CESR/09-1176
CEBS 2009 299
CEIOPS-3L3-19-09

3L3 TASK FORCE ON INTERNAL GOVERNANCE (TFIG)

Cross-sectoral stock-take and analysis of internal governance requirements

Please note that the report had a cut off date as of October 2009

TABLE OF CONTENTS

PART A

1. EXECUTIVE SUMMARY AND MAIN FINDINGS OF THE REPORT

The "3L3 Task Force on Internal Governance" (TFIG), which is composed of experts from the banking, insurance and securities markets supervisors, was created with the aim of exploring ways of promoting greater convergence of regulatory and supervisory practices in the area of internal governance.

In its mandate, it committed itself to conduct a stock-take of the internal governance requirements applicable to some specific activities undertaken in the financial sector and to analyse them in order to (i) identify consequences of differences which have significant practical impact on institutions and make recommendations for Level 3 measures to enhance convergence; and (ii) develop cross-sector guidance for institutions operating in different financial sectors in the area of internal governance.

This report realises part of this commitment, as it contains the result of the stock-take that was performed by the TFIG on the existing requirements for entities[1] undertaking activities in the areas of banking, insurance and securities, and the subsequent analysis of the differences identified, as well as some proposed options to achieve the intended level of harmonisation.

The report is divided into three parts:

- **Part A**, which includes the present executive summary and the main findings of the work undertaken by the TFIG;
- **Part B**, which sets the background for the work undertaken by the TFIG (including its mandate, scope and framework) and TFIG's underlying approach (including a description of the building blocks adopted by the TFIG from those delineated in its preliminary report, issued in December 2008);
- **Part C**, which contains the detailed analysis by subject area. The report uses the building block approach designed to capture the key elements of an effective system of internal governance for each area considered and sets out for each the relevant requirements (with a summary table), the differences identified and their impact, and proposed harmonisation options that were designed to capture the key elements of an effective system of internal governance. The TFIG report attributes a "desirable degree of harmonisation" rating according to a scale of "low", "medium" or "high, for each of the issues covered by these building blocks.

The report also includes two annexes: **Annex I**, which contains the list of the material considered for the analysis, and **Annex II**, which summarises TFIG's view on the desirable degree of harmonisation for each area analysed.

[1] The use of the word "entity" throughout this report covers variously the terms "credit institution", "firm", "investment firm" and "undertaking" that are used in the directives TFIG has considered for its stock-take.

The results of the analytical work performed by the TFIG led it to conclude that the existing (or, in the case of insurance, perspective) internal governance requirements for the activities undertaken in the banking, insurance and securities sectors are generally similar and have the same intended outcomes or comparable outcomes, i.e. despite the fact that in many cases requirements are set at different levels of compliance, varying from European Level 1 directives to Level 3 guidance or recommendations, the final intention is approximately the same.

It was often observed that high-level principles for internal governance that are e.g. defined in the Level 1 directive for the insurance sector, are only detailed in Level 3 for the banking sector.

Some differences in the terminology used – or in its interpretation – were also identified, which the TFIG considers would benefit from some further standardisation to promote further convergence between sectors. The same applies to some general concepts, such as "proportionality" and "independence", that could be interpreted differently depending on the context.

When the requirements for each specific sector are analysed and compared, it is possible to conclude that there are in many areas common features, although they may be set at different levels of compliance (e.g. outsourcing). For other subjects, the provisions for a subject vary, according to the types of risks e.g. the banking and the insurance sectors specifically focus on, or the importance that e.g. the securities sector attributes to the management of conflicts of interest.

With regard to the differences between MiFID and CRD, further harmonisation of Level 1 and 2 provisions could be considered in order to reduce the number of different requirements for banks that also undertake investment activities.

As for the building blocks that were analysed by the TFIG, the main conclusions were as follows:

- Corporate structure and organisation (including management body): no major differences were identified regarding requirements for setting and organising the entities' organisational structure; however, some of the details that stem from the importance of the management of conflicts of interest for a securities business could be extended to other sectors;
- Risk management system: the general requirements relating to the management of risks and to the implementation of a system to support it are very similar between sectors; however, requirements on the detail of policies, processes and procedures for risk management could be further harmonised across all sectors;
- Internal control system: similar requirements for the implementation of an internal control system and the functions[2] that should support it exist; however, guidance

[2] Unless stated otherwise, the use of the word function along this report is made in the sense explicitly provided in the Level 1 Solvency II directive, i.e. a function is "an administrative capacity to undertake particular governance tasks" (Recital (18b)).

on what is meant by the independence of e.g. the compliance function or the internal audit function could be helpful;

- Supervisory review, internal reporting and public disclosure: while the requirements for reporting, both internally and externally, are broadly similar, with some differences justified by the different sectoral focus, the supervisory review process could benefit from a better aligned framework for the three sectors;
- Group structures and group specific issues: the existing differences between sectors are more or less covered by the Financial Conglomerates Directive; however, as the latter is under revision, the TFIG considers it is not appropriate to propose, for the time being, any type of recommendation in this area, although some harmonisation could be envisaged at a later stage.

None of the areas analysed by the TFIG was attributed a "high" desirable degree of harmonisation rating. However, several were rated as "medium" and the TFIG has chosen a set on which to focus attention, notably from those subjects referred to above.

2. SUMMARY OF MAIN RECOMMENDATIONS

The stock-take performed by the TFIG and the subsequent analysis of the differences identified in sectoral requirements enabled TFIG to attribute a "high", "medium" or "low" "desirable degree of harmonisation" rating to the issues covered under each of the building blocks described above.

While none of the subjects analysed by the TFIG was attributed a "high" desirable degree of harmonisation and therefore demands an immediate intervention, the TFIG considers that there are a number of areas where some guidance would be beneficial, including:

- Management of conflicts of interest;
- Policies, processes and procedures related to the risks covered by the risk management systems;
- How the risk management, compliance and internal audit functions might be "independent" in the light of their different sectoral requirements;
- The supervisory review process.

Accordingly, it is recommended to invite all interested parties to comment on whether cross sectoral convergence is needed in the above mentioned areas. This includes a view as to whether there are any conflicting rules and additional implementation burden due to differences in the regulation for the different financial sectors which need to be remedied.

The TFIG considers that the development of guidance in these areas would, on the one hand, contribute to a more harmonised interpretation of these requirements for each sector and,

on the other, complement the existing gaps between sectors in the cases where no specific requirements exist.

The TFIG would also like to highlight the fact that while some of the proposed new guidance could take into account existing Level 3 material, a consequence might be that some sectoral guidance would need to be replaced or revised.

For this purpose, a practical impact assessment seems desirable before any harmonisation steps are taken to clarify whether existing differences or gaps really harm the industry in practical terms compared to the cost of any changes to the regulatory environment by harmonising requirements.

PART B

3. BACKGROUND TO THE REPORT

3.1. MANDATE

The Three Level 3 (3L3) "Medium Term Work Programme" for 2008-2010 identified internal governance as one of six priority pieces of joint cross-sector work, for delivery by the end of 2010 (medium term)[3]. The aim was to explore ways of promoting greater convergence of regulatory and supervisory practices in this key area. To take this work forward, a Task Force on Internal Governance (TFIG), comprising members of banking, insurance and securities markets supervisors, was established.

The mandate for the work tasked the TFIG with:

- Developing cross-sector guidance for institutions and conglomerates operating in different financial sectors in the area of internal governance, within the current legal framework; and
- Identifying consequences of differences in internal governance requirements in sectoral legislation (both Level 1 and Level 2) which have significant practical consequences for institutions, and making recommendations for Level 3 measures to enhance convergence.

The scope, approach and timeline for the work were set out in the TFIG's Preliminary Report in December 2008, which was approved by the 3L3 Committees. The key elements of the approach were:

- To base the analysis on a "building block" approach, that is, to group internal governance requirements under a number of key headings to facilitate comparison between sectoral requirements;
- To identify the differences between those sectoral requirements (both in designation and in concept) and assess their significance; and
- Where significant, to recommend ways in which greater convergence could be achieved.

The basis of the analysis would be a "stock-take" of the internal governance requirements[4] in the Capital Requirements Directive (CRD), the Capital Adequacy Directive (CAD), the Markets in Financial Instruments Directive (MiFID) and the Undertakings for Collective Investment in Transferable Securities (UCITS) Directive, as well as relevant Level 3 measures produced by each of the Level 3 Committees. For (re)insurers, it would also include the

[3] "3L3 Medium Term Work Programme", November 2007 (http://www.ceiops.eu/media/docman/public_files/consultations/consultationpapers/3L3MediumTermWorkProgrammeCP.pdf)

[4] The details of the material referred to in this paragraph (and along the report) are provided in Annex I.

emerging text of the Level 1 directive (Solvency II), and the draft CEIOPS' advice to the European Commission (EU Commission) on Level 2 implementing measures (CEIOPS CP 33)[5].

3.2. SCOPE

The mandate of the TFIG, set out above, clearly establishes that the work to be developed should cover the legislative framework for entities within the EU internal financial market that develop activities in the fields of banking, insurance, securities and UCITS, as well as the field of financial conglomerates.

However, the TFIG has concluded that, for the time being, it should focus on issues related to the areas of banking, insurance[6] and securities. The reason for the narrowing of the initial scope is that both the UCITS directive and the Financial Conglomerates Directive (FCD) are being revised. Hence, the TFIG recommends that it should take account of relevant developments in these fields in due course.

In the case of financial conglomerates, the working group that was created, the FRWG (FCD Review Working Group), focussed also on internal control issues, which covers other internal governance aspects as well. The work of this group was recently subject to consultation[7].

The TFIG has also concluded that, to avoid duplicating other initiatives, this report will not at this stage cover two issues that would normally be included in the scope of internal governance, namely, "fit and proper" requirements and remuneration. "Fit and proper" requirements are the subject of a separate review by another 3L3 group, while remuneration is the subject of review by the EU Commission, a number of national supervisors, and by CEBS and CEIOPS. CEBS has issued some high-level principles on remuneration for banks[8], while CEIOPS consulted on a document on the same issue for insurers[9], which is consistent with the previous one. After the consulting period, CEIOPS will include some recommendations in its advice to the EU Commission on Level 2 implementing measures for Solvency II. The TFIG has concluded that it should, where appropriate, reflect the outcome of these initiatives in the present report.

---

[5] Only the material that is included in the "blue boxes" of CEIOPS' consultation papers containing draft advice to the Commission on Level 2 implementing measures is, for the purposes of this report, considered to be equivalent to Level 2 material.

[6] For the sake of simplicity, when referring to "insurance" both the insurance and reinsurance activities are covered.

[7] "Consultation on proposed solutions to address some issues noted in the Financial Conglomerates Directive", until 28 August 2009 (http://www.c-ebs.org/Publications/Consultation-Papers/All-consultations/3L3-Cross-sectoral/JCFC-09-10.aspx)

[8] "High-level principles for Remuneration Policies", 20 April 2009 (http://www.c-ebs.org/getdoc/34beb2e0-bdff-4b8e-979a-5115a482a7ba/High-level-principles-for-remuneration-policies.aspx)

[9] Consultation Paper no. 59 on "Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Remuneration Issues"

Despite the aspects that the TFIG tried to take into consideration for the development of recommendations, it considers that there are others that deserve being looked into more thoroughly in a near future. Among these are the issues related to the establishment of committees and the respective structures, as well as group issues, particularly where different group entities perform different financial activities.

3.3. INITIATIVES ON INTERNATIONAL AND EUROPEAN LEVEL AS A SEQUENCE OF THE CRISIS

Since the 3L3 Committees first agreed to include this work as a priority in their medium-term programme, and approved the mandate for the TFIG, financial markets have gone through a period of severe stress and turmoil. In considering the causes of the financial crisis, there is a general consensus that weaknesses and failures in governance in some banks and other financial institutions were a significant contributory factor. In considering their response to the crisis, authorities at national, European and international level are examining the case for strengthening regulatory frameworks and key regulatory requirements, including standards on governance.

In the area of governance, some important initiatives are in train which are relevant to the subject matter of this report. Among the more significant are:

- A review by OECD[10] of its "Principles of Corporate Governance"[11], due for completion in Autumn 2009;
- A review by the Basel Committee of its principles on corporate governance for banking organisations[12], due for completion in 2010;
- The development of an OECD/IAIS[13] project on corporate governance for insurers[14], which was under public consultation until the end of April 2009;
- Work by CEBS to review its standards and guidelines on internal governance and risk management[15]; and
- Work by the EU Commission to report on current corporate governance practices by the end of 2009.

At national level, in the UK the Turner Review highlighted key areas for improvement in standards of governance and Sir David Walker has been appointed by the UK Government to

[10] Organisation for Economic Co-operation and Development

[11] "OECD Principles of Corporate Governance", 2004 (http://www.oecd.org/dataoecd/32/18/31557724.pdf) and IAIS /OECD joint paper published in July 2009 regarding Corporate Governance Issues

[12] "Enhancing corporate governance for banking organisation", February 2006 (http://www.bis.org/publ/bcbs122.pdf)

[13] International Association of Insurance Supervisors

[14] "Issues Paper on Corporate Governance", Draft, 13 March 2009 (http://www.oecd.org/dataoecd/43/21/42366179.pdf)

[15] Consultation Paper on "High-level principles for risk management" (CP 24), Committee of European Banking Supervisors, 8 April 2009

report on ways in which standards of governance in banks and other financial entities could be strengthened[16]. His final report[17] will take into account responses to his consultation document published on 16 July 2009.

These activities focus principally on improvements in the following key areas: board practices, risk governance and management, remuneration and shareholder engagement. Addressing these issues involves consideration of the rights and duties that derive mainly from company rather than regulatory law, and which therefore strictly speaking fall outside the scope of this report. Where these reviews deal with the role and structure of functions, such as risk management, audit and other functions, and the responsibility of entities' senior management for their proper operation, the findings will be directly relevant to this report. The TFIG intends to take due account of relevant conclusions and recommendations in these areas in due course.

The TFIG is also mindful of the conclusions reached by the European Council in June on strengthening EU financial supervision, which endorse the earlier recommendations of the de Larosière Group[18].

3.4. INTERCONNECTIONS BETWEEN DIRECTIVES

As indicated above, the stock-take of internal governance requirements on which the analysis in this paper is based has compared the requirements in the Level 1 and 2 directives and associated Level 3 measures. However, the TFIG notes that there are significant interconnections between certain directives. In particular:

- Article 34 of the CAD, which applies Article 22 of the CRD and respective Level 3 measures to every investment firm that is not an exempt CAD firm; and
- Article 1(2) of MiFID, which applies the organisational requirements in its Article 13 (and in the Level 2 implementing directive) to credit institutions that carry on one or more investment services or activities.

The effect of this is that every investment firm that is not an exempt CAD firm is subject to both MiFID and CAD/CRD governance requirements, e.g. general risk management requirements, and consequently many banks are subject to both MiFID and CRD organisational requirements – at least in relation to the conduct of their securities business. The TFIG acknowledges that many entities or groups look to operate consistent organisational structures, policies and procedures across all business lines. As a consequence, differences in the governance requirements of the directives may, in practice, not result in inconsistent internal governance arrangements within individual entities or groups. On the other hand, those with a broad spread of business will need to consider

[16] Walker Review of Corporate Governance of UK Banking Industry (http://www.hm-treasury.gov.uk/walker_review_information.htm)

[17] Final Walker Report to be published on 26 November 2009,

[18] Report by the High-level group on financial supervision in the EU, 25 February 2009 (http://ec.europa.eu/internal_market/finances/docs/de_larosiere_report_en.pdf)

whether entity- or group-wide internal governance arrangements do in fact comply with the relevant requirements of MiFID, CRD and CAD, and their associated Level 3 measures.

Whether this presents a problem in practice may depend in part on how Member States have implemented these requirements. The TFIG understands that some Member States have, for example, addressed this issue by implementing the internal governance provisions of MiFID and CRD in a single, consolidated set of national requirements that apply to all of an entity's business. But this is not generally the case. The TFIG has, however, concluded that an assessment of the practical impact of the various national approaches to implementation of directive requirements is beyond the scope of this report.

The approach in this report has been to compare the internal governance requirements of the Level 1 and 2 directives on a stand-alone basis, i.e. as if each directive or set of requirements would apply exclusively to a specific type of business, such as banking, insurance or a securities-related activity. However, in considering whether differences between those requirements are significant enough to warrant a recommendation for further harmonisation, the TFIG has borne in mind the overlap between MiFID, CRD and CAD discussed above.

4. GENERAL APPROACH

4.1. THE CASE FOR HARMONISATION AND OPTIONS TO PROCEED

As outlined above, the main focus of this report is to compare the internal governance provisions in sectoral EU directives and relevant Level 3 materials for banking, insurance and securities entities, and to make recommendations for delivering a greater degree of convergence in EU regulatory standards. In approaching this task, the TFIG has borne in mind two key factors:

- The first is the need to maintain an appropriate balance between delivering harmonised standards, while maintaining justifiable sectoral differences on the other;
- The second is the need to consider carefully the means of delivering effective harmonisation where that is desirable on policy grounds.

On the first point, the directives that are the subject of this report cover the activities and services of a range of financial institutions – banks, insurers and reinsurers and investment firms. Many financial services groups have entities carrying on business in all three sectors. And banks – uniquely – can carry on both banking and securities businesses. However, the types of financial business and business model covered vary widely in range, scale and complexity. MiFID, for example, applies to broker-dealers and principal securities traders, stockbrokers and private wealth managers, institutional asset managers and financial advisers. To cater for this variety, the application of sectoral internal governance requirements is subject to the proportionality principle.

The application of the proportionality principle is usually related to a higher degree of flexibility in the implementation of certain legal or regulatory requirements, as long as the nature, scale and complexity of the activities undertaken by a certain entity, as well as the underlying risks, justify this adaptation. However, it is necessary to highlight that proportionality "works two-ways", i.e. in the same fashion, entities whose activities are more complex should also implement requirements in a more sophisticated manner. In any case, in the analysis of the requirements of the three sectors the existing proportionality considerations were taken into account[19].

In the response to the financial crisis, one of the key issues being considered by the initiatives mentioned in Section 3.3. (Initiatives on international and European level as a sequence of the crisis) is whether governance requirements for banks and other significant financial institutions, particularly those of systemic importance, should be more stringent than for other types of entity. In particular, for those entities (e.g. banks, insurers, securities traders) whose business models are based on risk-taking and pricing, effective enterprise-wide risk management and governance is recognised as essential to their very survival. Such considerations do not apply with the same force to those entities whose business models do not involve the taking of principal financial risk (for example, asset managers and advisers).

In considering the case for harmonisation, the TFIG has therefore considered whether there are valid arguments for differences in the substance of internal governance requirements to cater for differences between types of business model in a way that would not be adequately addressed by application of the proportionality principle.

Turning to the second point, in the present report the TFIG has analysed several internal governance aspects[20] in terms of the respective "desirable degree of harmonisation", and considered a classification scale composed of the levels "high", "medium" or "low". However, in the end, none of the items was attributed a "high desirable degree of harmonisation" (which would have been because existing requirements did not suffice or produce a similar effect).

A "low" desirable degree of harmonisation was attributed in those cases where the requirements – or their consequences – are largely similar or justifiable by sectoral specificities, or where no harmonisation seems to be necessary for the time being.

Although in the majority of the aspects analysed the differences reside in the detail and are not significant, the TFIG still believes that some work could be done in order to enhance harmonisation both in the interpretation and in the implementation of requirements. In these situations, as well as in others where the TFIG considers that some requirements could be extended to all the sectors, the desirable degree of harmonisation was set to "medium".

Where the TFIG pointed out that some level of harmonisation could be achieved, the available possibilities include the development of:

[19] Please refer also to Section 4.3.2..

[20] Please refer to Part B of the report.

- ***Legislation***: that is, amendment of Level 1 directives and/or Level 2 directives or regulations where relevant, including the Level 2 measures currently under consideration for Solvency II; and
- ***Guidance:*** that is, production or amendment of Level 3 guidance either by individual committees (CEBS, CEIOPS and CESR) or by the 3L3 committees together.

Elements of both could be used, of course, depending on the circumstances.

4.1.1. Legislation

The merit of the legislative route is that it would be an opportunity to create a consistent set of minimum mandatory standards applicable to all financial institutions regulated at European level. In some cases this option could be put in place in a very practical manner, which would be e.g. to extend MiFID rules to the other banking activities of banks that do securities business. In effect this is already a reality for some EU members that have applied the so-called "universal banking system", where MiFID and CRD regulations are applied simultaneously.

However, this could amount to a considerable programme of legislative change, which could be difficult to deliver. On the one hand, in the cases where directives are under revision (which is the case for CRD, FCD and UCITS), as well as in the case of Level 2 implementing measures for the insurance sector, when the TFIG delivers these conclusions it might be too late for them to be taken into account.

4.1.2. Guidance

Using Level 3 guidance to harmonise standards in targeted areas may be a more practical option, in that it might be easier to produce, and could be more flexible.

The issuing of sectoral individual Level 3 guidance seems to be adequate in the cases where the identified differences call for some degree of harmonisation in terms of the extension of existing requirements. It could also be used where requirements at Levels 1 and/or 2 are incomplete or inexistent for one or two of the analysed sectors. However, in these cases it has to be taken into account that Level 3 guidance cannot make up for lacking legal requirements on Level 1 or 2.

In some cases the TFIG has proposed that market-wide Level 3 guidance for the banking, insurance and securities sectors prepared by the 3L3 committees is developed. These proposals are related to aspects where the TFIG considers that a more coherent view of internal governance requirements is necessary.

The solution of developing Level 3 guidance – whether issued by the 3L3 or individual committees – has some drawbacks, however. The strongest arguments against this option

are the fact that guidance, by its very nature, is not legally binding[21] and the fact that the issues to be targeted would need to be given priority the 3L3 or relevant Level 3 Committee, and included in what are already full programmes of work. Additionally, account would also have to be made to the fact that in some sectors Level 3 material already exists, although some adjustments could have to be made.

Given the crucial importance of sound governance and internal control, both to the stability of individual entities and the financial sector in general, in the longer run there could be merit in an overarching 3L3 internal governance framework, drawing on existing or emerging sectoral standards and on the recommendations of the initiatives mentioned above, designed to apply to all financial institutions regulated at European level. A single set of provisions could better deliver consistent high-level standards, using the same concepts, language and expectations across the financial sectors. However, it is important to notice that such framework has to allow for different emphases between sectors where appropriate and therefore has to be on a high-level basis.

Nevertheless, this framework could be an important step in the direction of a "single rulebook", as envisaged by the European Council's June conclusions. Its adoption and implementation, including its relationship to the legislative framework, would be for the new European Supervisory Authorities and the new Steering Committee to consider in due course[22].

4.2. BUILDING BLOCK APPROACH

In its preliminary report, the TFIG agreed on a "building block approach", which should cover all areas in the context of internal governance for the whole legislative framework.

In order to define the appropriate set of building blocks to focus the analysis on, a reflection on the concept of internal governance had to be made. This is very often mistaken with the concept of corporate governance, but in the TFIG's opinion the latter has a wider scope. For the purposes of this report, "corporate governance involves a set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and its shareholders and should facilitate effective monitoring"[23]. As for internal governance, it

[21] In this particular case it is important to note that some Level 3 technical standards might become binding in line with the revised framework proposed both by the de Larosière Group and the European Commission (see footnote 18).

[22] In line with the European Commission's recommendation on "European financial supervision" (http://ec.europa.eu/internal_market/finances/docs/committees/supervision/communication_may2009/C-2009_715_en.pdf)

[23] See "OECD Corporate Governance Principles", as revised in 2004 (http://www.oecd.org/dataoecd/32/18/31557724.pdf)

"aims at ensuring that an institution's management body (…) is explicitly and transparently responsible for its business strategy, organisation and internal control. Internal governance is the responsibility of the management body (…). 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 (…) is organised"[24].

For setting the building blocks these aspects were grouped into three main blocks which the TFIG considers summarise what internal governance comprises: an adequate organisational structure, a risk management system and an internal control system.

Additionally, the effectiveness of the internal governance structure as a whole requires its supervision and revision, notably by the supervisory authority (under the supervisory review process).

Another key aspect that should be considered in the context of internal governance is whether the flow of information is adequate, both internally (e.g. between different hierarchical levels) and externally (to the supervisory authority, different stakeholders and the general public).

On this basis Part C of the report, which focuses on the analysis performed by the TFIG, was divided into the following building blocks:

- Corporate structure and organisation (including management body);
- Risk management system;
- Internal control system; and
- Supervisory review, internal reporting and public disclosure.

When entities are part of a group, there are also some specificities that should be accounted for. Consequently, an additional chapter that is subdivided into the four items referred above was also created to deal with group structures and group specific issues.

The chapters of the analysis under Part C are structured in a similar manner. For each detailed area, which corresponds to a section, a similar analysis was performed: the differences between sectors were identified and analysed and the desirable degree of harmonisation was set as "high", "medium" or "low" (in line with Section 4.1. on "The case for harmonisation and options to proceed").

Furthermore, each chapter contains a table which summarises the relevant material (requirements and/or recommendations) for each building block, as well as the respective nature. For the purpose of this table, the relevant material was classified into three different categories, each corresponding to a specific business area or type of activity. This categorisation was chosen to allow an easier interpretation of the table, as otherwise it would have to reflect the fact that e.g. the MiFID applies to the investment activities undertaken by banks, as underlined in Section 3.4. (Interconnections between directives) above.

[24] See "CEBS' Guidelines on the Application of the Supervisory Review Process under Pillar 2 (CP03 revised)"

What is considered to be relevant material in this report is the set of directives (both Levels 1 and 2 or equivalent) and Level 3 guidance that is specific to the banking, insurance and/or securities sectors. A list of this material is provided in Annex I (Relevant material).

Annex II of this report presents the summary of the desirable degree of harmonisation options as recommended by the TFIG.

4.3. GENERAL CONCEPTS AND OBSERVATIONS

Despite the detailed analysis that was performed for each building block and that is presented in Part C of the report, there are some general concepts and requirements applicable to all internal governance areas that should be highlighted.

4.3.1. The management body

The TFIG is aware of the fact that, due to differences in their domestic corporate law, governance and board structures differ across EU Member States. Yet, within each entity and regardless of the specific governance structure, there are two key functions that must be fulfilled: management and supervision. These functions can either be entrusted to a single body or spread over separate bodies.

In order to embrace the different board structures that exist in Member States, this paper utilizes the concept of "management body". This concept is theoretical and purely functional, used for the sole purpose of defining guidance and principles irrespective of specific governance structures. According to this concept, the management body encompasses the management function and the supervisory function[25]. Therefore, for the most part, the paper will address the management body as a whole and not refer to a specific function. To decide which function of the management body the tasks and responsibilities addressed in this paper are assigned to, and which internal body of the entity represents the supervisory and which the management function, is ultimately up to each national authority.

Sound internal governance requires that the decision-making process be clearly stated within each entity, in terms of hierarchy and level of responsibility. The management body may delegate some of its tasks. It can also allocate certain functions, under its responsibility, to a committee or other body, instituted within the management body itself. The paper will not expand on further delegations and allocations of tasks, which remain a sole matter of organisation[26].

[25] Please note that these guidelines thus apply this term in a broader interpretation than the more limited use of the term in the context of e.g. Annex VII of Directive 2006/48/EC (CRD).

[26] Such delegation can be to senior management, which term is used amongst others in various parts of Directive 2006/48/EC. CEBS does not attempt to define this concept, as it is used in various interpretations in the EU context (as well as in the global context). The term "management body" is used in these guidelines for the sake of convenience and consistency. It is not intended to cut across the allocation of responsibilities in the

However, the management body carries full and complete responsibility for both abovementioned functions, irrespective of the delegation or allocation of tasks and functions.

4.3.2. Proportionality

The proportionality principle, already commented on in Section 4.1. (The case for harmonisation and options to proceed), is applicable to most of the requirements on internal governance entities are subject to, independently of the sector(s) in which they operate. However, the concept may be interpreted in different manners depending on the sector.

The concept of proportionality, as laid down in the provisions of the CRD and Solvency II, also applies to internal governance and its policy. This means that the internal governance framework of an entity should be related to the nature, scale and complexity of its activities.

Furthermore, supervisory authorities will adapt their supervisory approach to ensure it is proportionate to the nature, scale and complexity of the activities of an entity. Similarly, the depth, frequency and intensity of the supervisory evaluation will be determined by the risks posed to the supervisor's statutory objectives of ensuring the soundness of the financial system as a whole and the protection of the end-customers, such as depositors, policyholders and investors.

Supervisors will be open to explanations from entities as to how differing approaches would still meet the aims of the guidelines, i.e. there is no "one-size-fits-all" approach. In any case, it is important to stress that, under Solvency II, the principle of proportionality does not justify the non-application of any sort of requirements, i.e. it does not exempt any entity from its obligation, but conversely allows for their proportionate application.

In MiFID, the proportionality principle is dealt with slightly differently than in the CRD and Solvency II. In the first case, the wording is often "shall where appropriate and proportionate". It is, however, dealt with in different ways in different subtitles of internal governance, which are mentioned along the report.

4.3.3. Requirements set at different levels across sectors

Another general remark that can be drawn from the stock-takes and their subsequent analysis is that, for the majority of the internal governance aspects that were analysed, many requirements are set at different levels in different sectors[27]. In particular, in the

CRD (in particular Annex VII), including the requirements as to who should understand and approve the IRB (Internal Ratings Based) and AMA (Advanced Measurement Approach) models.

[27] This affirmation is not totally correct. In effect, as CRD has the characteristics of Lamfalussy Level 1 and 2 measures, but is not a full Lamfalussy directive, strictly speaking the terms "Level 1", "Level 2" or "Level 3" cannot be used in the case of the banking sector and of investment firms subject to the CRD and CAD in the same manner as it is used for the other two sectors. However, and in order to allow for comparability between the legislation in force for the three sectors, both the CRD and the CAD relevant articles are considered

banking sector many requirements are based on the broad concepts of Articles 22 and 123 of the CRD, but are only elaborated in more detail on Level 3. In any case, while in a few cases that impact could be significant, in most situations it is not, as the key aspect is that (at least) issues are dealt with.

4.3.4. Differences in terms and concepts across sectors

Differences in the terms and concepts used were also identified. On the one hand, there does not seem to be a clear reason why different terms were used for the same aspects. On the other hand, there does not seem, for the majority of the internal governance requirements, to be an interpretation problem where the terms are different but equivalent. Hence, the existing language differences are, in practical terms, not relevant.

The TFIG acknowledges that some of these differences are related to the specificities of each sector and the businesses undertaken, having necessarily an impact in internal governance requirements. However, setting internal governance requirements at different levels and using different terminology might result in confusion or visible differences among individual sector regulations and recommendations and might recall for some effort on harmonisation.

Consequently, and in line with the rationale developed in Section 4.1. (The case for harmonisation and options to proceed), in the following part of the report the TFIG presents its analysis of the identified differences and proposes some harmonisation options.

equivalent to a Level 1 directive, while their annexes are considered as corresponding to Level 2 implementation measures in the referred above logic.

PART C

This part of the report sets out the detailed analysis, findings and recommendations under the "building block" approach described under Section 4.2..

5. CORPORATE STRUCTURE AND ORGANISATION (INCLUDING MANAGEMENT BODY)

This chapter focuses on the organisational aspects related to internal governance, such as the principles to be applied to the corporate structure of the entities, as well as requirements related to the management body.

The following table summarises the relevant material applicable to entities in the context of corporate structure and organisational matters, as well as the respective nature[28].

Area	Relevant material (by activity/business)		
	Banking	**Insurance**	**Securities**
Lines of responsibility and accountability (including supervision and monitoring arrangements)	Level 1: **CRD**: Article 22 Level 3: **CEBS SRP**: IG 1, IG 2, IG 6, IG 8, IG 10, IG 18	Level 1: **Solvency II**: Articles 40, 41(1) Level 2: **CEIOPS CP 33**: §3.24; §3.26	Level 1: **MiFID**: Article 13(2)&(3) Level 2: **MiFID Implementing Directive**: Articles 5, 9
Conflicts of interest	Level 1: **CRD**: Article 22 Level 2: **CRD:** Annex V, §1 Level 3: **CEBS SRP**: IG 8 **CEBS Liquidity Risk**: Recommendation 3 **CEBS AMA/IRB**: §451-461	Level 1: **Solvency II**: Article 41(1) Level 2: **CEIOPS CP 33**: §3.25	Level 1: **MiFID**: Article 13(3)
Tasks and responsibilities of the management body	Level 1: **CRD**: Article 22 Level 2: **CRD**: Annex V, 1(§1) Level 3: **CEBS SRP**: IG 4-IG 13	Level 1: **Solvency II**: Article 40 Level 2: **CEIOPS CP 33**: §3.24(b)	Level 1: **MiFID**: Article 9(1) Level 2: **MiFID Implementing Directive**: Articles 5, 9

[28] In this table, as well as in the similar tables that are presented in all chapters, only material that has a direct impact for each area is identified.

Area	Relevant material (by activity/business)		
	Banking	**Insurance**	**Securities**
Record keeping and data quality aspects	Level 1: **CRD**: Articles 22, 29(1st sub-§), 63(1)(a)&(b), 87(12) (2nd sub-§), 109 Level 2: **CRD**: Annexes III (Part 6, §27-28), VII (Part 4, 5.1. and 5.2.); VIII (Part 3, §16); X (Part 3, 1.1.(§4), 1.2.2.(§13-18) and 1.2.3.(§19)), XII Level 3: **CEBS SRP**: IG 18(b)	Level 1: **Solvency II**: Articles 35(5), 54(1) Level 2: **CEIOPS CP 33**: §3.24(i)&(j); §3.67 **CEIOPS CP 43**	Level 1: **MiFID**: Articles 13(5)&6), 25(2) **CAD**: Articles 30(2), 31(1st sub-§(e) & 2nd sub-§), 32(1)(3rd sub-§), 35 Level 2: **MiFID Implementing Directive**: Article 5(1)(f)
Accounting systems and procedures	Level 1: **CRD**: Articles 22, 63, 109 Level 3: **CEBS SRP**: IG 8	Level 1: **Solvency II**: Article 45 Level 2: **CEIOPS CP 33**: §3.67	Level 1: **MiFID**: Article 13(5) Level 2: **MiFID Implementing Directive**: Article 5(4)
"Four eyes" composition	Level 1: **CRD**: Article 11(1)	Level 1: **Solvency II**: Article 42	Level 1: **MiFID**: Article 9(4)
Committees and subcommittees and their terms of reference	Level 2: **CRD**: Annex VII, Part 4 Level 3: **CEBS SRP**: IG 6, RAS 4	Level 2: **CEIOPS CP 56**: §4.49	-
Outsourcing	Level 3: **CEBS Outsourcing**	Level 1: **Solvency II**: Articles 38, 48 Level 2: **CEIOPS CP 33**: §3.343-3.348	Level 1: **MiFID**: Article 13(5) Level 2: **MiFID Implementing Directive**: Articles 13, 14, 15

5.1. LINES OF RESPONSIBILITY AND ACCOUNTABILITY

5.1.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3)[29]:	**Banking**	**Insurance**	**Securities**
Have an organisational structure with well defined, transparent and consistent lines of responsibility	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 41(1))	**Level 1** (MiFID Art. 13(2))

[29] The purpose of this table – as well as of the equivalent tables that are presented along the report – is to provide a generic idea of what sort of requirements exist for each of the three activities/businesses and what is the highest level at which these are set. Hence, a reference to existing e.g. Level 1 material does not imply that no Level 2 or Level 3 material also exists.

Entities shall (Levels 1 and 2) or should (Level 3)[29]:	Banking	Insurance	Securities
Have an organisational structure with documented lines of responsibility	**Level 3** (CEBS SRP IG 2, 4, 8)	**Level 2** (CEIOPS CP 33 §3.24(b))	**Level 2** (Impl. MiFID Art. 5(1)(a))
Have an organisational structure with a clear and precise allocation of responsibilities and authority	**Level 3** (CEBS SRP IG 2, 4, 8)	**Level 1** (SII Art. 41(1))	**Level 2** (Impl. MiFID Art. 5(1)(a))
Have an organisational structure that establishes, implements and maintains decision-making procedures	**Level 3** (CEBS SRP IG 8)	**Level 2** (CEIOPS CP 33 §3.24(f))	**Level 2** (Impl. MiFID Art. 5(1)(a))
Have an organisational structure that ensures that all personnel are aware of the procedures for the proper discharge of their responsibilities	**Level 3** (CEBS SRP IG 2, 5)	**Level 2** (CEIOPS CP 33 §3.24(e))	**Level 2** (Impl. MiFID Art. 5(1)(b))
Have an effective system for ensuring the transmission of information	**Level 3** (CEBS SRP IG 18)	**Level 1** (SII Art. 41(1))	**Level 1** (MiFID Art. 13(5))
Have a system that establishes, implements and maintains effective internal reporting and communication of information at all relevant levels	**Level 3** (CEBS SRP IG 2, 5, 18)	**Level 2** (CEIOPS CP 33 §3.24(a))	**Level 2** (Impl. MiFID Art. 5(1)(e))
Have a system of governance that is subject to regular internal review	**Level 3** (CEBS SRP IG 10)	**Level 1** (SII Art. 41(1))	**Level 2** (Impl. MiFID Art. 5(5))
Have a system of governance that is proportionate to the nature, scale and complexity of the operations and/or activities of the company	**Level 1** (CRD Art. 22(2))	**Level 1** (SII Art. 41(1))	**Level 2** (Impl. MiFID Art. 5(1))

Entities operating in the banking, insurance and securities sectors are all required to have a governance structure that has well defined, transparent and consistent lines of responsibility. The differences in each sector's requirements amount to variations in text rather than in outcome.

One difference identified concerns the obligation to ensure that areas of responsibility and authority are also sufficiently clear and transparent for any reporting lines that deviate from the entity's legal structure, which is applied only to the banking sector by the CEBS SRP (IG 2).

Some rules or guidelines are phrased in a more detailed or explicit way in one sector than in the others. For example, the obligation to have an organisational structure with appropriate segregation of responsibilities or duties is well described in the CEBS SRP (IG 8), applicable to the banking sector, and in Solvency II (Article 41), for the insurance sector, but is less clearly described for the securities sector, where Article 13(3) of MiFID provides that an entity "shall maintain and operate effective organisational and administrative arrangements with a view to taking all reasonable steps designed to prevent conflicts of interest".

The most important difference concerns the level at which the rules or guidelines are provided. Most of the rules covered by Level 1 and Level 2 provisions in the insurance and securities sectors are provided by Level 3 guidelines in the banking sector, based on Articles

22 and 123 of the CRD. However, and as referred in Subsection 4.3.3. (Requirements set at different levels across sectors), this feature is common to most internal governance requirements.

5.1.2. Analysis of the differences

Although detailed requirements in the banking sector are only set up in non-binding Level 3 guidance, while requirements in the insurance and securities sectors are regulated on a higher level (Level 1 or Level 2), the general conclusion is that these issues are covered across sectors.

As for the wording differences between the requirements, these are not significant, as they have little impact on the outcomes.

5.1.3. Harmonisation options

Desirable degree of harmonisation	**Low**	

Since the creation of lines of responsibility and accountability is not sector-specific but closely connected with the nature, scale and complexity of the entity's structure the TFIG thinks it could be desirable to harmonise the provisions relating to the creation of lines of responsibility and accountability.

In effect, to have common regulations on the same level, which would imply developing 3L3 guidance, would be the ideal solution. The advantage of Level 3 guidance is that it provides more detailed guidelines on how to create lines of responsibility and accountability within entities.

5.2. CONFLICTS OF INTEREST

5.2.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Have an organisational structure with a clear allocation and appropriate segregation of responsibilities or effective organisational and administrative arrangements with a view to taking all reasonable steps designed to prevent conflicts of interest	**Level 3** (CEBS SRP IG 8)	**Level 1** (SII Art. 41)	**Level 1** (MiFID Art. 13(3))

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Have written conflicts policies	**Level 2** (CRD Annex V, 1(§1))	-	**Level 2** (Impl. MiFID Art. 22)
Make disclosures to clients where organisational measures are insufficient to deliver the intended outcome	-	-	**Level 1** (MiFID Art. 18(2))
Identify and record types of conflicts that could arise	-	**Level 2** CEIOPS CP 33 §3.25	**Level 2** (Impl. MiFID Art. 23)
Take into account the principle of proportionality	**Level 1** (CRD Art. 22(2))	**Level 1** (SII Art. 41(2))	-

Conflicts of interest can exist in all types of entities, although these are particularly risky in a financial context, due to the systemic risks involved, the nature of the business and frequent group structure, and the volumes at stake. An effective management of conflicts is a key element of any internal governance system, both to protect the interests of an entity's clients and to maintain market confidence.

In this respect, both the banking and the insurance sectors have regulations in place that refer to adequate or appropriate "segregation of duties" or "segregation of responsibilities", while MiFID explicitly states that an entity should put in place "effective organisational and administrative arrangements with a view to taking all reasonable steps designed to prevent conflicts of interest". That is, that the purpose is to manage conflicts of interest in order to prevent them from adversely affecting the interests of an entity's clients. There is no equivalent statement of purpose in the CRD or in Solvency II.

Requirements designed to deliver this outcome are spelled out in some detail in MiFID at both Levels 1 and 2, as can be inferred from the table above. Additionally to those, MiFID also specifies what administrative arrangements must include, as a minimum, focusing on independence between business areas, separate supervision of relevant staff, and controlling incentives that could arise from inappropriate remuneration policies. It also requires entities to set out in a written policy the main conflicts they face, and the measures adopted to manage them.

By contrast, under the CRD there are few explicit requirements on conflicts of interest, beyond high-level expectations that they should be managed: it is for the management body to define arrangements for "the segregation of duties in the organisation and the prevention of conflicts of interest", and to ensure their internal control system delivers this. There is no explicit reference to disclosure as an appropriate control mechanism.

Under Solvency II there is no comprehensive statement of an entity's obligations in relation to the management of conflicts of interest. Only at Level 2 the proposed advice recognises that conflicts of interest may be an issue in small entities where management of conflicts by segregation of duties may not be feasible, and calls for "additional controls". CEIOPS CP 33 §3.24 also contains more details about segregation of responsibilities.

MiFID also covers the management of conflicts of interest that can arise:

- In the production by an entity of "independent" investment research for its clients; and
- Between the interests of a regulated market or its owner or operator, and the sound functioning and efficiency of the market and the interests of market participants.

Being securities sector-specific issues, these matters are naturally not addressed in banking and insurance requirements, and are not considered further in this analysis.

5.2.2. Analysis of the differences

It is likely that the more detailed approach in MiFID, compared to CRD and Solvency II, has two main explanations.

First, MiFID has consumer protection as one of its main objectives. Measures to protect consumers from the effects of conflicts of interest in investment firms have long been an objective of EU securities markets law.

Secondly, in recent years there has been significant regulatory focus on particular types of conflicts in investment firms: for example, conflicts between proprietary trading and corporate finance activities; between investment research departments and sales trading/advice; and between portfolio management and securities trading functions. In particular, there has been concern that disclosure, often generic and/or overly legalistic, has been inadequate as a means of delivering effective consumer protection. Hence, the greater focus in MiFID on organisational and administrative measures to manage conflicts.

The lack of specificity in banking and insurance legislation may well reflect the "prudential" focus of CRD and Solvency II. These directives have a different approach to the MiFID. Whereas CRD and Solvency II address e.g. legal, operational and reputational risks, the MiFID intends to protect the confidence of the investors in the functioning of the capital markets and aims to strengthen consumer protection. However, it is possible that the more granular approach to risk management in these directives addresses some of the risks to the business that might otherwise arise through failure to control or manage conflicts of interest. It is also the case that banks providing MiFID services will be subject to the MiFID conflicts of interest provisions, and they may decide to apply those provisions across the whole business of the entity.

Other identified difference concerns the lexicon. While the CEBS SRP uses the expression "segregation of duties", Solvency II uses the wording "segregation of responsibilities". However, the outcome is the same and consequently no amendment seems to be necessary in this regard.

5.2.3. Harmonisation options

Desirable degree of harmonisation	Medium	

There could be merit in exploring the case for articulating a clearer statement of purpose for tackling conflicts of interest in banking and insurance regulation and there may also be a case for importing some of the more specific MiFID provisions, particularly the requirement to have a written conflicts of interest policy.

Realistically, for this to happen, a case would need to be made for including changes of this nature in the CRD review programme, and the Solvency II Level 2 programme. Before this could be done, a business case for change would also need to be constructed. This would at least need to show that the risks that the MiFID approach seeks to address are not dealt with adequately by alternative organisational and governance measures in the banking and insurance fields.

On the other hand, the major source of conflicts of interest that is likely to arise in a banking or insurance context relates to the adequate balance that should be established between the performance of individual units and the remuneration of their employees. Although remuneration issues are outside of the scope of the present report (as referred in Section 3.2. on "Scope"), the TFIG would like to highlight, in this context, the importance of having a coherent remuneration framework for the three sectors.

For the reasons stated above, this is one of the issues that the TFIG considers requires the development of cross-sectoral guidance.

5.3. TASKS AND RESPONSIBILITIES OF THE MANAGEMENT BODY

5.3.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Define the allocation of tasks and responsibilities:			
• To an entity	**Level 1** (CRD Art. 22(1))	-	**Level 1** (MiFID Art. 13(1))
• To an entity's management body	**Level 2** (CRD Annex V, §1)	**Level 1** (SII Art. 40)	**Level 2** (Impl. MiFID Art. 9(1))
Have a management body with the ultimate responsibility for the compliance with laws, regulations and administrative provisions	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 40)	**Level 2** (Impl. MiFID Art. 9(1))

Entities shall (Levels 1 and 2) or should (Level 3):	Banking	Insurance	Securities
Have the responsibilities of the management body clearly defined in a written document. These should include setting the entity's business objectives, risk strategies and risk profile, and adopting the policies needed to achieve these objectives	**Level 1** (CRD Art. 22(1))	**Level 2** (CEIOPS CP 33 §3.24(b))	**Level 2** (Impl. MiFID Art. 5(1)(a))
Have a management that develops and maintains a strong internal control system	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 45)	-

The requirements for banking and securities entities are similar in content, but vary from being addressed to the entities themselves or to the management body[30]. For insurers, Article 40 of Solvency II makes it clear that the administrative or management body of an undertaking is ultimately responsible for compliance with internal governance requirements.

Another difference is that the "ensuring a strategy" and "know-your-structure" requirements are stressed more in the banking sector, mainly because of the principles on corporate governance for banking organisations issues by the Basel Committee[31]. The first requires that the management body should align its corporate structure with the risk-appetite and the internal governance system of the bank. The second is that the management body should understand the operational structure of the entities, including the environment where the bank operates, and the risks that may arise from that structure.

These high-level requirements are self-explanatory and intrinsic as principles for all sectors. Furthermore, the financial crisis has shown that compliance with these principles is fundamental, though it has not been implemented at European level yet. Therefore, in the TFIG's opinion they need to be stressed as general principles on a cross-sectoral basis.

In the context of the tasks and responsibilities of the management body, there are two other aspects that deserve a more detailed analysis: those related to record keeping and data quality aspects and the establishment of accounting systems and procedures. However, and for functional reasons, these are dealt with in the following sections of the report.

5.3.2. Analysis of the differences

Prior to Solvency II, there appeared to be no consistent use within the sectors or across the sectors of the terminology used to identify management structures. In some cases the terminology used is different, though it appears that the same entity's representatives are meant (and sometimes the same term is used, but the context indicates a different meaning).

[30] The TFIG recalls the concept of "management body" defined in Subsection 4.3.1. (The management body).

[31] Please refer to footnote 12.

The TFIG understands that this inconsistency was discussed during Solvency II negotiations, culminating in Article 40 described above. As a consequence, all the internal governance requirements set out in Articles 41 to 48 of Solvency II are addressed to undertakings and there is no doubt where responsibility for complying with them lies (and by implication associated Level 2 measures). The focus is therefore rightly on the obligations in the individual subject areas of governance and no longer who in the entity might or might not be held responsible for ensuring compliance with them.

No equivalent or similar approach however exists for the banking or securities areas, leading to the referred above situation where requirements vary from being addressed to the entities themselves or to the management body.

Additionally, the requirement to align the governance system and risk appetite with the strategy of an entity and the "know-your-strategy" principle are basic internal governance issues that should prevail for all entities and not only for credit institutions. They should therefore be set out explicitly also for the insurance and securities sectors[32].

5.3.3. Harmonisation options

Desirable degree of harmonisation	**Medium**	

Article 40 of Solvency II approach is sensible, pragmatic and above all simple and it would therefore be helpful to carry it across to the banking and securities sectors. For the avoidance of doubt, a similar provision could be introduced to the Level 1 text for the other two sectors, since their aim is undoubtedly the same in internal governance.

As the "know–your-structure" principle and the risk-alignment objective of the Basel Committee are not yet implemented, the most reasonable solution would be to insert them on Level 1. For the time being, however, the most feasible alternative appears to introduce these principles on Level 3.

5.4. RECORD KEEPING AND DATA QUALITY ASPECTS

5.4.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Maintain adequate and orderly records of their business and internal organisation	**Level 1** (CRD Art. 22(1))	**Level 2** (CEIOPS CP 33 §3.24(i))	**Level 2** (Impl. MiFID Art. 5(1)(f))

[32] Please refer to page 40 of OECD analysis "Corporate Governance and the Financial Crisis: Key Findings and Main Messages", June 2009 (http://www.oecd.org/dataoecd/3/10/43056196.pdf)

Entities shall (Levels 1 and 2) or should (Level 3):	Banking	Insurance	Securities
Establish, implement and maintain an adequate business continuity policy aimed at ensuring, in the case of an interruption to their systems and procedures, the preservation of essential data and functions	**Level 1** (CRD Art. 22(1))	-	**Level 2** (Impl. MiFID Art. 5(3))
Have written policies on the appropriateness of information	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 35(5), Art. 54(1))	-
Implement suitable processes and procedures to ensure the reliability, sufficiency and adequacy of both the statistical and accounting data	**Level 1** (CRD Art. 22(1))	**Level 2** (CEIOPS CP 33 §3.67)	-
Safeguard the security, integrity and confidentiality of information	**Level 1** (CRD Art. 22(1))	**Level 2** (CEIOPS CP 33 §3.24(j))	**Level 2** (Impl. MiFID Art. 5(2))
Retain records for a pre-specified period of time	**Level 1** (CRD Art. 22(1))	-	**Level 1** (MiFID Art. 25(2))

As referred in the previous section, issues related to record keeping and data quality aspects should be dealt within the context of the tasks and responsibilities of the management body, as this holds the responsibility of such a task. Although this attribution of responsibilities is not obviously expressed in the relevant material applicable to this issue (except for the insurance sector, because of Article 40), the previous section highlights that, in practical terms, the attribution of a responsibility to the entity itself, which is the case for both the banking and the securities sectors, ultimately rests with the management body.

For the banking sector, in the context of record keeping a visible emphasis is put on large exposures records. Article 109 of the CRD sets a general requirement for credit institutions to identify and record all large exposures and subsequent changes to them. Additionally, for IRB[33] institutions (CRD Annex III, Part 6, §28) an explicit track record is required in models' use, while for AMA[34] institutions this is required for internal loss historical data (CRD Annex X, Part 3, §14). However, it can be observed that the CRD does not impose a general obligation to maintain adequate and orderly records of the business and of the internal organisation for banks.

In the case of insurance, there is no explicit requirement for record keeping in Solvency II, but a requirement for ensuring the on-going appropriateness of the information submitted to the supervisory authorities. CEIOPS CP 33 tackles the issue of record keeping and the implementation of suitable processes and procedures to ensure the reliability, sufficiency and adequacy of both the statistical and accounting data. More specific requirements related to the criteria for the assessment of quality of data used for the valuation of technical provisions are also provided for in CEIOPS' Level 2 advice on standards for data

[33] IRB stands for "Internal Ratings Based" under the CRD.

[34] AMA stands for "Advanced Measurement Approach" under the CRD.

quality[35]. In this document, requirements related to the quality of data (§3.55-3.81), the implementation of a system for the management of data quality (§3.69-3.73) and the implementation of procedures for the collection, storing and processing of data (§3.74-3.77) are set.

In the case of securities, MiFID requires keeping records of all services and transactions undertaken and further specifies the data to be kept and a holding period of at least five years. The MiFID Implementing Directive goes beyond this and states that investment firms shall maintain adequate and orderly records of their business and internal organisation (identical to CEIOPS CP 33) and also deals with business continuity policy concerning data.

5.4.2. Analysis of the differences

Only legislation for the securities business provides a clear holding period for data, which is not referred in the other directives applicable to the banking and insurance activities, and provides a provision concerning the safeguarding of essential data in the case of an interruption to systems and procedures. On the other hand, only for the insurance business there is an explicit reference to processes and procedures to ensure the reliability, sufficiency and adequacy of both the statistical and accounting data.

However, the main difference seems to be that insurance and securities legislation have a wide and identical understanding regarding record keeping, as records of the internal organisation have to be kept, whereas no such general rule exists for the banking business. One reason for this difference between sectors might be that record keeping, in particular the one related to transactions in financial instruments, is also important for consumer protection, which is one of the main objectives of MiFID.

5.4.3. Harmonisation options

Desirable degree of harmonisation	**Medium**	

Convergence between the three sectors could be enhanced in a sensible way by updating CEBS SRP Level 3 guidance, including a provision to maintain orderly records of the business and the internal organisation. The existing sector requirements, such as those related to the recording of large exposures, would obviously remain valid.

[35] Consultation Paper no. 43 on "Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Technical Provisions – Article 85 f – Standards for Data Quality"

5.5. ACCOUNTING SYSTEMS AND PROCEDURES

5.5.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Have (sound) administrative and accounting procedures	**Level 1** (Art. 22(1))	**Level 1** (Art. 45(1))	**Level 1** (Art. 13(5))
Establish, implement and maintain accounting policies and procedures that enable them to deliver financial reports which reflect a true and fair view of their financial position and which comply with all applicable accounting standards and rules	-	-	**Level 2** (Art. 5(4))
Take into account the principle of proportionality	**Level 1** (Art. 22(2))	-	-

As referred in Section 5.3. (Tasks and responsibilities of the management body), and in line with the previous section, issues related to the implementation of accounting systems and procedures should be dealt with in the context of the tasks and responsibilities of the management body. However, this deserves a more detailed analysis.

From the table above it is possible to infer that all sectors require appropriate and sound administrative and accounting procedures. However, it should be noted that Solvency II includes this provision in the context of the implementation of an internal control system.

In the case of securities, the MiFID Implementing Directive, at Level 2, provides (in Art. 5(4)) further detail on the accounting policies and procedures that should be established that enables investment firms to deliver financial reports in a timely manner.

In terms of sector-specific requirements, it should be noted that the CRD stresses the concept of own funds to cover banking risk and that these should be properly registered in the internal accounting records.

5.5.2. Analysis of the differences

The general provision stated in each of the referred directives is rather similar and is set in the context of high-level requirements regarding governance arrangements.

As for the differences described above, these result from the specificities of the activities held in each sector and are not significant from a harmonisation point of view, except for the fact that only the CRD explicitly refers to the application of the principle of proportionality in this context. However, the general principles underpinning Solvency II and MiFID seem to imply that no such a specific requirement is necessary, as the principle of proportionality should be applied where appropriate.

5.5.3. *Harmonisation options*

Desirable degree of harmonisation	**Low**	

There are no material sectoral differences, as the common features are the requirements to have "sound administrative and accounting procedures".

5.6. "FOUR EYES" COMPOSITION

5.6.1. *Differences identified*

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Have their management undertaken by at least two persons	**Level 1** (CRD Art. 11(1))	**Level 1** (implicitly)	**Level 1** (MiFID Art. 9(4))
Have a management of sufficiently good repute and sufficiently experienced to ensure the sound and prudent management of the entity	**Level 1** (CRD Art. 11(1))	**Level 1** (SII Art. 42)	**Level 1** (MiFID Art. 9(1))
Have sole trader exemption	-	-	**Level 1** (MiFID Art. 9(4))

The CRD explicitly requires the banking business to be effectively directed by at least two persons of sufficient good repute and experience. No exceptions are allowed.

The same requirement applies to securities entities, though the wording is slightly different. However, a securities entity may be a sole trader (a natural person or a legal person managed by a single natural person) provided it has alternative arrangements in place which ensure sound and prudent management of the entity. This latter requirement is by way of derogation and the extent to which it is significant in practice depends on whether Member States have exercised it.

Solvency II does not have an explicit "four eyes" requirement, although it could be inferred, from Chapter IV (Conditions governing business) of the directive proposal that a sole trader is not permitted[36].

[36] In order to make this requirement explicit, in its final Level 2 advice to the European Commission for implementing measures related to the system of governance, CEIOPS' will add a provision determining that at least two persons should be indicated as being those who effectively run the undertaking (in the context of general governance requirements).

5.6.2. *Analysis of the differences*

There seems to be a common aim for all three directives: to ensure that, with the exception of securities entities that are sole traders, no entity is to be run by just one person. This may be for practical reasons because of the complexity of the business and the expertise needed to run it effectively and/or to prevent an entity being run by one dominant individual.

On the other hand, Article 11 of the CRD applies to all credit institutions and leaves no room for exceptions to small local entities with low risk profile, which proved to be relatively stable during the recent financial crisis.

5.6.3. *Harmonisation options*

Desirable degree of harmonisation	**Low**	

No harmonisation seems to be required in this field, as CEIOPS is going to include this specific requirement in its Level 2 advice to the EU Commission on the "System of governance".

5.7. COMMITTEES AND SUBCOMMITTEES AND THEIR TERMS OF REFERENCE

5.7.1. *Differences identified*

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Have an audit committee[37]	**Level 1**	**Level 1**	**Level 1**
Consider what committee structure is appropriate, if this facilitates the development and maintenance of good governance practices	**Level 3** (CEBS SRP IG 6)	-	-
Designate a credit committee responsible for the financial institution's rating systems (IRB banks only)	**Level 2** (CRD Annex VII, Part 4, §124)	-	-

[37] In this case the reference is not any of the Level 1 directives (i.e. CRD, CAD, Solvency II, MiFID) or the MiFID Implementing Directive, but Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC. Although the TFIG had decided that only directives specific to the sectors under analysis would be considered as relevant material (see introduction of Part C), this particular aspect seems to deserve a wider approach.

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Set up an internal control committee for the internal model (for (re)insurers using internal models)	-	**Level 2** (CEIOPS CP 56 §4.49)	-

The only requirement for the setting up of committees or subcommittees that is common to all sectors is related to the obligation for "public-interest entities" to have an audit committee, provided for in Article 41 of Directive 2006/43/EC.

In addition to this requirement, Level 3 guidance for banks let these consider what committee structure is appropriate, if this facilitates the development and maintenance of good governance practices. In the case of IRB banks, these are challenged to designate a credit committee responsible for the financial institution's rating systems.

Although in the case of the insurance sector the CEIOPS CP 33 (§3.13) refers the fact that the administrative or management body should consider whether a committee structure is appropriate in the context of the system of governance, this idea is not included in CEIOPS' Level 2 advice to the EU Commission (i.e. in the document's "blue boxes"). However, this could indicate that Level 3 guidance may be developed regarding this issue.

The only requirement that seems likely to exist for the insurance sector is the need to set up a committee for the revision of the internal model, for (re)insurance undertakings that have developed one. This is reflected in CEIOPS CP 56, which contains the proposed Level 2 advice for the approval of internal models[38].

5.7.2. Analysis of the differences

Only the banking and the insurance sectors mention options to set up designated committees in very specific cases: for banks, in order to address all material aspects related to the IRB approach, as well as risk management, if these committees facilitate the development and maintenance of good governance practices, and for insurers if these have developed internal models.

Then again, there is a mention about the existence of various committees within a credit institution as a helpful tool for supervisory authorities regarding the review and evaluation process of the risk assessment systems (e.g. asset and liabilities committee or credit committee).

[38] Consultation Paper no. 56 on "Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Articles 118 to 124 – Tests and Standards for Internal Model Approval"

5.7.3. *Harmonisation options*

Desirable degree of harmonisation	Low	

Considering that the existing references to committees and/or subcommittees are sector-specific, except for the referred above Directive 2006/43/EC, the only way to reach harmonisation would be to develop some requirements or guidance for all sectors.

On the one hand, it would seem sensible to develop Level 3 guidance, as several committees with the same or very similar functions already exist for entities operating in each sector, such as remuneration, ALM or risk management committees, among others. This could give evidence to the need to regulate committees on Level 3.

On the other hand, there are some committees which are more likely to be sector-specific, such as rating system committees or credit committees. Additionally, the establishment of committees, their duties, the delegation of powers and the limits of this delegation are elements of corporate law and there could be some reluctance in introducing this kind of elements in the sectoral regulation.

Hence, the TFIG considers it sensible to conclude that the desirable degree of harmonisation in this case is low for the time being. However, the regulatory developments that might result from the lessons learnt from the crisis (see Section 3.3. on "Initiatives on international and European level as a sequence of the crisis") may lead to the need of revisiting this recommendation.

5.8. OUTSOURCING

5.8.1. *Differences identified*

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Notify/inform the supervisory authorities regarding the outsourcing of critical, important or material functions or activities, as well as of any subsequent material developments with respect to those activities	**Level 3** (CEBS Outsourcing Guideline 4.3)	**Level 1** (SII Art. 48(3))	-
Make available on request to the competent authority all information necessary to enable the authority to supervise the compliance of the performance of the outsourced activities with the applicable requirements	**Level 3** (CEBS Outsourcing Guideline 11)	**Level 1** (SII Art. 38(1)(b))	**Level 2** (Impl. MiFID Art. 14(5))

Entities shall (Levels 1 and 2) or should (Level 3):	Banking	Insurance	Securities
Be ultimately responsible for the proper management of the risks associated with outsourcing/discharging its obligations	**Level 3** (CEBS Outsourcing Guideline 2)	**Level 1** (SII Art. 48(1))	**Level 2** (Impl. MiFID Art. 14(1))
Never outsource critical, important or material functions or activities in a way as to impair materially the quality of their internal governance and the ability of the supervisor to monitor the entity's compliance with its obligations	**Level 3** (CEBS Outsourcing Guideline 4)	**Level 1** (SII Art. 48(2))	**Level 2** (MiFID Art. 13(5))
Define the outsourcing arrangements in a written agreement/contract	**Level 3** (CEBS Outsourcing Guidelines 8&9)	**Level 2** (CP 33 §3.347)	**Level 2** (Impl. MiFID Art. 14(3))
Exercise due skill, care and diligence when entering into, managing or terminating any arrangement for the outsourcing to a service provider of critical, important or material functions or activities	**Level 3** (CEBS Outsourcing Guidelines 6&8)	**Level 2** (CP 33 §3.346-3.347)	**Level 2** (Impl. MiFID Art. 14(2))

Likewise in other areas, the requirements related to outsourcing are set out at different levels of European legislation[39]. Whereas for insurance and securities the binding requirements for outsourcing are regulated on Levels 1 and 2, for the banking sector a non-binding guideline on Level 3 is established.

However, the existing requirements are, in practical terms, rather similar, as can be inferred from the table above.

It is important to highlight that the notification requirement is different in all three sectors: while the CEBS Outsourcing guidelines suggest that an outsourcing entity should take particular care when outsourcing material activities and should inform its supervisory authority accordingly, Solvency II requires that entities give prior notice – although this does not imply a pre-approval. For the securities sector notification is only required under certain conditions laid down in the MiFID Implementing Directive related to service providers located in third countries.

It should also be referred that in the case of the MiFID Implementing Directive (Article 13) there is a list of exclusions for the concept of outsourcing.

5.8.2. Analysis of the differences

The main purpose of the regulation is the same for all sectors. Outsourcing of core management board functions shall by no means lead to an "empty mailbox" scenario where no clear responsibility structure exists, as the delegation of functions or activities by way of outsourcing shall, by no means, imply a delegation of the entity's – or of its management

[39] Please refer to Section 4.3.3. (Requirements set at different levels across sectors).

body – responsibilities. The powers and/or decisions of the management body of the entity cannot, in any case, be outsourced.

Legislation in all three sectors distinguishes between material activities or critical or important functions and non-material activities or non-important functions. Whereas the underlying definitions for material and non-material functions/activities are equivalent in all sectors, the requirement of notification is treated differently in the securities sector. The MiFID Implementing Directive states that entities shall make information available to the competent authority only on request, whereas CEBS Outsourcing and Solvency II additionally stipulate a notification obligation.

The reason for not introducing a notification requirement in the securities sector was the "reduction of bureaucracy", which would consequently avoid an overburden both on supervisors and entities. However, the supervisory authority can have access to the information related to the outsourced activities upon request.

Finally, since the outsourcing requirements are set at different levels across the sectors, it might be worth to consider whether outsourcing requirements for banking activities should be stipulated on the regulatory Level 1 or 2 in order to enhance legal security and consistency among the three sectors or whether there is no need for a change in level if the outcome is the same.

5.8.3. Harmonisation options

Desirable degree of harmonisation	**Medium**	

To gain harmonised legal requirements for outsourcing in all three sectors, one option could be to introduce the notification requirements for the MiFID Implementing Directive. It is difficult to see any specific reasons for treating the notification requirement differently. The purpose of notification is equivalent in all sectors: to give supervisors the opportunity to assess outsourcing plans of material, critical or important functions beforehand to exercise their expertise in a way that ensures outsourcing compliance with the legal provisions. The supervisor does not have to approve or authorise the outsourcing. Rather the prior notification presents an opportunity for the supervisor to discuss concerns with the entity. Therefore, there should be enough time for the supervisor to examine the proposed outsourcing before it comes into force.

However, it should be thoroughly evaluated whether amendments to the MiFID Implementing Directive are appropriate for the time being, as this directive has been brought forward only recently. Consequently a harmonisation attempt should – if at all – only be considered at a later stage, i.e. in the context of an overall reset round of revisions of the directives in force.

Another option would be to change CEBS Guidelines Outsourcing (notably Guideline 4.3., second sentence, which reads "the outsourcing institution should adequately inform its supervisory authority about this type of outsourcing", referring to material outsourcing, and to introduce instead the equivalence of Article 14(5) of the MiFID Implementing Directive whereby entities "make available on request to the competent authority all information necessary to enable the authority to supervise the compliance of the performance of the outsourced activities with the requirements" of the directive. This option is comparatively simpler, as it just requires a change in Level 3 guidance. It would harmonise MiFID and CRD under this matter and be in accordance with the statement of the EU Commission[40] whereby the MiFID and its implementation directive are of higher ranking. However, under this option the insurance and banking/securities sectors would be treated differently, although there seems to be no sectoral-specific reason for that.

Furthermore, it has to be considered that if information about outsourcing is available to the competent authority on request only, it cannot be ensured that the competent authority has knowledge of all relevant information in that regard in a standardised, continuous, and up to date way. From this point of view, the first option seems to be preferable and changes at a later stage should be considered on Levels 1 or 2 of MiFID.

6. RISK MANAGEMENT SYSTEM

This building block focuses on the aspects related to the implementation of a risk management system, including the analysis of the requirements related to the risks that it should cover. It also includes aspects related to business continuity and stress testing being part of the risk management framework in financial institutions.

The concept of a "risk management system" is not straightforward and may be misinterpreted. Some material refers to it with the terminology "enterprise risk management", while in some other cases this is a part of an entity's internal control system.

For the purposes of this report, the risk management system is a set of rules, processes and procedures which enable an entity to adequately identify, assess, monitor, measure, manage, report and control the risks it is or could be exposed to.

The following table summarises the relevant material applicable to entities regarding risk management systems, as well as the respective nature.

[40] Please refer to the European Securities Committee working document ESC/35/2006 (http://ec.europa.eu/internal_market/securities/docs/esc/meetings/2006-06-26-report_en.pdf)

Area	Relevant material (by activity/business)		
	Banking	**Insurance**	**Securities**
Implementation of a risk management system	Level 1: **CRD**: Articles 22, 84, 109, 123 **CAD**: Article 34 Level 2: **CRD**: Annex V, §2; Annex IX, Part 4, §43(g); Annex X, Part 2, §12; Annex X, Part 3, §1-7 Level 3: **CEBS SRP**: IG 3, IG 6, IG 9, IG 14 **CEBS CP24** **CEBS Liquidity Risk**: Recommendation 3 **CEBS AMA/IRB**: §468, §473-476, §482-487, §615	Level 1: **Solvency II**: Articles 43, 44 Level 2: **CEIOPS CP 33**: §3.53	Level 1: **MiFID**: Article 13(5)(2nd sub-§) Level 2: **MiFID Implementing Directive**: Articles 7 and 13(2)
Risk management function	Level 1: **CRD:** Article 84 Level 2: **CRD:** Annex V, §2; Annex IX, Part 4, §43(g); Annex X, Part 3, §3; Annex XII, Part 2, §1(b) Level 3: **CEBS CP24:** §19-26	Level 1: **Solvency II**: Article 43(4)-(5) Level 2: **CEIOPS CP 33**: §3.190-3.192 CEIOPS CP 56 §4.47-4.51	Level 2: **MiFID Implementing Directive**: Article 7(2)
Risks covered by the risk management system	Level 2: **CRD**: Annex V, §3-15 Level 3: **CEBS SRP**: Annex 1	Level 1: **Solvency II**: Article 43(2)&(3) Level 2: **CEIOPS CP 33**: §3.67-3.69; §3.82-3.85; §3.108-3.113; §3.119-3.120; §3.128-3.129; §3.143-3.146; §3.158-3.161; §3.169-3.170	-

Area	Relevant material (by activity/business)		
	Banking	**Insurance**	**Securities**
Risk assessment and stress testing	Level 1: **CRD**: Article 114 Level 2: **CRD**: Annex III, Part 6, §24, §32-33; Annex VII, Part 4 §40-42, 115(g), 127; Annex VIII, Part 3, §16(g), §50; Annex X, Part 3, §11, Annex XI, §1(a)(g); Annex XII, §10(a)(ii) **CAD**: Annex V, §2(g) Level 3: **CEBS SRP**: ICAAP 7, ICAAP 8 **CEBS Liquidity Risk**: Recommendation 8, Recommendation 14, Recommendation 24, Recommendation 27 **CEBS Stress Testing**	Level 1: **Solvency II**: Articles 43(1), 44(2), 50(1)(c), 103, 104(1), 122 (for internal models) Level 2: **CEIOPS CP28**: § 3.65-3.92 **CEIOPS CP 33**: §3.119 **CEIOPS CP 39** **CEIOPS CP 47**: §4.11-4.12, §4.26-4.29, §4.46-4.50, §4.72-4.82, §4.93-4.96, §4.133-4.170, §4.177 **CEIOPS CP 48**: §3.66-3.116 **CEIOPS CP 49**: §3.23-3.47, §3.48-3.52, §3.70-3.72, §3.85-3.86, §3.97-3.98, §3.159-3.169, §3.117-3.119 **CEIOPS CP 51**: §3.88-3.124 **CEIOPS CP 53**: §3.36-3.41 **CEIOPS CP 56**: §5.223, §5.252, §5.255, §8.158-8.165	-
Business continuity	Level 2: **CRD**: Annex V, §13 Level 3: **CEBS SRP**: IG 18	Level 1: **Solvency II**: Article 41(3a) Level 2: **CEIOPS CP 33**: §3.27-3.28	Level 1: **MiFID**: Article 13(4) Level 2: **MiFID Implementing Directive**: Articles 5(3), 13(1), 14(2)(g)

6.1. IMPLEMENTATION OF A RISK MANAGEMENT SYSTEM

6.1.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Have effective procedures to manage the risks the entity is or could be exposed to	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 43(1))	**Level 1** (MiFID Art. 13(5))
Establish, implement and maintain adequate (written) risk management policies	**Level 2** (CRD Annex V, §2)	**Level 1** (SII Art. 41(3))	**Level 2** (Impl. MiFID Art. 7(1)(a))
Establish a risk management function	**Level 2** (Annexes IX, X, XII)	**Level 1** (SII Art. 43(4))	**Level 2** (Impl. MiFID Art. 7(2))
Take into account the principle of proportionality	**Level 1** (CRD Art. 22(2))	**Level 1** (SII Art. 41(2))	-

The provisions for implementing a risk management system, in the terms defined above, are broadly similar for the three sectors.

The high-level requirements in MiFID and the MiFID Implementing Directive, Solvency II and CEIOPS CP 33, as well as CRD and its Annexes, require an entity to have adequate strategies, policies and procedures to control all the risks the entity faces and effectively manage them. Solvency II has far more detail at Level 1, including sector-specific requirements for internal models, and consequently CEIOPS CP 33 is more comprehensive. The CRD requirement in this area is embedded in Articles 22 and 123, with related requirements for specific risks in the Annexes. As for MiFID, the requirement is much more general, as it refers to "effective procedures for risk assessment", though it could be assumed that the risks are those that the entity faces or could have to face.

Regarding the definition of risk management policies for the banking business, it is important to highlight that the CRD sets requirements for this in the context of the management of concentration risk. However, only in Annex V of the CRD a more general requirement exists.

In addition to the information presented in the table above, it is important to highlight that while in the case of the banking and securities activities the risk management system is explicitly embedded in the internal control activities, for (re)insurers Solvency II describes this as a system *per se*.

6.1.2. Analysis of the differences

Solvency II has more detail at Level 1 than either of the other two directives, which are more high-level. However, the banking and the securities businesses have similar requirements at Level 2 and Level 3 and consequently the outcome is approximately the same in practice.

6.1.3. Harmonisation options

Desirable degree of harmonisation	**Low**	

While the detail differs, the high-level aims are similar. It therefore seems unnecessary to seek to harmonise the Level 1 text in this area.

6.2. RISK MANAGEMENT FUNCTION

6.2.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Establish a risk management function	**Level 2** (CRD Annexes IX, X, XII)	**Level 1** (SII Art. 43(4))	**Level 2** (Impl. MiFID Art. 7(2))
Establish an independent risk management function	**Level 3** (CEBS CP 24 §20, §24)	-	**Level 2** (Impl. MiFID Art. 7(2))
Require that the risk management function reports to the "top" hierarchy of the entity	**Level 3** (CEBS CP 24 §20)	**Level 2** (CP 33 §3.191)	**Level 2** (Impl. MiFID Art. 7(2)(b), Art. 9(2))

Solvency II and MiFID require the establishment of a risk management function where this is proportionate, i.e. dependent on the nature, scale and complexity of the entity's business and the risks it faces. MiFID requires an entity that does not establish such a function to show its risk management system remains effective and specific regulatory requirements are met. Solvency II has no similar requirement[41], which may be explained by the difference in these directives as to the meaning of "function": in MiFID it is a dedicated unit, while in Solvency II it means "an administrative capacity to undertake particular governance tasks"[42]. Both directives state how a risk management function has to be established and what its purpose is – including, in Solvency II, sector-specific internal models material.

However, CRD is silent on the establishment of a separate risk management function other than in sector-specific circumstances, such as the use of internal risk measurement methods for regulatory capital calculation for market risk, credit risk (IRB) and operational risk (AMA). A risk management function is also generally mentioned in Annex XII of the CRD, in the context of disclosure. Explicitly, the establishment of a risk management function is required on Level 3 in the CEBS CP 24, where in contrast to the insurance and securities sector its role and function is even further elaborated.

[41] Although under Solvency II there is not a requirement for an independent risk management function, in its final Level 2 advice to the European Commission, CEIOPS will include a provision related to the predefined key functions (i.e. risk management, compliance, internal audit and actuarial) where these should have "an appropriate standing in terms of organisational structure".

[42] Accordingly to the Recital (18b) of Solvency II: "A function is an administrative capacity to undertake particular governance tasks. The identification of a particular function does not prevent the undertaking from freely deciding how to organise this function in practice unless this is otherwise specified in this Directive. This should not lead to unduly burdensome requirements because account should be taken of the nature, complexity and scale of the operations of the undertaking. These functions can therefore be staffed by own staff or can rely on advice from outside experts or can be outsourced to experts within the limits set by this Directive."

CEBS SRP (IG 3) also explicitly refers to a risk management function organised in a way that facilitates the implementation of risk policies and managing risk within the institution.

It is important to mention that CEBS CP 24 does not assign control tasks to the "risk management function", which should not be confused with the "risk control function" as presented in CEBS SRP (IG 14 and IG 15)[43].

6.2.2. Analysis of the differences

As described in the previous section ("Implementation of a risk management system"), while the aims of the three directives may appear similar in terms of the general framework, the requirements for the risk management function differ between them.

The CRD itself is silent with regard to governance aspects, except in particular circumstances, but requirements are posed on institutions by CEBS CP 24. As for Solvency II and MiFID, these vary as to the detail of their wording, their approaches and the different level of requirement. There are other differences in how the functions should operate, not all explained by the difference in approach between the directives.

There is generally a requirement to report to the "top" level of its entity, though there are slight differences in wording: Solvency II speaks of administrative or management body (in line with Article 40), CEBS SRP and CEBS CP 24 speak of management body (both supervisory and management functions) and MiFID speaks of senior management and supervisory function. However, in practical terms there does not seem to exist a significant difference.

More importantly, there are gaps and/or inconsistencies in the directives such as whether and how the risk management function should be independent from and/or interact with the other (obligatory and dedicated) functions (internal audit in Solvency II, the compliance function in MiFID), and their respective tasks.

6.2.3. Harmonisation options

Desirable degree of harmonisation	**Medium**	

There are some key areas which deserve further analysis.

[43] In the context of the CRD and its related guidance, it is possible to make a distinction between the two concepts. The "Risk control function" is one of the primary functions (as compliance function and internal audit) in order to implement an effective and comprehensive system of internal control. The risk control function should ensure compliance with risk policies working independently from the business lines it monitors and controls. As for the "Risk management function", this implements the risk policies and manages risk within the entity, including ongoing identification, measurement and assessment of all material risks that could adversely affect the achievement of the entity's goals.

First, the requirement to have a risk management function, which for the banking sector is only addressed explicitly on Level 3. Consistency in this regard could only be achieved by amending the relevant Level 1 or 2 texts, as the existence of mandatory requirements is the only real way of achieving convergence.

Secondly, the difference in language as to whom the function should report. This may not be essential and could fall away as a consequence of the recommendations for the tasks of the management body and/or reporting.

However, there is scope for useful Level 3 guidance on setting out how the risk management function may or may not interact with other functions and the implications for their independence and objectivity. In this context, some questions could arise:

- Does "functions independently" (MiFID) mean the same as "the function is objective" (CEIOPS CP 33) or "the risk management function is independent from the operational units whose activities they review" (CEBS CP 24)?
- When should an entity have a risk management function?
- When and how may a risk management function interact with other functions without compromising its independence/objectivity? For example, can someone exercising the risk management function also perform other tasks outside the scope of this function?

Guidance could also cover the tasks of the risk management function including a clear distinction in relation to the "risk control function". The CEBS CP 24 could usefully be taken into account.

For the reasons stated above, this is one of the issues that the TFIG considers requires the development of cross-sectoral guidance.

6.3. RISKS COVERED BY THE RISK MANAGEMENT SYSTEM

6.3.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Manage the risks the entity is or could be exposed to	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 43(1))	**Level 1** (MiFID Art. 13(5))

In terms of Pillar II, the CRD requires an entity to manage all the risks it is or might be exposed to, taking into account the principle of proportionality. There is no explanation of which risks or risk types have to be covered. However, Annex V sets outs requirements for aspects of some risks (credit, counterparty, concentration, securitisation, market, interest rate arising from non-trading activities, operational and liquidity risks).

Solvency II states explicitly that the risk management system to be implemented by undertakings should cover the risks that are included in the calculation of the SCR (Solvency Capital Requirement)[44], i.e. life underwriting risk, non-life underwriting risk, health underwriting risk, market risk, credit risk and operational risk, as well as other areas referred to in Article 43(2), including among others liquidity risk, for which a risk management policy should be developed.

CEIOPS CP 33 advice covers each of the risks set out in Article 43 and has explanatory text on credit risk, reputational risk and strategic risk (though only the first it suggests should result in Level 2 related text). Where the advice covers risks also covered by CRD, for example, liquidity and operational risks, the underlying definition is consistent. The main focus of the advice is the policies and processes/procedures entities should have for the risk rather than the risk itself.

MiFID has no risk specific material, except for the general requirement to have "effective procedures for risk assessment".

6.3.2. Analysis of the differences

Some differences exist regarding the scope to which the risk management system applies. The CRD is generally targeted at all risks an entity is or might be exposed to – taking into account the nature, scale and complexity of the activities and without imposing further prescriptions which risks or risk types have to be covered, whereas MiFID is designed to ensure a high level of investor protection and to promote confidence in the market.

Besides generically referring to the risks an entity is or could be exposed to, Solvency II focuses on the risks that are quantifiable and therefore considered under the SCR. Additionally, it also contains specific requirements to address the risks that are not covered by the SCR standard formula, such as e.g. reputation or strategic risks. However, these differences seem to be justifiable by the business undertaken in each of the cases and insignificant in practice.

As for the other material, this appears to be sector-specific.

6.3.3. Harmonisation options

Desirable degree of harmonisation	**Medium**	

The differences in the directives are largely sector-specific, so a high level of harmonisation appears inappropriate.

[44] As defined in Article 101 of Solvency II.

However, where the same risk is covered explicitly by different directives (e.g. operational risk), there may be grounds for harmonisation at Level 3 as to what the relevant policies, processes and procedures might be for those risks. When doing this, different approaches (e.g. AMA, TSA[45], BIA[46] for operational risk) should be taken into account for calculating the capital requirements existing, which go together with different qualitative requirements.

For the reasons stated above, this is one of the issues that the TFIG considers requires the development of cross-sectoral guidance.

6.4. RISK ASSESSMENT AND STRESS TESTING

6.4.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Use stress tests (explicitly) as a validation method	**Level 1** (CRD Art. 22(1), Art. 123)	**Level 2** CEIOPS CP 56 §8.158-8.165)	-
Carry out risk assessment analysis and/or stress tests for different purposes:	-	**Level 1** (SII Art. 43(1), Art. 44(2), Art. 103, Art. 104(1))	-
• Credit-risk concentrations/concentration risk	**Level 1** (CRD Art. 114(3))	**Level 2** (CEIOPS CP 47 §4.133-4.170)	-
• Market risk	**Level 2** (CAD Annex V)	**Level 2** (CEIOPS CP 47 §4.26-4.29 (interest rate); §4.46-4.50; §4.72-4.82; §4.93-4.96;)	-
• Counterparty credit risk (CCR) or counterparty default risk	**Level 2** (CRD Annex III, Part 6, §32-33)	**Level 2** (CEIOPS CP 28 §3.65-3.92; CEIOPS CP 51 §3.88-3.124)	-
• Liquidity risk	**Level 3** (CEBS Liquidity Risk)	**Level 2** (CEIOPS CP 33 §3.119)	
• Operational risk	**Level 2** (CRD Annex X, Part 3, §11)	**Level 2** (CEIOPS CP 53 §3.36-3.41)	-

[45] TSA stands for "Standardised Approach", as for the CRD.

[46] BIA stands for "Basic Indicator Approach", as for the CRD.

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
• Life insurance risk	-	**Level 2** (CEIOPS CP 49 §3.23-3.47; §3.48-3.52; §3.70-3.72; §3.85-3.86; §3.97-3.98; §3.156-3.169; §3.117-3.119)	
• Underwriting risks	-	**Level 2** (CEIOPS CP 48 §3.66-3.116)	-
Provide the scope of the stress tests	**Level 1** (CRD Art. 114)	**Level 2**[47] (CEIOPS CP 56 §8.158-8.165)	-
Define an appropriate frequency of validation (stress tests), which may be on regular basis/once a year or when the risk profile changes	-	**Level 2**[48] (CEIOPS CP 56 §8.158-8.165)	-
Report the results of the stress tests	**Level 2** (CRD Annex XI, §1)	**Level 1** (SII Art. 50(1)(c)&(e)(ii))	-

In the case of the banking sector a specific Level 3 guidance exists dealing with the issue of stress tests. CEBS Guidelines on Stress Testing[49] contains guidelines on CRD requirements with respect to stress testing in terms of risk management and for the assessment of capital adequacy. As mentioned in the respective executive summary, "they aim to provide some clarification in relation to stress testing as part of CEBS's guidelines on the application of the supervisory review process (SRP). Accordingly, they will be implemented as part of the SREP/ICAAP dialogue and should not be interpreted as resulting in automatic capital add-ons". The application of these guidelines is subject to the proportionality principle taking into account the size, sophistication and diversification of the activities.

These guidelines cover (i) the definition and uses of stress testing (diagnostic tool and forward looking); (ii) the methodology of sound stress testing, including its review and update; and (iii) the provision of an overview of the stress testing by risk categories (market risk, credit risk and liquidity risk).

As for insurers, there are several Consultation Papers containing advice on Level 2 implementing measures that deal with the issue of risk assessment and stress testing. These requirements stem from the Level 1 directive (Article 34(4)), which states that "Member States shall ensure that supervisory authorities have the power to develop, in addition to the calculation of the Solvency Capital Requirement and where appropriate, (…) necessary quantitative tools under the supervisory review process to assess the ability of the insurance

[47] In the cases where the SCR is calculated using the standard formula the previous references include this scope. References are thus not included here in order to facilitate the reading of the table.

[48] Please refer to the previous footnote.

[49] CEBS due to consult on its proposed updates to its Stress Testing Guidelines, CP32 on 14th December 2009

or reinsurance undertakings to cope with possible events or future changes in economic conditions that could have unfavourable effects on their overall financial standing. The supervisory authorities shall have the power to require that such tests are performed by the undertakings". The references above mostly refer to the description of formulas or scenarios of the standard formula or used in internal models for each risk. In practice, this is the setting of the stress tests embedded in the formula for the calculation of the SCR (both using the standard formula or an internal model).

No such requirements exist for the securities sector.

6.4.2. Analysis of the differences

The performance of stress tests for the insurance sector is not explicitly mentioned in Solvency II. However, a general validation should be carried out for technical provisions and for the capital requirement calculated both by an internal model or the standard formula. More details are provided in CEIOPS' Level 2 draft advices for implementing measures, although in many cases references are made to "scenario analysis" or "risk assessments".

In the particular case of the validation of technical provisions (e.g. assumptions on non-linearity, quality of estimation, tail distributions) different tools can fit better to the different purposes. Hence, stress tests for insurers are only one of the recommended tools existing for the time being at Level 2 (e.g. for credit risk, ALM risk, market-to-model valuation), although they are not required, except for the case of liquidity issues. The performance of these tests also depends on the availability of data.

Credit institutions are obliged to apply the stress tests mentioned explicitly in the CRD for credit risk concentration (Article 114) and at Level 2 for the internal methods (counterparty credit risk, market risks, credit risks, LGD[50] in IRB, effects of credit risk mitigation, securitisation, and operational risk). The liquidity risks shall also be dealt with credible validation tools. However, the stress tests are not mentioned explicitly in CRD and, as referred before, only in Level 3 recommendations (CEBS Liquidity Risk and CEBS Stress Testing).

It should also be noted that in the banking sector stress tests are also applied in the scope of sensitivity analysis, while this is not the case in the insurance or in the securities sectors (at least explicitly). However, this seems to be no more than a matter of terminology. In this context, the insurance Level 2 advice differentiates between simple shocks, more complex scenarios and reverse stress tests (scenario that could threaten the entity's survival).

The MiFID does not deal with the stress tests issue or with validation methods, referring to the banking regulations as far as capital requirements are considered.

[50] LGD stands for "Loss Given Default", as defined under the CRD.

6.4.3. *Harmonisation options*

Desirable degree of harmonisation	**Low**	

The identified differences seem to be justifiable by the specificities of each sector. Consequently, there does not seem to exist a case for harmonisation.

6.5. BUSINESS CONTINUITY

6.5.1. *Differences identified*

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Implement contingency and/or business continuity plans that allow the entity to operate on an ongoing basis and/or continuously and regularly	**Level 2** (CRD Annex V, §13)	**Level 1** (SII Art. 41(3a))	**Level 1** (MiFID Art. 13(4))
Implement contingency and/or business continuity plans that allow the entity to limit losses in the event of severe business disruption	**Level 2** (CRD Annex V, §13)	-	-
Establish, implement and maintain an adequate business continuity policy	-	-	**Level 2** (Impl. MiFID Art. 5(3))
Take into account the principle of proportionality	-	**Level 1** (SII Art. 41(3a))	**Level 1** (MiFID Art. 13(4))

Although high-level requirements to implement contingency and/or business continuity plans are generically equivalent, where the main purpose is to ensure the continuity of the activity, it should be noted that in the case of the insurance and securities directives the terminology is actually the same ("continuity" and "regularity" of the provision of services/performance of activities), while in the banking sector the term "ongoing basis" is used.

CEIOPS CP 33 refers to the need of regularly testing and updating the existent business continuity plans, and the MiFID Implementing Directive also requires the definition of a business continuity policy, including some detailed rules on Level 2, as well as some specificities related to the particular case of outsourcing.

In the case of the banking sector, the only additional requirement (at Level 3) is related to the management of information technologies (IT) related risks.

6.5.2. Analysis of the differences

Although the general requirements are approximately the same, it seems that there is a need for harmonising some of the details related to the implementation of the business continuity plans, since the CRD requirement applies to severe business disruption and risks other than operations risks e.g. liquidity risks, whereas the MiFID requires the establishment, implementation and maintenance of a business continuity policy to ensure continuity of the entity's investment services in the case of an interruption to its systems and procedures.

The requirements to test and update the plan, as defined in the proposed Level 2 implementing measures for the insurance sector (CEIOPS CP 33), as well as the definition of a business continuity policy, as stated in the MiFID Implementing Directive, seem to be sensible requisites that all sectors should have. However, before harmonising provisions on business continuity, the criticality of business disruptions within the different sectors should be analysed. Different needs for resilience and recovery times should be taken into account.

6.5.3. Harmonisation options

Desirable degree of harmonisation	**Medium**

It seems that the most useful and sensible option would be to develop cross-sectoral guidance on the implementation of business continuity and/or contingency plans, including, in particular, specific provisions related to the need to define a business continuity policy and to test regularly the existing plans.

7. INTERNAL CONTROL SYSTEM

This building block focuses on the aspects related to the implementation of an internal control system[51], including the establishment of a compliance function and an internal audit function.

The main objective of an internal control system is to ensure an appropriate operational risk control that prevents and/or mitigates the operational risks and provides additional independent mechanisms (controls).

While applying the proportionality principle it is crucial to retain the objectives of the internal control system, that is to guarantee an independent internal assessment within the

[51] The COSO (Committee of Sponsoring Organizations of the Treadway Commission) defines internal control as a process effected by an organisation's structure, work and authority flows, people and management information systems, designed to help the organisation accomplish specific goals or objectives (http://www.coso.org/IC-IntegratedFramework-summary.htm). This does however not imply that the TFIG advocates the use of the COSO Framework.

internal organisational framework, i.e. certain objectives may be performed by different control functions, however they must not be omitted.

The following table summarises the relevant material applicable to entities regarding internal control systems, as well as the respective nature.

Area	Relevant material (by activity/business)		
	Banking	**Insurance**	**Securities**
Implementation of an internal control system	Level 1: **CRD**: Articles 22, 109 Level 2: **CRD**: Annex VII, Part 3, §9; Part 4, §32; Annex X, Part 3, §9, §21-24 Level 3: **CEBS SRP**: IG7, IG8, IG14-19 **CEBS Liquidity Risk**: Recommendation 3	Level 1: **Solvency II**: Article 45 Level 2: **CEIOPS CP 33**: §3.224-3.225	Level 1: **MiFID**: Article 13(5)
Compliance function	Level 3: **CEBS SRP**: IG 14, IG 16	Level 1: **Solvency II**: Article 45 Level 2: **CEIOPS CP 33**: §3.226-3.228	Level 1: **MiFID**: Article 13(2) Level 2: **MiFID Implementing Directive**: Articles 5(1)(c) and 6
Internal audit function	Level 2: CRD: Annex III, Part 6, §17,36; Annex VII, Part 4, §131; Annex VIII, Part 3, §16(h), §56 Level 3: **CEBS SRP**: IG 14, IG 17 **CEBS AMA/IRB**: §389-392, §428, §447-450	Level 1: Solvency II: Article 46 Level 2: CEIOPS CP 33: §3.245-3.248	Level 2: **MiFID Implementing Directive**: Article 8

7.1. IMPLEMENTATION OF AN INTERNAL CONTROL SYSTEM

7.1.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Have internal control mechanisms or systems	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 45(1))	**Level 1** (MiFID Art. 13(5))
Include sound administrative and accounting procedures in the context of the internal control mechanisms or systems	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 45(1))	-

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Have appropriate reporting arrangements at all levels	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 45(1))	-
Have written policies in relation to internal control and ensure that those policies are implemented and reviewed at least annually and subject to prior approval by the management body	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 41(3))	-
Have in place policies, systems or plans to ensure compliance with the relevant directives	**Level 3** (CEBS SRP IG 7, 16)	**Level 1** (SII Art. 45(2))	**Level 2** (Impl. MiFID Art. 5(1)(c), Art. 9(1))
Monitor and ensure the adequacy of the compliance policies and procedures, monitor and report on the level of compliance, and monitor and report on the adequacy and effectiveness of measures taken to address any deficiencies in those policies and procedures	**Level 3** (CEBS SRP IG 7)	**Level 2** (CEIOPS CP 33 §3.224)	**Level 2** (Impl. MiFID Art. 5(1)(c), Art. 6)
Take into account the principle of proportionality	**Level 1** (CRD Art. 22(2))	**Level 1** (SII Art. 41(2))	**Level 2** (Impl. MiFID Art. 5(1))

The provisions for implementing an internal control system are broadly similar. In all three sectors there is a requirement to have effective internal control, with the requirements in the banking and insurance sectors providing additional detail about what this entails.

There is also a requirement across all three sectors to have in place policies and/or systems to ensure compliance with the relevant directives. Additional requirements are all directed to ensuring the effective monitoring and implementation of these policies and systems.

Finally, only in the case of the insurance sector, there is an explicitly stated obligation to have a written policy in relation to internal control.

7.1.2. Analysis of the differences

Although there is some additional detail provided for the insurance sector, the described differences do not appear material.

7.1.3. Harmonisation options

Desirable degree of harmonisation	**Low**	

Given that the recent financial crisis has revealed the importance of effective internal controls, harmonisation could be pursued to ensure that effective internal control is defined for the securities sector and that all sectors (and not just the insurance sector) are required to produce a written policy in relation to internal controls.

Although the TFIG considers that no change in the Level 1 framework seems necessary for the moment, in order to achieve harmonisation, it however recommends 3L3 guidance regarding:

- A consistent definition/understanding of internal control and internal control systems or mechanisms;
- The use of a common methodology for internal control; and
- A consistent documentation of internal control policies.

7.2. COMPLIANCE FUNCTION

7.2.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Have in place a compliance function	**Level 3** (CEBS SRP IG 14, 16)	**Level 1** (SII Art. 45(1))	**Level 2** (Impl. MiFID Art. 6(2))
Ensure that the compliance function and/or the person(s) performing it is/are organisationally separate from the activities that it/they is/are assigned to monitor and control	**Level 3** (CEBS SRP IG 14 (a)&(b))	-	**Level 2** (Impl. MiFID Art. 6(3)(c))
Ensure that the compliance function is organisationally independent of other control functions (risk and internal audit)	**Level 3** (CEBS SRP IG 14(b)&(c))	-	**Level 2** (Impl. MiFID Art. 6(2))
Ensure that the compliance function has direct access to the management body and/or audit committee	**Level 3** (CEBS SRP IG 14(b))	**Level 2** (CEIOPS CP 33 §3.226)	-
Have an appointed compliance officer who is responsible for the compliance function and the reporting of compliance	-	-	**Level 2** (Impl. MiFID Art. 6(3)(b))
Ensure that the responsibilities of the compliance function include monitoring, assessing, advising, verifying, reporting and assisting the entity/management body in order to ensure compliance with the entity's obligations under the applicable directive	**Level 3** (CEBS SRP IG 16(c))	**Level 1** (SII Art. 45(2))	**Level 2** (Impl. MiFID Art. 6(1))

Entities shall (Levels 1 and 2) or should (Level 3):	Banking	Insurance	Securities
Ensure that the responsibilities of the compliance function include the management of compliance risk	**Level 3** (CEBS SRP IG 16)	**Level 1** (SII Art. 45(2))	-
Ensure that the remuneration of the compliance function staff is not linked to the performance of the activities that the control function is intended to monitor and control or not likely to compromise their objectivity	**Level 3** (CEBS SRP IG 14(b))	**Level 2** (CEIOPS CP 59 §3.54)	**Level 2** (Impl. MiFID Art. 6(3)(d))
Ensure that the compliance function has the necessary resources, expertise and access to relevant information	**Level 3** (CEBS SRP IG 14(c))	**Level 2** (CEIOPS CP 33 §3.226)	**Level 2** (Impl. MiFID Art. 6(3)(a))
Take into account the principle of proportionality	**Level 3** (CEBS SRP IG 14)	**Level 1** (SII Art. 41(2))	**Level 2** (Impl. MiFID Art. 6(1)&(3))

The requirement to have a compliance function is defined across all three sectors. While some differences in the text and the level of detail provided exist, the desired outcome across all three sectors is similar: to ensure that the compliance function has the necessary structure, policies and resourcing to minimise any exposure to compliance risk the entity faces and to ensure that the compliance function can truly operate independently.

The main difference between the requirements is that, in the securities sector, a dedicated officer must be appointed to the compliance function, not subject to proportionality considerations. For this sector, proportionality only applies in respect of the compliance policies and procedures that an investment firm needs to ensure it meets its obligations and the associated risks (Article 6(1) of the MiFID Implementing Directive). Having a compliance function, i.e. a dedicated compliance unit, is obligatory. Proportionality also applies to the separation and remuneration of the compliance function provided it continues to be effective (Article 6(3) of MiFID Implementing Directive).

On the other hand, under MiFID there are no requirements to ensure that the compliance function has direct access to the management body and/or audit committee. Instead, MiFID Implementing Directive (Article 6(2)) requires that the compliance function advises and assists "the relevant persons responsible for carrying out investment services and activities" to comply with the obligations under the legislation in force.

In the case of the banking sector, CEBS SRP IG 14 includes some specificities regarding the "head of the function", including a requirement for the function to be "organisationally separate from the activities it is assigned to monitor and control", although this is subject to the principle of proportionality.

In the case of Solvency II, no requirement for independence regarding the compliance function exists, although CEIOPS CP 33 (§3.226) states that "The compliance function shall have appropriate standing within the undertaking"[52].

7.2.2. Analysis of the differences

Similarly to what was described in relation to the risk management function, one of the most relevant differences that exist between the requirements for each sector is the concept of "independence".

In effect, while the Level 2 advice for insurers refers to the "appropriate standing" of the function, and in CEBS SRP there is a general requirement for institutions to establish some functions, including a compliance function (although subject to the principle of proportionality), the MiFID Implementing Directive goes beyond these requirements and requires the appointment of a compliance officer.

7.2.3. Harmonisation options

Desirable degree of harmonisation	**Medium**	

Whilst the existing differences between requirements, notably the MiFID Implementing Directive provision on the need to appoint a compliance officer, seem to be justifiable by the specificities of each sector, a greater level of consistency may be beneficial for the sake of simplicity and certainty.

On the one hand, most of the requirements already exist, although with different levels of enforcement (depending on whether they are set on Levels 1, 2 or 3). In any case, the final result is that at least one person within the entity undertakes the compliance function.

However, the requirement to appoint a dedicated compliance officer in the securities sector may be significant. Given the requirement for organisational segregation, this requirement is also likely to apply to the banking and insurance sectors. Hence, and as compliance is so important to the achievement of good governance, this requirement could be made explicit in these sectors. In addition, given the potential for securities entities to be sole traders, the principle of proportionality should be extended to this requirement for these entities, as well as for both banks and insurers, where it would be inappropriate, if not impossible, to have a dedicated compliance officer.

Consistency in this regard could only be achieved by amending the relevant Level 1 or 2 texts, as the existence of mandatory requirements is the only real way of achieving convergence. However, it is not clear in practice that this is feasible.

[52] Please refer also to footnote 41.

For the time being, Level 3 guidelines could be developed in order to harmonise the requirement to appoint a dedicated compliance officer and to ensure that this requirement is applied proportionately.

For the reasons stated above, this is one of the issues that the TFIG considers requires the development of cross-sectoral guidance.

7.3. INTERNAL AUDIT FUNCTION

7.3.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	Banking	Insurance	Securities
Have an independent internal audit function	**Level 2** (CRD, Annex VII, Part 4, §131)	**Level 1** (SII Art. 46(3))	-
Have an independent internal audit function, subject to the proportionality principle	**Level 3** (CEBS SRP IG 14, 17)	-	**Level 2** (Impl. MiFID Art. 8)

The Directives in all three sectors have provisions with regard to the internal audit function, i.e. in general terms, for the banking, insurance and securities sectors entities are required to have an audit function. The important cornerstones of an effective internal audit function, such as independence and reporting requirements, are also common to all three sectors. It also requires investment firms to establish and maintain an independent internal audit function charged with detailed responsibilities e.g. establish and maintain an audit plan whereas in the banking sector the CRD is not as explicit in stating such requirements, but like in other areas detailed requirements can be found on Level 3.

In the case of the banking and the securities sectors the requirement of independence is subject to the principle of proportionality, unlike in the case of the insurance sector. This fact is further detailed in CEIOPS' proposed Level 2 implementing measures (CEIOPS CP 33).

7.3.2. Analysis of the differences

Taking account of all three levels of rules and common interpretations, the requirements for an effective internal audit function seem to be very similar. It is, however, to be noted that important constituting elements of how an internal audit function should be established and operate in supervised entities, such as independence and scope of operation, are not always regulated in binding directives.

Additionally, the existing Level 3 guidance for the banking sector provide further detail on the requirements that should be applied in order to ensure operational independence between the internal audit function and other functions.

7.3.3. Harmonisation options

Desirable degree of harmonisation	**Medium**	

Given that the requirements are broadly similar, the focus should be, to the extent legally possible, on consistent interpretation of the requirements for an internal audit function over all three sectors. As a first step and as far as this is possibly by way of interpretation, 3L3 guidelines on internal auditing could be useful to make progress towards this goal.

In particular, these guidelines could focus on the definition of recommendations related to the operational independence of the internal audit function in the cases where the principle of proportionality applies, which could include, for example, a reference to the possibility of outsourcing the internal audit function.

Similarly to the cases already described for the risk management and compliance functions, effective harmonisation could only be achieved by amending the relevant Level 1 or 2 texts, as the existence of mandatory requirements is the only real way of achieving convergence.

However, the most feasible option for the time being would be to develop Level 3 guidelines in order to harmonise the requirements related to the internal audit function regarding both the interpretation of "independence" and the interaction with other functions.

For the reasons stated above, this is one of the issues that the TFIG considers requires the development of cross-sectoral guidance.

8. SUPERVISORY REVIEW, INTERNAL REPORTING AND PUBLIC DISCLOSURE

This building block focuses on three complementary aspects that play an important role in the setting of internal governance arrangements: the supervisory review process undertaken by the supervisory authorities, the internal reporting requirements related to internal governance aspects and requirements for public disclosure related to the entities' system of governance.

The rationale underlying the issues which are covered under this chapter is that the existence of a system of governance does not suffice, no matter how complete it is, as it will necessarily have to be monitored and supervised.

The following table summarises the relevant material applicable to entities regarding supervisory review, internal reporting and public disclosure, as well as the respective nature.

Area	Relevant material (by activity/business)		
	Banking	**Insurance**	**Securities**
Supervisory review process	Level 1: **CRD:** Articles 123, 124, 136 Level 2: **CRD:** Annex XI Level 3: **CEBS SRP**	Level 1: **Solvency II**: Article 36	-
Internal reporting requirements	Level 1: **CRD**: Articles 22, 29(1st sub-§), 63(1)(a)&(b) Level 2: **CRD**: Annex X, Part 2, §12(c) Level 3: **CEBS SRP:** IG18, IG19	Level 1: **Solvency II**: Articles 43(1), 45(1), 52 Level 2: **CEIOPS CP 33**: §3.24(a)&(k), §3.26, §3.53(d), §3.191(d)	Level 2: **MiFID Implementing Directive**: Article 5(1)(a)&(e) & (4)
Disclosure, transparency and accountability issues	Level 1: **CRD**: Articles 22, 29(1st sub-§); 109; 110; 111(4), 138(2); 145-149 Level 2: **CRD**: Annex VI (Part 2, 2.2.); Annex VII Part 4, 5.2.); Annex XII Level 3: **CEBS SRP:** IG20, IG21	Level 1: **Solvency II**: Articles 35, 50, 52, 53 and 54	Level 1: **MiFID**: Articles 19(8), 25-30, 43(2) and 44-45 Level 2: **MiFID Implementing Directive**: Articles 9(2)&(3)

8.1. SUPERVISORY REVIEW PROCESS

8.1.1. Differences identified

Supervisory authorities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Review the strategies, processes and mechanisms/procedures implemented by entities to comply with the directive and evaluate the risks to which the entities are or might be exposed	**Level 1** (CRD Art. 124 (1)&(3)&(4))	**Level 1** (SII Art. 36(1))	-

Supervisory authorities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Be required, and have the necessary powers, to monitor the entities' compliance with the legal requirements in force	**Level 1** (CRD Art. 124)	**Level 1** (SII Art. 36(1))	**Level 1** (MiFID Art. 48, Art. 50)
Be empowered to verify the system of governance and to require that the system of governance be improved and strengthened to ensure compliance with legal requirements in force	**Level 1** (CRD Art. 136)	**Level 1** (SII Art. 36(1)&(5))	-
Require entities to submit them the information which is necessary for the purposes of supervision, including elements to assess, among others, the system of governance, the risk management system and the capital structure, needs and management	-	**Level 1** (SII Art. 35(1)(a))	-
Take into account the principle of proportionality	**Level 1** (CRD Art. 124(4))	**Level 1** (SII Art. 36(6))	-

Across all three sectors, and mostly at Level 1, there are requirements relating generally to the obligations of regulators to monitor compliance by entities with the relevant directive requirements, as well as to provide information to regulators to enable them to carry out that monitoring. However, in the case of the securities sector there does not seem to exist so much detail as in the case of the other two sectors.

It is also worth noting that both the CRD and Solvency II describe the supervisory review process to be undertaken by the supervisor, process which presents several similarities. As regards designations, the acronym "SREP" that is used in the case of banks and investment firms corresponds to the insurance sector's "SRP" and stands for the same concept of "supervisory review process".

8.1.2. Analysis of differences

The main difference seems to be that Solvency II imposes a specific obligation on regulators to be satisfied that the entity's system of governance is adequate and requires entities to provide information that would enable the regulator to make that assessment.

8.1.3. Harmonisations options

Desirable degree of harmonisation	**Medium**	

As highlighted at the start, the financial crisis that has been affecting entities operating in the financial services sector all over the world was in part originated by inefficiencies in the implemented systems of governance and, in particular, in the entities' internal controls.

This raises the question on what can be done, not only from the entities' side, but also from the supervisory authority's perspective, in order to enhance the implemented systems of governance.

Consequently, the TFIG considers that this aspect calls for some degree of harmonisation and that some 3L3 work should be undertaken in order to accomplish this objective.

The TFIG's proposal regarding this issue is that the whole supervisory review process, as well as its consequences, is thoroughly analysed and revised. In particular, it is necessary to provide supervisors with the necessary powers that allow them to adequately assess:

- The quality of the decision-making processes, i.e. to what extent the predefined decision-making processes are followed and complied with, if decisions are taken on the appropriate *fora*, how are committees established and managed, etc.
- The "fit and proper" requirements of the members of the management body and senior management;
- The effectiveness of the internal control procedures, including the use is made of the reported information; e.g. the supervisory review process should allow that a follow-up is made regarding the information on identified deficiencies that was reported to the top hierarchy and the measures taken thereafter;
- The effectiveness of the risk management systems, including the analysis of self-assessments performed by the entity (e.g. ICAAP[53]/ORSA[54]).

The final result would be that supervisory authorities are able to assess each entity's risk profile, based not only on the quantitative/financial aspects, but also on the qualitative aspects, that would include the system of governance, i.e. the effectiveness of the implemented system of governance would integrate the definition of the entity's risk profile.

It is however important to acknowledge that the banking and the insurance sectors already have their own requirements on the supervisory review process, on which this framework could build upon.

For the reasons stated above, this is one of the issues that the TFIG considers requires the development of cross-sectoral guidance.

[53] ICAAP stands for "Internal Capital Adequacy Assessment Process", as defined in CEBS SRP guidelines.

[54] ORSA stands for "Own Risk and Solvency Assessment", as defined under Article 44 of Solvency II.

8.2. INTERNAL REPORTING REQUIREMENTS

8.2.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	Banking	Insurance	Securities
Report the risks they are exposed to	**Level 1** (CRD Art. 22(1))	**Level 1** (SII Art. 43(1))	-
Ensure that information related to compliance, risk management and internal audit issues is reported to the management body	**Level 3** (CEBS SRP IG 14)	**Level 1** (SII Art. 45(1), Art. 43(1), Art. 46(4))	**Level 2** (Impl. MiFID Art. 9(2)&(3))

In the case of internal reporting, the most relevant requirements relating to the reporting lines for the banking sector are defined at Level 3, in CEBS SRP guidelines. These state that internal reporting is crucial for the assessment of the adequacy of internal controls.

In the case of the insurance sector, Article 41 foresees "an effective system for ensuring the transmission of information", but articles on the risk management system, internal control and internal audit provide further requirements on the reporting of these specific subjects. More details are presented in the Level 2 advice with regard to all the key functions foreseen by the directive: the risk management function, the compliance function, the internal audit function, and the actuarial function.

As for the securities sector, effective internal reporting and communication of information are required also by MiFID and its implementing measures, although it focuses more on the trading activity of the investment firms than on their financial standing and risk management. On Level 2, the MiFID Implementing Directive also states that the investment firm has to "establish, implement and maintain effective internal reporting and communication of information at all relevant levels". MiFID also mentions information for competent authorities, public and clients, while the guidance for other sectors is applicable only for authorities and the public. Additionally, MiFID states the obligation to report breaches of rules (Article 26(2)), while in the other sectors this is not clearly stated.

8.2.2. Analysis of the differences

All sectoral principles and rules recognise that effective governance and effective board decision-making depends on the quality and timeliness of the information received. The internal reporting system, its comprehensiveness and correct use make an entity efficient.

Well developed banks, insurers and investment firms should develop internal reporting systems that include all risks they are exposed to, at all levels. Consequently, a good system of reporting and the extent the management body takes account of such information is essential, in particular in times of financial crisis.

8.2.3. Harmonisation options

Desirable degree of harmonisation	**Low**	

Relevant sectoral requirements should remain and material reporting requirements on the financial standing and risk exposure of securities sector entities could be developed in the future.

8.3. DISCLOSURE, TRANSPARENCY AND ACCOUNTABILITY ISSUES

8.3.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**
Disclose information regarding the main risks on a regular basis (at least annually), e.g. in an annual report	**Level 1** (CRD Art. 110(1))	**Level 1** (SII Art. 50(1))	-
Make accessible and available individual credit assessments	**Level 2** (CRD Annex VI, Part 2, §10-11)	-	-
Report periodically to the supervisory authority	**Level 1** (CRD Art. 29)	**Level 1** (SII Art. 35)	**Level 2** (Impl. MiFID Art. 5(4))

Both the banking and the insurance sectors require information regarding the strategies, policies and main risks to be disclosed on a regular basis. Additionally, in the case of the banking sector the existing requirements emphasise the monitoring of large exposures.

As for Solvency II, the description of the system of governance and the assessment of its adequacy for the risk profile of the undertaking should also be disclosed. Article 35 of Solvency II details the information that has to be provided for supervisory purposes and that should allow the supervisor to assess the system of governance existing in the entity, the business it is carrying on, the risks faced and the risk management system. Some general rules about the content and the principles of the information to be provided are foreseen by the directive as having to be further specified in Level 2 measures and Level 3 guidance. However, when it comes to public disclosure requirements, Solvency II includes the minimum criteria regarding information to be made available to the public.

As referred already in the case of internal reporting requirements, the MiFID focuses more on the trading activity of the investment firms than on their financial standing and risk management. This directive also mentions information for competent authorities, public and clients, while the guidance for other sectors is applicable only for authorities and the public.

The MiFID also states the obligation to report breaches of rules (Article 26(2)), while in the other sectors this is not clearly stated.

8.3.2. Analysis of the differences

The existing requirements for the banking and insurance sectors focus on the risks the entity is exposed to.

For the insurance sector the directive also prescribes that the information should comprise qualitative and quantitative elements and that it should reflect the principle of proportionality.

Relevant financial standing and risk management reporting requirements for securities sector are not set out.

8.3.3. Harmonisation options

Desirable degree of harmonisation	**Low**	

Transparency and disclosure involve many stakeholders with different priorities and interests, although they have the common aim to foster an effective market discipline, by helping the public to understand the activities, strategies, and policies of a specific entity.

Furthermore, public disclosure allows for a comparison of governance practices, helping the identification of the entities which use the best practices, increasing the accountability of the management bodies.

However, it is very difficult to come up with a universal formula for the "right" level of disclosure.

Differences identified in the different reporting requirements reflect the different purposes and objectives pursued by the directives and the relevant supervisors. Therefore, it is important to note that relevant sectoral requirements should remain. Consequently, there does not seem to be a case for a high degree of harmonisation in this respect. In any case, relevant reporting requirements on the financial standing and risk exposure of entities performing securities activities could be developed.

9. GROUP STRUCTURES AND GROUP SPECIFIC ISSUES

In each of the three analysed sectors group structures have to comply with specific rules (Level 1 or 2) or recommendations (Level 3). Securities group supervision (meaning the consolidated supervision of investment firm groups) runs parallel to the consolidated supervision of credit institutions (Article 2 of CAD applies Article 68 to Article 73 of the CRD

(*mutatis mutandis*) to investment firms, as referred in Section 3.4. "Interconnections between directives"). Consequently, in the tables below, only specific MiFID provisions regarding investment services activities undertaken in a group context are mentioned in the column "Securities".

In addition to the rules governing each of these sectors, there is the Financial Conglomerates Directive (FCD) that is organising a supplementary supervision on the level of the conglomerate. This supplementary supervision is exercised on the basis of specific Level 1 rules related to:

- Capital adequacy;
- Risk concentration;
- Intra-group transactions;
- Internal control mechanisms and risk management processes.

When there is a mixed financial holding on the top of the financial conglomerate, the FCD also provides specific rules governing the management body.

The review process of the FCD in place (as mentioned in Section 3.2., "Scope") will not necessarily have an important impact on the governance rules of the financial conglomerates. In its Consultation Paper of 28 May 2009, the Joint Committee of Financial Conglomerates (JCFC) has indeed identified some issues where the FCD may not achieve its objectives. Relevant for the present report is the proposition to modify the definitions of an "Insurance Holding Company" and a "Financial Holding Company" in order to allow that both can constitute at the same time a "Mixed Financial Holding Company". The objective of this recommendation is to ensure that sectoral rules will continue to apply at the same holding level on a group that has been identified as a financial conglomerate.

The following table summarises the relevant material applicable to entities regarding group structures and group specific issues, as well as the respective nature.

Area	Relevant material (by activity/business)			
	Banking	**Insurance**	**Securities**	**Financial Conglomerates**
Corporate structure and organisation	Level 1: **CRD:** Article 73(3) Level 3: **CEBS SRP**: IG 1	Level 1: **Solvency II**: Articles 250(1)	Level 2: **MiFID Implementing Directive**: Art. 22(1))	-
Risk management system	Level 1: **CRD**: Articles 22, 71, 73, 123 Level 2: **CRD**: Annex V (ICAAP), Annex X, Part 3 (3)	Level 1: **Solvency II**: Articles 248, 250(1)	-	Level 1: **FCD**: Article 9(1)&(2)

Area	Relevant material (by activity/business)			
	Banking	**Insurance**	**Securities**	**Financial Conglomerates**
Internal control system	Level 1: **CRD**: Articles 22, 73, 123	Level 1: **Solvency II**: Article 250(1)	-	Level 1: **FCD**: Article 9(1)&(3)
Supervisory review, internal reporting and public disclosure	Level 1: **CRD**: Articles 68(3), 72(1)&(2), 123, 124, 139(1)	Level 1: **Solvency II**: Articles 249(2), 250, 258, 260	-	Level 1: **FCD**: Articles 7(2), 8(2), 9(3)(b), 9(4), 9(5), 14(1)

9.1. CORPORATE STRUCTURE AND ORGANISATION

9.1.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**	**Financial Conglomerates**
Implement the existing requirements for corporate structure and organisation both on a solo basis and at group level	**Level 1** (CRD Art. 73(3)	**Level 1** (SII Art. 250(1))	-	-
Have a corporate structure that is transparent, clear and well-defined and that provides for an effective, sound or prudent management of the entity	**Level 1** (CRD Art. 73(3))	**Level 1** (SII Art. 41(1))	-	**Level 1** (FCD Art. 9)
Establish, implement and maintain an effective conflicts of interest policy which takes into account any circumstances which result of the structure of the group	-	-	**Level 2** (Impl. MiFID Art. 22(1))	-

Banking and insurance entities are required to have a transparent corporate or organisational structure both at solo and group level. The system has to provide an effective, sound and/or prudent management. Additionally, the FCD puts the tone on the sound governance and management with respect to all the risks that different entities assume.

In the case of the securities sector, the only specific requirement in this context refers to the conflicts of interest policy, which should take into account the situations where an entity is part of a group.

9.1.2. Analysis of the differences

Both in the banking and in the insurance sectors, there is a general provision that extends the requirements for solo entities to the level of the group. The wording of the underlying solo provisions differs, but the content and the intent are the same (see also Section 5.1. on "Lines of responsibility and accountability"). For example, it is rather difficult to see the difference between "effective and prudent" and "sound and prudent".

In the Implementing MiFID Directive, a provison can be found regarding conflicts of interest at the level of the group. It concerns conflicts of interest that are potentially detrimental to a client and that arise in the course of providing investment and ancillary activities or a combination thereof. Since the CRD and Solvency II focus on the prudential supervision of institutions, rather than on how certain activities are undertaken by these institutions (or the relationship of the institutions with their clients), it is logic that a similar provison as in Article 22 of the MiFID Implementing Directive does not appear either in the CRD or Solvency II.

9.1.3. Harmonisation options

Desirable degree of harmonisation	**Low**	

The reasons for the existing differences between the banking/insurance and the securities sectors can be motivated by the different approaches of CRD, Solvency II and MiFID. The objective of CRD and Solvency II is to take account of all types of risk to which a specific type of intermediary is exposed and to manage those risks effectively. In this regard, governance rules regarding the group relationship aim to mitigate risks arising from e.g. the complexity or non-transparency of the entity's group structure leading to the inefficiency of the management and control processes. In this context, governance rules regarding the group relationship are deemed necessary. Conversely, MiFID does not relate to a specific type of intermediary, but to a specific type of activities (i.e. investment activities). Due to the existence of these different objectives in the regulation for the banking/insurance on the one hand and the securities sector on the other hand, no changes in Levels 1, 2 or 3 seem to be necessary.

Groups generally tend to efficiently steer and control the business activity of their various entities by relying on a single group strategy and vision that fully exploits possible synergies. The group remains subject to the requirements, on the part of the parent company, as well as its subsidiaries, to duly take into account the existence of independent legal persons and the need for the parent company, as well as the subsidiaries, to have an adequate governance structure. In this perspective it could be useful to develop common Level 3 guidance in this area for all group structures, including financial conglomerates, although this does not seem to be a priority for the time being.

These guidelines could in particular cover the following dimensions:

- **"Know Your Structure"**. Financial groups that *via* their different subsidiaries and/or branches in different countries offer a large variety of financial services and products (banking, insurance, investment products) should set up adequate structures that make it possible to follow up the risks arising from their organisation and activities. Groups also make use of complex service schemes and company structures in their activities (company creation, special-purpose vehicles, trust structures), be it for own account or to propose these schemes and structures to their customers. The financial crisis has shown the importance for the management on the top of the group to understand the different structures of the group in order to be able to take their responsibilities and to manage the risks adequately;
- **Matrix Management**. Matrix management and business line management – meaning that operational powers for regulated subsidiaries' activities are held not at subsidiary level, but at the level of the parent company as part of a group steering policy – are often used within a group to improve the manner in which its activities are steered. The persons leading a business line or a centralised support service at group level should been assimilated with senior managers if they have a direct and decisive influence on the decision-making process within the parent company and/or subsidiaries. Group steering need to be without prejudice to the responsibilities of the governing bodies of the subsidiaries as regards their activities. Matrix structures need to be transparent and well defined, with clear reporting lines; and
- **Plurality of functions**. With a view to maintaining the necessary checks and balances within a group, concrete allocation of mandates in the corporate bodies, of key posts and of matrix or business line responsibilities should duly take into account any plurality of functions. The proposed separation of functions or of conflicting interests should not turn out to be neutralised in practice by a single person holding a plurality of functions within the group.

9.2. RISK MANAGEMENT SYSTEM

9.2.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**	**Financial Conglomerates**
Implement the existing requirements for the risk management system both on a solo basis and at group level	**Level 1** (CRD Art. 23, Art. 73)	**Level 1** (SII Art. 250(1))	-	-
Have in place adequate risk management processes	**Level 1** (CRD Art. 22, Art. 123)	**Level 1** (SII Art. 43(1))	-	**Level 1** (FCD Art. 9(1)&(2))

As mentioned before, in the banking sector Article 73 of the CRD extends the general provision of Article 22 of the CRD applicable to solo entities to the level of the group. Article 71 also applies the ICAAP described in Article 123 at group level.

In the case of the insurance sector, Article 250 of Solvency II applies, *mutatis mutandis*, the provisions regarding the system of governance for solo level entities to the group level. Consequently, the ORSA has to be performed both at the solo and group level. A specific provision also exists in the case where the risk management function is centralised within a group, providing for the possibility to have a single ORSA at the level of the group (Article 250(4)).

As for the banking sector, Article 73 of the CRD extends the provisions applicable to solo entities to the level of the group.

For the securities sector, no specific provisions related to risk management at the level of a group exist.

9.2.2. Analysis of the differences

The existing differences between the banking/insurance sectors, on the one hand, and the securities sector, on the other, that seem to be justifiable by the underlying sectoral objectives, were already spelled out in Section 9.1. (Corporate structure and organisation).

In this particular case, the wording of the underlying solo requirements might differ, but the outcome is the same.

9.2.3. Harmonisation options

Desirable degree of harmonisation	**Medium**	

Due to the existence of the different objectives in the regulation for the banking/insurance on the one hand and the securities sector on the other hand, no changes in Levels 1, 2 or 3 seem to be necessary.

9.3. INTERNAL CONTROL SYSTEM

9.3.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**	**Financial Conglomerates**
Implement the existing requirements for the internal control system both on a solo basis and at group level	**Level 1** (CRD Art. 23, Art. 73)	**Level 1** (SII Art. 250(1))	-	-
Have in place adequate internal control mechanisms	**Level 1** (CRD Art. 22, Art. 123)	**Level 1** (SII Art. 45(1))	-	**Level 1** (FCD Art. 9(1)&(3))

In the context of a group, the existing sectoral requirements related to internal control are rather similar to those highlighted in the previous section.

Both in the banking and in the insurance sectors, the requirements applicable to the solo level are also valid for the group level.

The FCD establishes that the internal control mechanisms should consider the "capital adequacy to identify and measure all material risks incurred and to appropriately relate own funds to risks" and "sound reporting and accounting procedures to identify, measure, monitor and control the intra-group transactions and the risk concentration".

9.3.2. Analysis of the differences

As mentioned, since the banking and the insurance sectors focus on the management of the risks entities are exposed to, the existence of effective management and control processes plays a more relevant role in these sectors, including at the level of the group.

9.3.3. Harmonisation options

Desirable degree of harmonisation	**Medium**	

Due to the existence of the different objectives in the regulation for the banking/insurance on the one hand and the securities sector on the other hand, no changes in Levels 1, 2 or 3 seem to be necessary.

9.4. SUPERVISORY REVIEW, INTERNAL REPORTING AND PUBLIC DISCLOSURE

9.4.1. Differences identified

Entities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**	**Financial Conglomerates**
Report on a regular basis and at least annually to the group supervisor all significant intra-group transactions by entities within a group	**Level 1** (CRD Art. 22, Art. 123)	**Level 1** (SII Art. 249(2))	-	**Level 1** (FCD Art. 8(2))
Establish flows of information within the group	**Level 1** (CRD Art. 139(1))	**Level 1** (SII Art. 258)	-	**Level 1** (FCD Art. 14)

Supervisory authorities shall (Levels 1 and 2) or should (Level 3):	**Banking**	**Insurance**	**Securities**	**Financial Conglomerates**
Review the internal governance issues in a group context	**Level 1** (CRD Art. 124(2), Art. 129)	**Level 1** (SII Art. 250(3))		**Level 1** (FCD Art. 11(1)(d))

Requirements for the banking sector provide that EU parent credit institutions shall comply with the disclosure requirements by credit institutions on the basis of their consolidated financial situation. Credit institutions controlled by an EU parent financial holding company shall comply with the disclosure requirements by credit institutions on the basis of the consolidated financial situation of that financial holding company.

As for the insurance sector, Article 260(1) of Solvency II applies the requirements related to the "Solvency and Financial Condition Report" for a solo entity to the level of the group (*mutatis mutandis*). CEIOPS CP 58 details both the requirements for publicly disclosed information and the report to supervisors.

Requirements also exist for the reporting of intra-group transactions in the CRD, Solvency II and FCD. However, in the banking sector this is only done implicitly. The ICAAP defined in Article 123 of the CRD requires the management of all types of risks, thus also risks stemming from intra-group relations. However, neither Article 22 nor Article 123 make an explicit reference to intra-group transactions. The FCD provides, like Solvency II, an explicit legal basis for the supervision of intra-group transactions (in its Article 8). Furthermore, the FCD establishes that the internal control mechanisms should include "sound reporting and accounting procedures to identify, measure, monitor and control the intra-group transactions and the risk concentration".

In the case of the banking and insurance sector, risk management and internal control requirements also relate to the transactions with the parent mixed-activity holding company and its subsidiaries (Article 138 of the CRD and Article 267 of Solvency II).

The same difference between implicit/explicit wording plays up for the supervisory review process with regard to internal governance issues in a group context. Both in the cases of CRD and Solvency II the supervisory review must be performed at group level and must cover the systems and reporting procedures which entities are required to implement. For the insurance sector, this includes the review of the ORSA to be performed at the group (consolidated) level (Article 250(4)).

Solvency II provides an explicit legal basis to that end (Article 250(3)); the CRD covers this only implicitly. In the case of the FCD, there is also an explicit basis: Article 11(1)(d) states that the tasks of the coordinator, which is the competent authority responsible for exercising supplementary supervision, include the "assessment of the financial conglomerate's structure, organisation and internal control system as set out in Article 9".

As for the securities sector, the MiFID does not contain any group specific requirements in this respect.

Information should run freely throughout the group structures, to facilitate the group supervision. Both in the banking and in the insurance sector, and in the FCD, there are similar provisions to that end.

9.4.2. Analysis of the differences

There does not seem to be a logic explanation why the CRD is only implicit about the supervision of intra-group transactions and the supervisory review process with regard to the internal governance of the group. The more specific these group issues are spelled out, the better prudential supervision can get a grip on banking, insurance or mixed financial groups. Therefore, it would be useful if the CRD would declare explicitly on the matters of intra-group transactions and the supervisory review processwith regard to the internal governance of the group.

Since the banking and the insurance sectors focus on the management of the risks the entities are exposed to, the existence of a review process plays a more relevant role in these sectors, including at the level of the group.

9.4.3. Harmonisation options

Desirable degree of harmonisation	**Low**	

Some level of harmonisation of the high-level principles or processes could be achieved by trans-sectoral Level 3 guidance, including the supplementary supervision on financial conglomerates. However, this issue does not seem to deserve a high level of priority for the time being.

ANNEXES

I. RELEVANT MATERIAL

In order to facilitate the reading of the document, the acronyms and abbreviations used to make reference to the applicable legislation and guidance are the following:

Reference	Description	Level	Status
Capital Adequacy Directive (CAD)	Directive 2006/49/EC of the European Parliament and of the Council of 14 June 2006 on the capital adequacy of investment firms and credit institutions (recast) (http://eur-lex.europa.eu/LexUriServ/site/en/oj/2006/l_177/l_17720060630en02010255.pdf)	1	Final
Capital Requirements Directive (CRD)	Directive 2006/48/EC of the European Parliament and of the Council of 14 June 2006 relating to the taking up and pursuit of the business of credit institutions (recast) (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:177:0001:0200:EN:PDF)	1	Final (under revision)
CEBS AMA/IRB	"Guidelines on the implementation, validation and assessment of Advanced Measurement (AMA) and Internal Ratings Based (IRB) Approaches", Committee of European Banking Supervisors, 4 April 2006 (http://www.c-ebs.org/getdoc/5b3ff026-4232-4644-b593-d652fa6ed1ec/GL10.aspx)	3	Final
CEBS CP 24	Consultation Paper on "High-level principles for risk management" (CP 24), Committee of European Banking Supervisors, 8 April 2009 (http://www.c-ebs.org/getdoc/0861a22e-0eb8-4449-9b3a-f4b1959267c7/CP24_High-level-principles-for-risk-management.aspx)	3	Draft
CEBS Liquidity Risk	"Second Part of CEBS's Technical Advice to the European Commission on Liquidity Risk Management" (CEBS 2008 147), Committee of European Banking Supervisors, 18 September 2008 (http://www.c-ebs.org/getdoc/bcadd664-d06b-42bb-b6d5-67c8ff48d11d/20081809CEBS_2008_147_(Advice-on-liquidity_2nd-par.aspx)	3	Final
CEBS Outsourcing	"Guidelines on outsourcing", Committee of European Banking Supervisors, 14 December 2006 (http://www.c-ebs.org/getdoc/f99a6113-02ea-4028-8737-1cdb33624840/GL02OutsourcingGuidelines-pdf.aspx)	3	Final

Reference	Description	Level	Status
CEBS SRP	"Guidelines on the Application of the Supervisory Review Process under Pillar 2" (CP 03 revised), Committee of European Banking Supervisors, 25 January 2006 (http://www.c-ebs.org/getdoc/00ec6db3-bb41-467c-acb9-8e271f617675/GL03.aspx)	3	Final
CEBS Stress Testing	CEBS Guidelines on the Technical aspects of stress testing under the supervisory review process (CP 12), 14 December 2006 (http://www.c-ebs.org/getdoc/e68d361e-eb02-4e28-baf8-0e77efe5728e/GL03stresstesting.aspx)	3	Final
CEIOPS CP 28	"Consultation Paper no. 28 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR standard formula – Counterparty default risk module" (CEIOPS-CP-28/09), Committee of European Insurance and Occupational Pensions Supervisors, 26 March 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP28/CEIOPS-CP-28-09-Draft-L2-Advice-on-SCR-Standard-Formula-Counterparty-default-risk.pdf)	2	Draft Level 2 measures
CEIOPS CP 33	"Consultation Paper no. 33 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: System of Governance" (CEIOPS-CP-33/09), Committee of European Insurance and Occupational Pensions Supervisors, 26 March 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP33/CEIOPS-CP-33-09-Draft-L2-Advice-on-Governance.pdf)	2	Draft Level 2 measures
CEIOPS CP 39	"Consultation Paper no. 39 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Technical provisions – Article 85 a – Actuarial and statistical methodologies to calculate the best estimate" (CEIOPS-CP-39/09), Committee of European Insurance and Occupational Pensions Supervisors, 2 July 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP39/CEIOPS-CP-39-09-L2-Advice-TP-Best-Estimate.pdf)	2	Draft Level 2 measures
CEIOPS CP 43	"Consultation Paper no. 43 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Technical Provisions – Article 85 f – Standards for Data Quality" (CEIOPS-CP-43/09), Committee of European Insurance and Occupational Pensions Supervisors, 2 July 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP43/CEIOPS-CP-43-09-L2-Advice-TP-Standards-for-data-quality.pdf)	2	Draft Level 2 measures

Reference	Description	Level	Status
CEIOPS CP 47	"Consultation Paper no. 47 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR Standard Formula – Article 109 – Structure and Design of Market Risk Module" (CEIOPS-CP-47/09), Committee of European Insurance and Occupational Pensions Supervisors, 2 July 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP47/CEIOPS-CP-47-09-L2-Advice-Standard-Formula-Market-Risk.pdf)	2	Draft Level 2 measures
CEIOPS CP 48	"Consultation Paper no. 48 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR standard formula: Non-Life Underwriting Risk" (CEIOPS-CP-48/09), Committee of European Insurance and Occupational Pensions Supervisors, 2 July 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP48/CEIOPS-CP-48-09-L2-Advice-Standard-Formula-Non-Life-Underwriting-Risk.pdf)	2	Draft Level 2 measures
CEIOPS CP 49	"Consultation Paper no. 49 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Standard formula SCR – Article 109 c – Life underwriting risk" (CEIOPS-CP-49/09), Committee of European Insurance and Occupational Pensions Supervisors, 2 July 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP49/CEIOPS-CP-49-09-L2-Advice-Standard-Formula-Life-Underwriting-risk.pdf)	2	Draft Level 2 measures
CEIOPS CP 51	"Consultation Paper no. 51 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: SCR standard formula – Further advice on the counterparty default risk module (Complementary to CEIOPS' Consultation Paper no. 28) (CEIOPS-CP-51/09), Committee of European Insurance and Occupational Pensions Supervisors, 2 July 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP51/CEIOPS-CP-51-09-L2-Advice-Standard-Formula-Counterparty-Default-Risk.pdf)	2	Draft Level 2 measures
CEIOPS CP 53	"Consultation Paper no. 53 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Article 109 1 (g) – SCR standard formula – Operational Risk" (CEIOPS-CP-53/09), Committee of European Insurance and Occupational Pensions Supervisors, 2 July 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP53/CEIOPS-CP-53-09-L2-Advice-Standard-Formula-Operational-Risk.pdf)	2	Draft Level 2 measures

Reference	Description	Level	Status
CEIOPS CP 56	"Consultation Paper no. 56 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Articles 118 to 124 – Tests and Standards for Internal Model Approval" (CEIOPS-CP-56/09), Committee of European Insurance and Occupational Pensions Supervisors, 2 July 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP56/CEIOPS-CP-56-09-L2-Advice-Tests-and-Standards-for-internal-model-approval.pdf)	2	Draft Level 2 measures
CEIOPS CP 58	"Consultation Paper no. 58 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Supervisory Reporting and Public Disclosure Requirements" (CEIOPS-CP-58/09), Committee of European Insurance and Occupational Pensions Supervisors, 2 July 2009, (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP58/CEIOPS-CP-58-09-L2-Advice-Supervisory-Reporting-and-Disclosure.pdf)	2	Draft Level 2 measures
CEIOPS CP 59	"Consultation Paper no. 59 – Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Remuneration Issues" (CEIOPS-CP-59/09), Committee of European Insurance and Occupational Pensions Supervisors, 21 July 2009 (http://www.ceiops.eu/media/files/consultations/consultationpapers/CP59/CEIOPS-CP-59-09-L2-Advice-Remuneration-Issues.pdf)	2	Draft Level 2 measures
CESR Conflicts of Interest	"MiFID Supervisory Briefings – Conflicts of Interest" (CESR/08-733), Committee of European Securities Regulators (http://www.cesr.eu/popup2.php?id=5287)	3	Final
Directive 2006/43/EC	Directive 2006/43/EC of the European Parliament and of the Council of 17 May 2006 on statutory audits of annual accounts and consolidated accounts, amending Council Directives 78/660/EEC and 83/349/EEC and repealing Council Directive 84/253/EEC (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:157:0087:0107:EN:PDF)	1	Final
Financial Conglomerates Directive (FCD)	Directive 2002/87/EC of the European Parliament and of the Council of 16 December 2002 on the supplementary supervision of credit institutions, insurance undertakings and investment firms in a financial conglomerate and amending Council Directives 73/239/EEC, 79/267/EEC, 92/49/EEC, 92/96/EEC, 93/6/EEC and 93/22/EEC, and Directives 98/78/EC and 2000/12/EC of the European Parliament and of the Council (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2003:035:0001:0027:EN:PDF)	1	Final (under revision)

Reference	Description	Level	Status
Markets in Financial Instruments Directive (MiFID)	Directive 2004/39/EC of the European Parliament and of the Council of 21 April 2004 on markets in financial instruments amending Council Directives 85/611/EEC and 93/6/EEC and Directive 2000/12/EC of the European Parliament and of the Council and repealing Council Directive 93/22/EEC (http://eur-lex.europa.eu/LexUriServ/site/en/consleg/2004/L/02004L0039-20060428-en.pdf)	1	Final
MiFID Implementing Directive	Commission Directive 2006/73/EC of 10 August 2006 implementing Directive 2004/39/EC of the European Parliament and of the Council as regards organisational requirements and operating conditions for investment firms and defined terms for the purposes of that Directive (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:241:0026:0058:EN:PDF)	2	Final
Solvency II	Amended proposal for a Directive of the European Parliament and of the Council on the taking-up and pursuit of the business of Insurance and Reinsurance (recast), SOLVENCY II, 22 April 2009 (http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//NONSGML+TA+20090422+SIT-03+DOC+WORD+V0//EN&language=EN)	1	Draft
UCITS Directive	Council Directive 85/611/EC of 20 December 1985 on the coordination of laws, regulations and administrative provisions relating to undertakings for collective investment in transferable securities (UCITS) (http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31985L0611:EN:HTML)	1	Final (under revision)

II. SUMMARY OF RECOMMENDED HARMONISATION OPTIONS

Area	Desirable degree of harmonisation		
	High	Medium	Low
Corporate structure and organisation			
Lines of responsibility and accountability			✓
Conflicts of interest		✓	
Tasks and responsibilities of the management body		✓	
Record keeping and data quality aspects		✓	
Accounting systems and procedures			✓
"Four eyes" composition			✓
Committees and subcommittees and their terms of reference			✓

Area	Desirable degree of harmonisation		
	High	Medium	Low
Outsourcing		✓	
Risk management system			
Implementation of a risk management system			✓
Risk management function		✓	
Risks covered by the risk management systems		✓	
Risk assessment and stress testing			✓
Business continuity		✓	
Internal control system			
Implementation of an internal control system			✓
Compliance function		✓	
Internal audit function		✓	
Supervisory review, internal reporting and public disclosure			
Supervisory review process		✓	
Internal reporting requirements			✓
Disclosure, transparency and accountability issues			✓
Group structures and group specific issues			
Corporate structure and organisation			✓
Risk management system		✓	
Internal control system		✓	
Supervisory review, internal reporting and public disclosure			✓