internal audit function must also evaluate whether existing policies and procedures remain adequate. It is the responsibility of the entire management body (both supervisory and management functions) to ensure that the internal audit function has sufficient resources (well-qualified and experienced staff, as well as a sufficient number of staff) at its disposal.

IG 18: There should be effective internal control systems and reliable information systems covering all significant activities of the institution.

a. A critical component of an institution's activities is the establishment and maintenance of management information systems that cover the full range of its activities. This information is typically provided through both electronic and non-electronic means. Institutions must be particularly aware of the organisational and internal control requirements related to processing information in an electronic form, and of the necessity to have an adequate audit trail. Management decision-making could be adversely affected by unreliable or misleading information provided by systems that are poorly designed and controlled.

b. Information systems, including those that hold and use data in electronic form, must be secure, independently monitored and supported by adequate contingency arrangements.

IG 19: The management body should put in place appropriate internal alert procedures for communicating internal governance concerns from the staff.

a. Institutions are encouraged to adopt appropriate internal alert procedures that staff can use to draw attention to significant and legitimate concerns regarding matters connected with internal governance. These procedures should respect the confidentiality of the staff who raise such concerns. There should be an opportunity to raise these kinds of concerns outside regular reporting lines (e.g. to the head of compliance or internal auditor). The procedures on how to make their concerns known should be made available in writing to all staff within the institution. Information provided by the staff through the alert procedure should, if relevant, be made available to the management body (both supervisory and management functions).

b. In some Member States, in addition to any internal alert procedures within the institution, there may also be a possibility for staff to inform the supervisory authority of their concerns of this type.

D Public Disclosure and Transparency

IG 20: Institutions should aim for the highest standards of transparency in the conduct of their business.

a. Institutions should consider public disclosure going beyond regulatory requirements as a way of reinforcing their internal governance. For major institutions, the expectations of investors, customers, rating agencies and others may require a higher degree of transparency.

b. Public disclosure is desirable in the following areas: the structure of the management body (both supervisory and management functions), basic organisational structure, the incentive/remuneration structure of the institution and the nature and extent of transactions with affiliates and related parties. Such disclosures enable interested parties to form a true and accurate assessment of the institution.

c. Institutions may also find it desirable to describe how their risk management, risk control, compliance and internal audit functions are organised. Finally, they may want to outline the major tasks performed by these functions, describe how performance is monitored by the management body (both supervisory and management functions), and describe how any necessary improvements are being implemented.

IG 21: Each institution should present its current position and future prospects in a balanced, accurate and timely way.

a. Information about the current position of the institution should comply with any legal requirements regarding the disclosure of such information. The information should be accurate, relevant, timely and accessible, in order to meet the needs of supervisors, investors, customers, clients, rating agencies, external credit assessment institutions (ECAIs), and the public.

b. In cases where ensuring a high degree of accuracy would delay the release of time-sensitive information, the institution should make a judgement as to the appropriate balance between timeliness and accuracy, bearing in mind the requirement to provide a true and fair picture of the institution's situation. This reasoning should not be used to delay regular reporting requirements, and a satisfactory explanation of the circumstances warranting an exception should be provided.

c. Disclosures should include, but are limited to, material information on the financial and operating results of the company, foreseeable risk factors and governance structures and policies including, in particular, the content of any corporate governance code or policy and the process by which it is implemented.

2.2 Guidelines on ICAAP

This Chapter provides guidelines on what supervisory authorities expect of institutions under ICAAP.

ICAAP 1: Every institution must have a process for assessing its capital adequacy relative to its risk profile (an ICAAP).

Every institution must have an ICAAP. The scope of application (i.e. consolidated, sub-consolidated and/or solo) of this principle to institutions which are part of a group that is subject to consolidated supervision will depend on the final decision taken in the CRD on this point.

ICAAP 2: The ICAAP is the responsibility of the institution.

a. Each institution is responsible for its ICAAP, and for setting internal capital targets that are consistent with its risk profile and operating environment. The ICAAP should be tailored to the institution's circumstances and needs, and it should use the inputs and definitions that the institution normally uses for internal purposes.

b. At the same time, the institution must be able to demonstrate how the ICAAP meets supervisory requirements.

c. Without prejudice to ICAAP 4, any outsourcing of portions of the ICAAP must meet CEBS' standards on outsourcing (CP02, "The High Level Principles on Outsourcing," published 30 April 2004). Institutions retain full responsibility for their ICAAP regardless of the degree of outsourcing, and they should understand that outsourcing does not relieve them of the need to ensure that their ICAAP fully reflects their specific situation and individual risk profile.

ICAAP 3: The ICAAP's design should be fully specified, the institution's capital policy should be fully documented, and the management body (both supervisory and management functions) should take responsibility for the ICAAP.

a. The responsibility for initiating and designing the ICAAP rests with the management body (both supervisory and management functions). The supervisory function within the management body should approve the conceptual design (at a minimum, the scope, general methodology and objectives) of the ICAAP. The details of the design (i.e. the technical concepts) are the responsibility of the management function.

b. The management body (both supervisory and management functions) is also responsible for integrating capital planning and capital management into the institution's overall risk-management culture and approach. They must ensure that capital planning and management policies and procedures are communicated and implemented institution-wide and supported by sufficient authority and resources.

c. The institution's ICAAP (i.e. the methodologies, assumptions and procedures) and capital policy should be formally documented, and it should be reviewed and approved at the top level (management body in the sense of both functions) of the institution.

d. The results of the ICAAP should be reported to the management body (both supervisory and management functions).

ICAAP 4: The ICAAP should form an integral part of the management process and decision-making culture of the institution.

a. More sophisticated institutions should completely integrate the ICAAP into their management processes. This could range from using the ICAAP to allocate capital to business units, to having it play a role in the individual credit decision process, to having it play a role in more general business decisions (e.g. expansion plans) and budgets.

b. Less sophisticated institutions should construct the ICAAP in a way that allows the management body (both supervisory and management functions) to assess, on an ongoing basis, the risks that are inherent in their activities and material to the institution.

ICAAP 5: The ICAAP should be reviewed regularly.

a. The ICAAP should be reviewed by the institution as often as is deemed necessary to ensure that risks are covered adequately and that capital coverage reflects the actual risk profile of the institution. This review should take place at least annually.

b. The ICAAP and its review process should be subject to independent internal review.

c. Any changes in the institution's strategic focus, business plan, operating environment or other factors that materially affect assumptions or methodologies used in the ICAAP should initiate appropriate adjustments to the ICAAP. New risks that occur in the business of the institution should be identified and incorporated into the ICAAP.

ICAAP 6: The ICAAP should be risk-based.

a. The adequacy of an institution's capital is a function of its risk profile. Institutions should set capital targets which are consistent with their risk profile and operating environment.

b. Institutions may take other considerations into account in deciding how much capital to hold, such as external rating goals, market reputation and strategic goals.

c. However, if other considerations are included in the process, the institution must be able to show in its dialogue with its supervisor how they influenced its decisions concerning the amount of capital to hold.

d. Less sophisticated institutions that take a Pillar 1 approach as the starting point for their ICAAP (see below) should also begin to develop a fully risk-based approach, as the Capital Requirements Directive promotes a risk-based approach (including the Standardised Approach for credit risk), and because general management and control frameworks will increasingly be risk-based.

ICAAP 7: The ICAAP should be comprehensive.

a. The ICAAP should capture all the material risks to which the institution is exposed. The concept of materiality should be defined and justified by the institution.

b. At a minimum, the ICAAP should consider:

- Pillar 1 risks. The institution should note any differences between the treatment of Pillar 1 risks in the ICAAP and supervisory methods, including differences in the type of risks that are captured by each process, in the type of methodology, and in the parameters used in assessing risks.
- Risks not fully captured under Pillar 1. Risks which fall into this category could include underestimation of credit risk using the standardised approach, underestimation of operational risk using the basic indicator approach or standardised approach, and for stressed loss given default (LGDs). Specifically, regarding credit risk, the following should be taken into account, for example, stress-testing in IRB, residual risk in credit risk mitigation (CRM), and securitisation.
- Pillar 2 risks. The ICAAP should cover all Pillar 2 risks, including interest rate risk in the banking book, concentration risk, liquidity risk, settlement risk, reputation and strategic risk. Some of these risks are less likely to lend themselves to quantitative approaches, and therefore have tended to be more subject to interpretation by the institution. The ICAAP is intended

to promote greater convergence of individual outcomes at the national level, through benchmarking and peer-group analysis.

- Risk factors external to the institution. In addition, the ICAAP will need to cover other Pillar 2 risks which institutions themselves identify as key considerations which may arise from the regulatory, economic or business environment.

c. There is no standard categorisation of risk types, although supervisors will usually expect the institution to consider all material risks. The institution should be free to use its own terminology, but should be able to explain the details to the supervisor, including the methods used, the coverage of all risks and how its approach relates to its obligations under Pillar 1. This would be necessary, for example, if the institution used a definition of operational risk that differed from the definition in Pillar 1, or a definition of interest rate risk that included both banking book and trading book risk.

d. Most risks are quantifiable, and institutions should be expected to devise methods for measuring them. However, there may be some risks which are more qualitative in nature, and which require more qualitative methods of assessment and mitigation. These qualitative risks may need to be defined, but will probably include reputation and strategic risk. An institution is expected to be aware of all material risks, whether quantitative or qualitative in nature, and to have processes in place for assessing, monitoring, managing and controlling them.

ICAAP 8: The ICAAP should be forward-looking.

a. The ICAAP should take into account the institution's strategic plans and how they relate to macro-economic factors. The institution should develop an internal strategy for maintaining capital levels which can incorporate factors such as loan growth expectations, future sources and uses of funds and dividend policy, and a procyclical variation of Pillar 1 minimum regulatory capital. The institution should have an explicit, approved capital plan which states the institution's objectives and the time horizon for achieving those objectives, and it should set forth in broad terms the capital planning process and the responsibilities for that process.

b. The plan should also lay out how the institution will comply with capital requirements in the future, any relevant limits related to capital, and a general contingency plan for dealing with divergences and unexpected events (for example, raising additional capital, restricting business, or using risk mitigation techniques).

c. Institutions should conduct appropriate stress tests which take into account, for example, the risks specific to the jurisdiction(s) in which they operate and the particular stage of the business cycle. Institutions should analyse the impact that new legislation, the actions of competitors or other factors may have on their performance, in order to determine what changes in the environment they could sustain.

ICAAP 9: The ICAAP should be based on adequate measurement and assessment processes.

a. Institutions should have a documented process for assessing risks. This process may operate either at the level of the individual institution, or at group level.

b. The results and findings of the ICAAP should feed into an institution's evaluation of its strategy and risk appetite. For less sophisticated institutions in particular, for which genuine strategic capital planning is likely to be more difficult, the results of the process should mainly influence the institution's management of its risk profile (for example, via changes to its lending behaviour or through the use of risk mitigants).

c. Institutions will not be required to use formal economic capital (or other) models, although it is expected that more sophisticated institutions will elect to do so.

d. There is no single 'correct' process. Depending on proportionality considerations and the development of practices over time, institutions may design their ICAAP in different ways. For example, the ICAAP may use:

- The result produced by the regulatory Pillar 1 methodologies (which are themselves risk-based) and consideration of non-Pillar 1 elements. In other words, to obtain a capital goal, institutions may take the Pillar 1 requirements and then assess Pillar 2 concepts that relate to Pillar 1 (such as concentration risk, residual risk of CRM and securitisation) and concepts that are not dealt with under Pillar 1 (such as interest rate risk). The Pillar 1 approach may be appropriate for some less sophisticated institutions, although they would have to take an active role in justifying this choice, including consideration of forward-looking elements. Supervisors would expect the institution to demonstrate that it had analysed all risks outside Pillar 1 and found them to be absent, not material, or covered by a simple cushion over the Pillar 1 minimum.
- A 'building block' approach, using different methodologies for the different risk types (Pillar 1 and Pillar 2 risks) and then calculating a simple sum of the resulting capital requirements. This is explored in more detail in chapter 4.
- A more sophisticated and complex system, possibly using 'bottom-up' transaction-based approaches with integrated correlations.

e. Institutions are likely to find that some risks are easier to measure than others, depending on the availability of information. This implies that their ICAAPs could be a mixture of detailed calculations and estimates.

f. It is also important that institutions not rely on quantitative methods alone to assess their capital adequacy, but include an element of qualitative assessment and management judgement of inputs and outputs. Considerations such as external rating goals, market reputation and strategic goals should be taken into account in all three methodologies.

g. Non-quantifiable risks should be included if they are material, even if they can only be estimated. This requirement might be eased if the institution can demonstrate that it has an appropriate policy for mitigating/managing these risks.

ICAAP 10: The ICAAP should produce a reasonable outcome.

a. The ICAAP should produce a reasonable overall capital number and assessment. The institution should be able to explain to the supervisor's satisfaction the similarities and differences between its ICAAP (which should cover all risks) and its regulatory requirements.

b. Institutions might be encouraged to make greater disclosures of information which is not proprietary or confidential. This may provide them a means for comparing their ICAAP with their peer group, for internal purposes.

Chapter 3. Guidance for Supervisory Authorities

The supervisor's role in the SRP includes reviewing and evaluating the institution's ICAAP and performing an independent assessment of the institution's risk profile. It also includes taking prudential measures and other supervisory actions, when appropriate, to reflect the individual circumstances of the institution. These measures can include requiring additional regulatory capital.

The SREP should be structured with a view to ensuring consistency of capital treatment across institutions, keeping in mind that institutions differ in risk profile, strategy and management. Supervisors should have arrangements in place for the collection and verification of relevant information, and procedures to maintain the quality and consistency of risk assessments. An essential element of the SREP (and of the RAS) is the ability to assess qualitative elements adequately. Along with elements specifically related to each type of risk and its management, special attention should be given to the overall level of compliance with the principles and guidance for internal governance as set forth in Chapter 2 of this paper.

This paper stresses that it is the responsibility of European supervisory authorities to take full account of all the guidelines on internal governance in the preceding chapter, in their review and evaluation of institutions, both initially when a license is granted and on an ongoing basis. The guidelines on internal governance aim to establish and maintain a level playing field across Europe, covering the most important factors that supervisors should monitor within institutions.

In the performance of the SREP at the national level, supervisors generally have recourse to the tool of peer-group comparison. This tool is not available at the cross-border level. But it would seem desirable to hold regular confidential discussions between supervisors, in order to promote convergence, comparability and consistency and to ensure a level playing field in the supervision of large international groups.

Supervisors assess the risk profile of an institution using a variety of sources (including statistical, desk-based analysis, on-site visits, and routine relationship management) as part of risk-based prudential supervision. This should provide the foundation for the supervisor to undertake (among other things) an evaluation of the institution's risk profile, key inputs to which will be the evaluation of institution's ICAAP and the supervisory dialogue this generates with the institution. It should also enable the supervisor to determine appropriate prudential measures (including setting a capital requirement above the Pillar 1 minimum, if necessary), to apply those prudential measures over a period determined by the supervisor, and to maintain an accurate and up-to-date picture of the institution’s risk profile in light of its progress in implementing prudential measures and/or other events which may have a significant impact on the risk assessment.

For institutions that intend to apply for advanced approaches, the approval processes for credit, operational and market risks can help to identify any relevant aspects of the individual institution's methods which may have Pillar 2 implications (including system and control factors). Supervisors may wish to develop a similar approach to identifying those elements of standard approaches which are open to a degree of interpretation or provide scope for regulatory arbitrage.

This Chapter provides guidelines on SREP and RAS.

3.1 Guidelines on SREP

SREP 1: The SREP should be an integrated part of the authority's overall risk-based approach to supervision.

a. The evaluation process will be an integral, explicit and formal part of the authority's overall supervisory approach.

b. The evaluation process underpins the supervisor's dialogue with the institution (and does not replicate the role of the institution's management).

c. It is recognised that different supervisory authorities will use different types of evaluation processes. For example, there will be differences in the emphasis on qualitative versus quantitative judgements and the degree of automation within a system.

d. However, European supervisory authorities agree that while flexibility of approach is important, common minimum standards are needed in order to ensure consistency of application and a level playing field across Europe.

SREP 2: The SREP should apply to all authorised institutions.

The scope of application (i.e. consolidated, sub-consolidated and/or solo) of this principle with respect to institutions which are part of a group that is subject to consolidated supervision will depend on the final text of the CRD on this point.

SREP 3: The SREP should cover all the activities of an institution.

a. All significant business units of the institution, whether operating domestically or overseas, will be considered in the evaluation process.

b. Other risks to the consolidated group will also be captured, for example where services such as IT, accounting, or payment and settlement functions are being provided or control functions are being exercised from outside the consolidated group on an outsourced basis (even if within the wider group).

SREP 4: The SREP should cover all material risks and internal governance.

a. The supervisory authority will formally evaluate the institution's risks factors and control factors.

b. The evaluation will focus on identifying each institution's risk profile and assessing the quality of the institution's risk management system. The business risks covered should span all activities and all significant business units. The evaluation of controls should include, at a minimum, an assessment of the quality of internal governance, senior management, organisational structure, the risk management and control environment and internal audit and compliance functions. Supervisors should review the controls that have been put in place to mitigate risk, as well as the adequacy and composition of capital held against those risks.

c. The evaluation should be forward-looking in the sense that it should consider, based on information known at the time, whether the risk profile of the institution is likely to change over the forthcoming period.

d. The supervisor can use stress tests to help determine the need for early intervention.

e. Both qualitative and quantitative assessments for specific risks will require more elaborate and precise guidance, which will be laid out in future papers.

SREP 5: The SREP will assess and review the institution's ICAAP.

The supervisor will assess the institution's ICAAP as part of its SREP. This should include a consideration of the assumptions, components, methodology, coverage and outcome of the institution's ICAAP. This review should cover both the institution's risk-management processes and its assessment of adequate capital. Supervisors should review the controls in place to mitigate risk, as well as the adequacy and composition of capital held against those risks. This is laid out in more detail in chapter 4.

SREP 6: The SREP will assess and review the institution's compliance with the requirements laid down in the CRD.

As part of the SREP, the supervisor must also evaluate the institution's compliance with the various minimum requirements under the CRD. For instance, in addition to the ICAAP requirements, these include an evaluation of the methods and models used in advanced approaches under Pillar 1, large exposures and an evaluation of disclosure under Pillar 3.

SREP 7: The SREP should identify existing or potential problems and key risks faced by the institution and deficiencies in its control and risk management frameworks; and it should assess the degree of reliance that can be placed on the outputs of the institution's ICAAP.

This process will enable the supervisory authority to tailor its approach to the individual institution, provide the foundation for the supervisor’s general approach to the institution and its actions, and provide incentives for institutions to improve their risk management systems.

SREP 8: The SREP will inform supervisors about the need to apply prudential measures.

Once it has evaluated the adequacy of an institution's capital in relation to its risk profile, the supervisor should identify any prudential measures or other supervisory actions required. For example, where there is an imbalance between business and control risks, the supervisor should consider the range of remedial supervisory actions that may be needed to rectify a deficiency in controls and/or perceived shortfalls in capital, either as a long-term requirement(s) or as a short-term action(s). This is laid out in more detail in chapter 4.

SREP 9: The results of the SREP will be communicated to the institution at the appropriate level (usually the management body in the sense of senior management function) together with any action that is required of the institution and any significant action planned by the supervisory authority.

a. The authority will convey the results of its risk assessment to the institution. This may be done as part of the dialogue between the authority and the institution on the internal systems used to assess capital adequacy, which is described in more detail in chapter 4.

b. This review and evaluation allows the supervisor, among other things, to provide qualitative feedback to the institution about the adequacy of its risk management and internal controls in relation to its business risk profile, and to assess and understand the extent to which the output of the ICAAP can serve as an input to the SREP.

SREP 10: The supervisory evaluation should be formally reviewed at least on an annual basis, to ensure that it is up-to-date and remains accurate.

a. Supervisory authorities agree that this review may not always constitute a full risk assessment.

b. However, supervisory authorities should at least take stock of any significant changes to the overall risk profile over the past year. They will take into account the results of any supervisory visits, inspections and other information received during the period, and will consider whether the timing of the next full assessment, as agreed during the previous full assessment process, remains appropriate.

c. Notwithstanding the above, any significant new information received in the course of ongoing monitoring and supervision which may affect the institution’s risk profile will trigger consideration by the authority of the need for a formal review or a full risk assessment.

RAS

The RAS is the supervisor's tool for organising (i.e. planning, prioritising and allocating) the use of supervisory resources, and performing and managing the supervisory risk assessment. It is intended to provide structure and a practical step-by-step guide to the first phase of the SREP.

3.2 Guidelines on RAS

RAS 1: In order to carry out an overall assessment of an institution, the supervisory authority should define guidelines covering both risks and controls.

a. The overall assessment of the risks and controls should be done in a way that facilitates the allocation of resources to those institutions (or those areas within institutions) that require the most attention. Supervisory authorities should have individual ratings for risks and controls.

b. The guidelines for integration (or aggregation) may be based upon the following key principles:

- High risks are assigned a relatively higher weight than low risks.
- Weak controls are assigned a relatively higher weight than strong controls.
- Risks are assigned a relatively higher weight than controls, reflecting the fact that requirements for controls should increase as the level of inherent risk rises.

c. Given the different approaches used in different countries, the resulting overall assessment may not arrive at the same scoring or rating of risks and controls.

d. It may be useful to set a default score or rating for particular risks within business units of institutions. In certain circumstances, for example where there is insufficient information to set a score or rating at the outset, the supervisory authority may wish to set a conservative or high default score or rating and then correct it in the light of further analysis.

RAS 2: In order to assess an institution's risks and controls, the supervisor needs to prepare a breakdown of the institution's activities, down to the material business units or processes where risks are actually taken and where to a large extent controls are actually applied.

a. Supervisory authorities need to formulate rules for the breakdown process, taking into account the need to identify the various business elements under supervision for planning purposes. This implies that the level of detail of the breakdown needs to be geared to the level of detail of the planning process.

b. The starting point is a general description of the institution. To facilitate the detection, assessment and aggregation of risks and the quality of the

controls, the institution can be broken down into significant business units or processes.

c. This breakdown is especially useful for groups and major institutions. It may be simpler for smaller institutions.

d. This process can be structured as follows (the basic process will be the same for large and small institutions, but it will of course be more complex for larger entities):

- Identification of all business units or processes, using the institution's organisation chart as a starting point. Two types of business units or processes can be distinguished: (i) business lines (e.g. mortgages, treasury, credit cards) and (ii) management functions (e.g. centralised departments such as ALM, risk-management, internal audit, internal control).
- Identification of centralised group functions to facilitate the assessment of group-wide risks and controls, such as overall strategic risk, quality of the members of the management body (both supervisory and senior management functions), reporting lines at the highest level, and centralised management functions (e.g. risk management, internal audit and internal control).
- Determination of the significance (materiality) of each unit or process using both quantitative (e.g. contribution to earnings, profit or capital requirement) and qualitative criteria.
- Assessment of the relative impact of the business units or processes on the overall assessment of risks and controls in the light of the issues raised in the previous bullets.
- While this breakdown is important, particularly for the consolidating supervisor, an individual-entity approach is also very important for effective communication between home and host competent authorities when a group has cross-border subsidiaries. An individual-entity approach is also important for the dialogue between supervisors and institutions concerning the appropriate distribution of capital within a group. Keeping an individual-entity approach in mind will help to ensure that the distribution of capital remains appropriate: i.e. that the allocation of capital remains commensurate with the distribution of risks, so that each institution, including the parent, has the appropriate amount of capital relative to its risks in each country, and sufficient leeway for growth.

e. The supervisor should select the relevant risk categories it would like to include in the assessment, as not all risk categories may be applicable or relevant to each business unit or process.

f. In the final step of the breakdown process, the supervisor decides whether to perform a full-scale expert assessment or a simplified, less detailed assessment. In the latter case, scores or ratings could be assigned directly, at a more aggregated level. This decision should take into account the balance between workload and value-added. In jurisdictions with a large

number of smaller institutions, the use of default scores or ratings may be considered.

RAS 3: A Risk Assessment System should encompass all relevant risks and internal governance factors, while at the same time making a clear distinction between the two.

To support the comparability of different Risk Assessment Systems, and given the needs of cross-border cooperation and information-sharing, all supervisory authorities should take into account the full set of risks and principles elaborated in this paper.

RAS 4: In order to make the results of all risk assessments comparable, both between the various institutions within a country and between countries, the results of the supervisory authorities' risk assessments should be based on an assessment of both quantitative and qualitative information.

a. The core of the Risk Assessment System is the assessment of the risk profile and the quality of the controls of the institution under supervision. This assessment should cover all significant business units and processes. The rating system preferably should be designed to discourage the tendency to assign average risk scores or controls to groups of banks. Each risk and control category should be sub-divided into its underlying determinants (for example, credit risk may consist of three items: default probability, concentration and correlation, and recovery rate). The rating system may also cover the quality of the loan portfolio and the amount of provisions.

b. These determinants should be rated by means of a qualitative assessment, which may be expressed in a (quantitative) score or rating. Quantitative information, as well as qualitative information, is necessary to provide key insights to certain risks, and should be used to form the overall qualitative and quantitative assessment.

c. Supervisors may wish to lay out, by way of public disclosure, the criteria underlying each score or rating class, in order to:

- Explain the overall system.
- Assist in understanding the risks of a particular bank.
- Allow better comparisons between different national systems.

d. In addition to the knowledge and professional judgement of the individual supervisors regarding the supervised institutions, supervisors can draw upon a broad range of information sources to help them assess the risks and mitigating controls of institutions. These include:

- Information available in supervisory examination reports, including information available from on-site inspections.
- Mandatory financial reporting by supervised institutions (for example, information on credit risk provided in reports on large exposures, country

risk exposures, total provisions, non-performing loans, doubtful loans, etc.).

- Information from reporting by supervised institutions in compliance with other regulatory requirements.
- Interviews (and minutes of these interviews) with senior management and staff of supervised institutions.
- Internal management reports of the supervised institution, which can be made available on request (e.g. profit and loss account, balance sheet, strategy and policy papers and budgets).
- Internal minutes of various management and committee meetings (e.g. Management Board, ALCO, credit committee).
- The internal and external audit reports of the supervised institution.

e. Supervisory Authorities may wish to develop an IT-tool to support the risk assessment method. This may facilitate the assessment of risks and controls and improve its efficiency. It may also help standardise systems and facilitate comparisons and transfers of information between supervisors within the same country, or between countries. An IT-tool may also provide a useful audit trail.

RAS 5: Procedures for quality assurance should be in place in order to maintain the quality and consistency of risk assessments.

a. Quality assurance is one of the key elements in the overall risk assessment process. It maintains the quality and consistency of assessment results, and may consist of the following elements:

- An adequate challenge process, including a regular review of the global risk assessment process. One possible way of structuring this review in some countries might be to submit the results of the risk assessment to a quality assurance panel consisting of experienced supervisors.
- A regular review of individual assessments. Consistency and comparability can be ensured by having a minimum of two supervisors perform the various steps in the risk analysis (the 'four eyes' principle).
- The risk assessment process may be supported by a dedicated team. It may support the supervisors during the assessments, communicate with senior management and international authorities, further develop the risk assessment methodology and software tools, and maintain the risk assessment manual.
- A traceable rating history or audit trail, so that changes in the assessment can be traced back to the responsible supervisor.

RAS 6: The supervisory authority should compare the results of the RAS with the outcome of the ICAAP and analyse their consistency.

The RAS does not constitute a parallel or secondary ICAAP or a benchmark for an institution's own processes. However, if an institution's ICAAP is judged to be inadequate, the RAS should be able to assist the supervisory authority in determining, in general terms, the overall risk profile of the institution, and may provide an indication of the capital needed to cover all the risks.

Chapter 4: The SREP-ICAAP interaction and prudential measures

4.1 Guidelines on the dialogue

Dialogue 1: Supervisors should have a methodology for structuring the dialogue with the institution so that they can systematically perform their own assessment of whether the capital held by the institution covers all material risks.

a. A key element of the SREP is the dialogue between supervisors and institutions. It will inform the supervisor about the way the institution's ICAAP is structured, the assumptions which are used to determine underlying risks across different sectors and risk types, risk sensitivity and confidence levels, and how risks are aggregated.

b. The supervisory assessment should be based on a review of the institution's ICAAP. The SREP is not intended to perform a parallel calculation (although some form of independent calculation may be necessary in cases where an institution's ICAAP is so flawed that the supervisor decides it cannot be relied upon to form the basis for the dialogue).

c. It would be inappropriate for the supervisor to enter into the ICAAP-SREP dialogue with pre-conceived ideas as to how much capital may be necessary to cover Pillar 2 risks. It is up to the institution to justify its process for identifying and measuring its risks and then justify how much capital, if any, it allocates against them. The institution should be able to explain any differences between its own assessment of capital needs and targets under the ICAAP and regulatory requirements.

Dialogue 2: The structure of the dialogue should be based on a 'building block' approach.

a. Supervisors should use a building block approach as the basis of the dialogue:

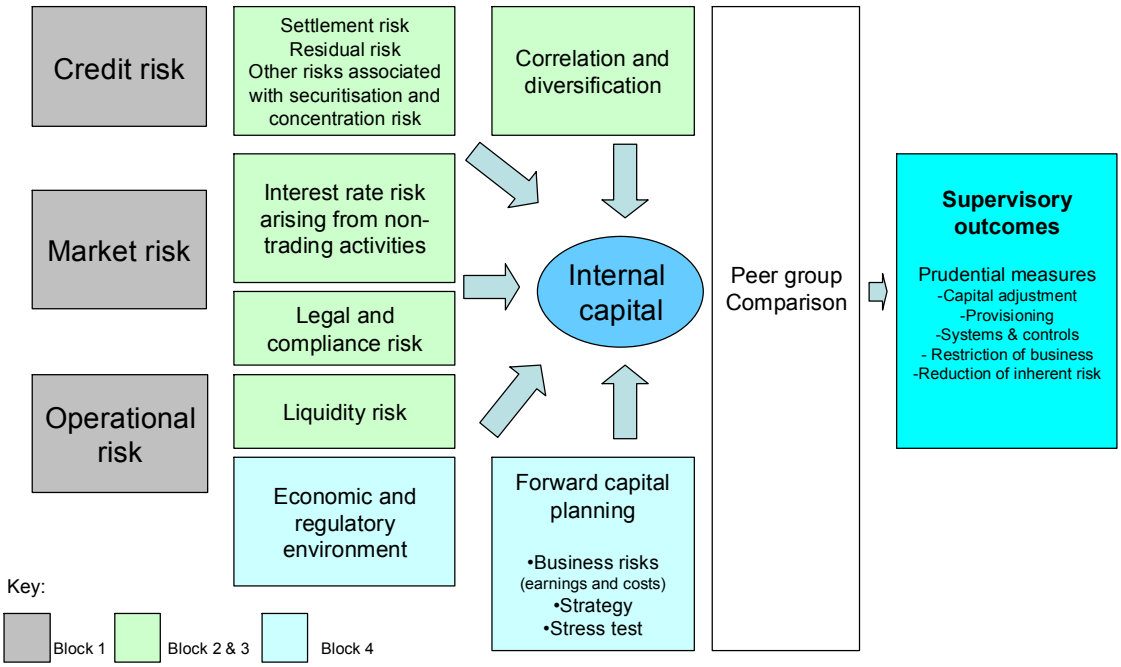
- Block 1: Pillar 1 risks (credit, market, and operational risk).
- Block 2: Risks not fully captured under Pillar 1 (for example, residual risk in CRM, stress-testing in IRB, and securitisation risk).
- Block 3: Risks covered by Pillar 2 (for example, interest rate risk in the banking book, concentration risk, liquidity risk, settlement risk, reputation risk, strategic risk). Under credit risk, block 3 would include underestimation of credit risk using standardised approaches and weaknesses in credit risk mitigation.
- Block 4: External factors.

b. The building block approach is illustrated in Diagram 2. As noted in the key to the diagram, some of the elements span more than one block (particularly for blocks 2 and 3). Further guidance will be provided in due

course on the content of these four building blocks and the individual risk buckets which fall within block 3.

c. It is important to stress that the building blocks should not be interpreted as a system of automatic capital add-ons. Supervisors will apply judgement when considering the relationship between qualitative and quantitative components.

Diagram 2: Supervisory review using the building block approach



Dialogue 3: Supervisors should use the dialogue with the institution to test and challenge the institutions' ICAAP and to exchange views, in order to reach a better understanding of the underlying assumptions and processes.

a. For this process to be effective, supervisors need to have a thorough understanding of how the ICAAP is determined and the differences between it and Pillar 1. This should also help them evaluate the ICAAP outcome. This process emphasises the importance of analysing each risk separately, understanding the differences between ICAAP assumptions and Pillar 1 assumptions, and understanding the extent to which the institution has introduced diversification and correlation effects.

b. As is the case with current supervisory practice, the supervisor may use the results of the RAS and a mix of on-site and off-site inspection to increase its understanding of the institution's ICAAP.

c. The institution may make changes to the ICAAP in the course of the dialogue, in response to challenge and feedback from the supervisor. Following the dialogue, the supervisor will reach an assessment.

Dialogue 4: The frequency and depth of the dialogue will be determined by the supervisor, according to its assessment of the risk profile and/or systemic importance of each institution.

a. It is up to the supervisory authority - not the institution - to determine when the dialogue should start and how intensive it will be. The supervisory authority will also determine the nature and depth of the dialogue, based on the type of institution and its peer-group ranking.

b. Once the process has begun, the dialogue will provide the opportunity for iteration between the ICAAP and SREP, with each informing the other.

c. Although the intensity of the dialogue will vary both between and within peer groups of institutions (reflecting the nature of the peer group and the levels of concern, based on risk assessment), supervisors will establish basic benchmarks for the intensity of supervisory resources that will be needed for each peer group. Supervisors will then be expected to scale up from these benchmarks for those institutions which are assessed as posing greater risk.

d. For larger and more sophisticated institutions, the dialogue is likely to be tailored to fit their particular needs. For smaller, less sophisticated institutions – for whom a detailed dialogue may not be necessary – more standardised guidance may be provided on the Pillar 2 components; but such guidance by the supervisor should not be allowed to develop into *de facto* regulation.

4.2 Guidelines on prudential measures

Measures 1: Prudential measures - to address issues identified either through the SREP or as part of ongoing supervision - should be applied promptly.

a. If the supervisor considers that an institution's ICAAP does not adequately reflect its overall risk profile, or does not result in the institution having adequate capital, then consideration should be given to applying prudential measures.

b. The measures available to the supervisory authorities include:

- Requiring an institution to hold own funds and/or Tier 1 capital above the minimum level required by Pillar 1, and/or imposing other limitations on own funds.
- Requiring the institution to improve its internal control and risk management frameworks.

- Requiring the institution to apply a specific provisioning policy or treatment of assets in terms of regulatory capital requirements
- Restricting or limiting the business, operations or network of the institution.
- Requiring the institution to reduce the risk inherent in its activities, products and systems.

c. The range of envisaged supervisory measures should be identified as one output of the SREP. The final decision on which measures to implement will be taken by the supervisor, taking into account the outcome of the dialogue with the institution.

d. The choice of prudential measures should be determined according to the severity and underlying causes of the situation and the range of measures and sanctions available to the supervisor. Measures can be used individually or in combination. A specific own funds requirement should, however, be imposed on any institution which exhibits an imbalance between its business risks and its internal control and risk frameworks, if that imbalance cannot be remedied by other prudential measures or supervisory actions within an appropriate timeframe.

e. A specific own funds requirement may also be set where the supervisor judges the level of own funds held by an institution to be inherently inadequate for its overall risk profile. It must be acknowledged that there is no 'scientific' method for determining the amount, and that capital is not a long-run substitute for remedying deficiencies in systems and controls. In practice, the process relies heavily on subjective judgement and peer-group consistency to ensure a level playing field and a defence to challenge by institutions.

f. A balanced view of all available supervisory measures (as set out in CRD Article 136) is essential as an outcome of the process.

Measures 2: Prudential measures should be communicated promptly and in sufficient detail.

a. In communicating its decision on prudential measures, the supervisory authority should:

- Explain in sufficient detail the factors which have led to the risk assessment conclusions.
- Indicate areas of weakness and the timeframe for remedial action.
- Explain the reasons for any adjustment to the institution's capital requirements.
- Indicate what improvements could be made to systems and controls to make them adequate for the risks and activities of the institution, and for this improvement to be reflected in the institution's capital requirements.

b. It is recognised that the relationship between the supervisory authority and the institution's external auditors varies from country to country and

that, depending on the various countries, it may not be appropriate for supervisors to communicate the results of their assessment to the external auditors or to discuss it with them.

Annex 1: Definitions and acronyms

Internal governance

In these guidelines, the term 'internal governance' is used, as opposed to the term 'corporate governance.' While corporate governance has a wider scope and includes issues that concern the shareholders and other stakeholders of an institution, internal governance focuses on the responsibility of management body (both supervisory and senior management functions). It is mainly concerned with setting the institution's business objectives and its appetite for risk, how the business of the institution is organised, how responsibilities and authority are allocated, how reporting lines are set up and what information they convey, and how internal control (including risk control, compliance, and internal audit) is organised.

Institutions

Credit institutions and investment firms as defined in the CRD.

Management body

The guidelines on internal governance in this document do not advocate any particular board structure. In order to be consistent with the CRD, the term 'management body' is used in this document to embrace different structures, such as one-tier and two-tier boards. (In some countries there is also an additional internal Statutory Body, which performs formal and legally required checks on the activities of the Board of Directors; in this case the supervisory function is performed by both the non-executive directors of the Board of Directors and by members of this Board of Statutory Auditors.)

Within any institution, there are two functions that must be fulfilled: supervision and management. Some Member States use a one-tier board structure, in which both functions are performed within the board of directors. The supervisory function is performed by the non-executive directors of the board and the management function is performed by the executive directors of the board.

Other Member States use a two-tier board structure. In a majority of these Member States, the supervisory function is performed by the board of directors and the management function is performed by the senior management. The board of directors is responsible, among other things, for supervising senior management to ensure that they fulfil their tasks. Senior management, on the other hand, is responsible for the day-to-day management of the institution.

In this document, when describing which functions within the management body we are referring to, this is mentioned in brackets. Reference is made to either the supervisory function, the management function, or both.

Internal Control

The management body is responsible for ensuring that the institution has in place the three independent functions that constitute an efficient system of internal control. These functions are risk control, compliance and internal audit. The risk control function ensures that risk policies are complied with. The compliance function identifies and assesses compliance risk. The internal audit function is an instrument for the management body to ensure that the quality of the risk control function and the compliance function is adequate. Internal control also includes, e.g. accounting organisation, treatment of information, risk assessment and measurement systems.

Risks

For the purposes of this paper, the risks faced by institutions are defined as follows:

Business risks: consists amongst others of credit risk, market risk, interest rate risk, liquidity risk, operational risk, strategic risk, and reputation risk.

Concentration risk: as part of credit risk, concentration risk includes (i) large (connected) individual exposures and (ii) significant exposures to groups of counterparts whose likelihood of default is driven by common underlying factors, e.g. sector, economy, geographical location, instrument type.

Credit risk: the current or prospective risk to earnings and capital arising from an obligor's failure to meet the terms of any contract with the institution or its failure to perform as agreed. This risk includes residual risk, the credit risk in securitisation and cross-border (or transfer) risk.

Interest rate risk: the current or prospective risk to earnings and capital arising from adverse movements in interest rates.

IT risk: sub-category of operational risk: the current or prospective risk to earnings and capital arising from inadequate information technology and processing in terms of manageability, exclusivity, integrity, controllability and continuity, or arising from an inadequate IT strategy and policy or from inadequate use of the institution's information technology.

Legal and compliance risk: sub-category of operational risk: the current or prospective risk to earnings and capital arising from violations or non-compliance with laws, rules, regulations, agreements, prescribed practices, or ethical standards.

Liquidity risk: the current or prospective risk to earnings and capital arising from an institution's inability to meet its liabilities when they come due.

Market risk: the current or prospective risk to earnings and capital arising from adverse movements in bond prices, security or commodity prices or foreign exchange rates in the trading book. This risk can arise from market-making, dealing, and position-taking in bonds, securities, currencies, commodities, or derivatives (on bonds, securities, currencies, or

commodities). This risk includes foreign exchange risk, defined as the current or prospective risk to earnings and capital arising from adverse movements in currency exchange rates.

Operational risk: the risk of loss resulting from inadequate or failed internal processes, people and systems or from external events. This risk includes IT, legal and compliance risk.

Reputation risk: the current or prospective risk to earnings and capital arising from adverse perception of the image of the financial institution on the part of customers, counterparties, shareholders, investors or regulators.

Residual risk: sub-category of credit risk: the risk that recognized risk measurement and mitigation techniques used by the credit institution prove less effective than expected.

Settlement Risk: The risk, that the credit institution will deliver the sold asset or cash to the counterparty and will not receive the purchased asset or cash as expected. As such a settlement risk comprises credit risk and liquidity risk.

Strategic risk: the current or prospective risk to earnings and capital arising from changes in the business environment and from adverse business decisions, improper implementation of decisions or lack of responsiveness to changes in the business environment.

Annex 2: Summary of the guidelines on the supervisory review process

Guidelines on Internal Governance

IG 1: Institutions should have a corporate structure that is transparent and organised in a way that promotes and demonstrates the effective and prudent management of the institution both on a solo basis and at group level.

IG 2: The reporting lines and the allocation of responsibilities and authority within an institution should be clear, precise, well-defined, transparent, coherent, and enforced.

IG 3: Institutions should ensure that the risk management function is organised in a way that facilitates the implementation of risk policies and the management of the institution's risks.

IG 4: The responsibilities of the management body should be clearly defined in a written document. They should include setting the institution's business objectives, risk strategies and risk profile, and adopting the policies needed to achieve these objectives.

IG 5: The management body should ensure that strategies and policies are communicated to all relevant staff throughout the organisation.

IG 6: The management body should systematically and regularly review the strategies and policies for managing the risks of the institution.

IG 7: The management body should develop and maintain strong internal control systems.

IG 8: The management body should ensure that internal control systems provide for adequate segregation of duties, in order to prevent conflicts of interest.

IG 9: The management body should set effective strategies and policies to maintain, on an on-going basis, amounts, types and distribution of both internal capital and own funds adequate to cover the risks of the institution. (See ICAAP section for further details.)

IG 10: The management body should monitor and periodically assess the effectiveness of the institution's internal governance structure.

IG 11: The management body should be active and independent, and should be able to explain its decisions to the supervisory authority and other interested parties.

IG 12: The management body should have policies for selecting, compensating, monitoring and planning the succession of key executives.

IG 13: The management body should promote high ethical and professional standards and an internal control culture.

IG 14: Institutions should establish, as a minimum, the following three primary functions in order to implement an effective and comprehensive system of internal control in all areas of the institution, namely (i) risk control function, (ii) compliance function, and (iii) internal audit function.

IG 15: The risk control function should ensure compliance with risk policies.

IG 16: The compliance function should identify and assess compliance risk.
IG 17: The internal audit function should allow the management body to ensure that the quality of the internal controls is adequate.
IG 18: There should be effective internal control systems and reliable information systems covering all significant activities of the institution.
IG 19: The management body should put in place appropriate internal alert procedures for communicating internal governance concerns from the staff.
IG 20: Institutions should aim for the highest standards of transparency in the conduct of their business.
IG 21: Each institution should present its current position and future prospects in a balanced, accurate and timely way.

Guidelines on ICAAP
ICAAP 1: Every institution must have a process for assessing its capital adequacy relative to its risk profile (an ICAAP).
ICAAP 2: The ICAAP is the responsibility of the institution.
ICAAP 3: The ICAAP's design should be fully specified, the institution's capital policy should be fully documented, and the management body (both supervisory and management functions) should take responsibility for the ICAAP.
ICAAP 4: The ICAAP should form an integral part of the management process and decision-making culture of the institution.
ICAAP 5: The ICAAP should be reviewed regularly.
ICAAP 6: The ICAAP should be risk-based.
ICAAP 7: The ICAAP should be comprehensive.
ICAAP 8: The ICAAP should be forward-looking.
ICAAP 9: The ICAAP should be based on adequate measurement and assessment processes.
ICAAP 10: The ICAAP should produce a reasonable outcome.

Guidelines on SREP
SREP 1: The SREP should be an integrated part of the authority's overall risk-based approach to supervision.
SREP 2: The SREP should apply to all authorised institutions.
SREP 3: The SREP should cover all the activities of an institution.
SREP 4: The SREP should cover all material risks and internal governance.
SREP 5: The SREP will assess and review the institution's ICAAP.
SREP 6: The SREP will assess and review the institution's compliance with the requirements laid down in the CRD.
SREP 7: The SREP should identify existing or potential problems and key risks faced by the institution and deficiencies in its control and risk management frameworks; and it should assess the degree of reliance that can be placed on the outputs of the institution's ICAAP.
SREP 8: The SREP will inform supervisors about the need to apply prudential measures.
SREP 9: The results of the SREP will be communicated to the institution at the appropriate level (usually the management body) together with any

action that is required of the institution and any significant action planned by the supervisory authority.
SREP 10: The supervisory evaluation should be formally reviewed at least on an annual basis, to ensure that it is up-to-date and remains accurate.

Guidelines on RAS
RAS 1: In order to carry out an overall assessment of an institution, the supervisory authority should define guidelines covering both risks and controls.
RAS 2: In order to assess an institution's risks and controls, the supervisor needs to prepare a breakdown of the institution's activities, down to the material business units or processes where risks are actually taken and where to a large extent controls are actually applied.
RAS 3: A Risk Assessment System should encompass all relevant risks and internal governance factors, while at the same time making a clear distinction between the two.
RAS 4: In order to make the results of all risk assessments comparable, both between the various institutions within a country and between countries, the results of the supervisory authorities' risk assessments should be based on an assessment of both quantitative and qualitative information.
RAS 5: Procedures for quality assurance should be in place in order to maintain the quality and consistency of risk assessments.
RAS 6: The supervisory authority should compare the results of the RAS with the outcome of the ICAAP and analyse their consistency.

Guidelines on the dialogue
Dialogue 1: Supervisors should have a methodology for structuring the dialogue with the institution so that they can systematically perform their own assessment of whether the capital held by the institution covers all material risks.
Dialogue 2: The structure of the dialogue should be based on a 'building block' approach.
Dialogue 3: Supervisors should use the dialogue with the institution to test and challenge the institutions' ICAAP and to exchange views, in order to reach a better understanding of the underlying assumptions and processes.
Dialogue 4: The frequency and depth of the dialogue will be determined by the supervisor, according to its assessment of the risk profile and/or systemic importance of each institution.

Guidelines on prudential measures
Measures 1: Prudential measures - to address issues identified either through the SREP or as part of ongoing supervision - should be applied promptly.
Measures 2: Prudential measures should be communicated promptly and in sufficient detail.