

## Consultation Paper No. 33

### **Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: System of Governance**

*CEIOPS welcomes comments from interested parties on the following Consultation Paper "System of Governance".*

*Please send your comments to CEIOPS by email ([Secretariat@ceiops.eu](mailto:Secretariat@ceiops.eu)) by 8 June 2009, indicating the reference "CEIOPS-CP-33-09".*

*Please note that comments submitted after the deadline or not submitted in the provided template format, cannot be processed.*

*CEIOPS will make all comments available on its website, except where respondents specifically request that their comments remain confidential.*

# Table of contents

<b>1. Introduction .....</b>	<b>3</b>
<b>2. Extract from Level 1 text .....</b>	<b>4</b>
<b>3. Advice.....</b>	<b>10</b>
3.1. General Governance Requirements .....	10
3.2. Fit and Proper Requirements .....	15
3.3. Risk Management System.....	17
3.4. Internal Control.....	41
3.5. Internal Audit.....	45
3.6. Actuarial Function .....	48
3.7. Outsourcing .....	57
<b>4. Annexes.....</b>	<b>66</b>
Annex A: Main conclusions taken out from the QIS 4 OpRisk questionnaire .....	66
Annex B: Actuarial Function – Issues and options considered .....	67

## 1. Introduction

- 1.1. In its letter of 19 July 2007, the European Commission requested CEIOPS to provide final, fully consulted advice on Level 2 implementing measures by October 2009 and recommended CEIOPS to develop Level 3 guidance on certain areas to foster supervisory convergence.
- 1.2. This Consultation Paper aims at providing advice for Level 2 measures with regard to the System of Governance as requested in Article 49 of the General approach on the Solvency II Directive proposal adopted by the ECOFIN Council on 2 December 2008<sup>1</sup> ("Level 1 text"). It also includes material that could be considered for the future when developing Level 3 guidance.
- 1.3. CEIOPS believes that the Level 1 text already comprises a considerably high level of detail concerning principles and requirements on the system of governance, especially compared to the Level 1 text and/or Level 2 implementing measures in other EU directives on financial services. The text covers the most important issues to be regulated to ensure appropriate governance standards within insurance and reinsurance undertakings.
- 1.4. In view of this CEIOPS considers the scope for essential and extensive measures on Level 2 to be limited. Article 49 of the Level 1 text stipulates the minimum contents of the future Level 2 implementing measures. CEIOPS covers all the areas mentioned in the article but the level of detail depends on how detailed the Level 1 text already is in its requirements. Appropriate consideration was also given to the existing governance requirements for credit institutions and investment firms as set out in the regimes laid down in the Capital Requirements Directive (CRD) and the Markets in Financial Instruments Directive (MiFID).
- 1.5. The Level 1 text places considerable importance on written policies in relation to crucial aspects of the system of governance, in particular to risk management, internal control, internal audit and outsourcing. CEIOPS also expects to elaborate on these policies via Level 3 guidance and only addresses the required content of the asset-liability management and investment policies as these are explicitly singled out for implementing measures by Article 49 of the Level 1 text.
- 1.6. CEIOPS view is that details on how the principle of proportionality applies cannot be properly prescribed in a principles based system and accordingly does not propose any specific Level 2 implementing measures with regard to proportionality. This Consultation Paper does however address the principle, where appropriate, in order to give some indication as to how proportionality might play out in practice.
- 1.7. CEIOPS has, in the last months, deeply discussed several options when drafting the current Paper. However, only the main policy options considered regarding the actuarial function are explicitly reflected in the Paper (in paragraphs 3.253, 3.262 and 3.283), as the European Commission is conducting a formal impact assessment regarding this function.

---

<sup>1</sup>See <http://register.consilium.europa.eu/pdf/en/08/st16/st16237.en08.pdf> and <http://register.consilium.europa.eu/pdf/en/08/st16/st16237-co01.en08.pdf>.

- 1.8. In drafting its advice CEIOPS has also taken into consideration the lessons learnt from the financial crisis. These have been reflected in suggested Level 2 implementing measures or earmarked for further consideration under Level 3 guidance as appropriate.

## **2. Extract from Level 1 text**

- 2.1. According to the guiding principles referred to in the Commission's letter, the main basis for the advice presented in this paper is primarily found in Articles 38, 41, 42, 43 and 45 to 49 of the Level 1 text which state:

### Article 38 - Supervision of outsourced functions and activities

1. Without prejudice to Article 48, Member States shall ensure that insurance or reinsurance undertakings which outsource a function or an insurance or reinsurance activity (...) take the necessary steps to ensure that the following conditions are satisfied:

(a) the service provider must cooperate with the supervisory authorities of the insurance and reinsurance undertaking in connection with the outsourced function or activity;

(b) the insurance and reinsurance undertakings, their auditors and the (...) supervisory authorities must have effective access to data related to the outsourced functions or activities;

(c) the supervisory authorities must have effective access to the business premises of the service provider (...) and (...) must be able to exercise those rights of access.

2. The Member State where the service provider is located shall permit the supervisory authorities of the insurance or reinsurance undertaking to carry out themselves, or through the intermediary of persons they appoint for that purpose, on-site inspections at the premises of the service provider (...). The supervisory authority of the insurance or reinsurance undertaking shall inform the appropriate authority of the Member State of the service provider prior to conducting the on-site inspection. In the case of a non-supervised entity the appropriate authority shall be the supervisory authority.

The supervisory authorities of the Member State of the insurance or reinsurance undertaking may delegate such on-site inspections to the supervisory authorities of the Member State where the service provider is located.

- 2.2. Article 41 - General governance requirements

1. Member States shall require all insurance and reinsurance undertakings to have in place an effective system of governance which provides for sound and prudent management of the business.

That system shall at least include an adequate transparent organisational structure with a clear allocation and appropriate segregation of responsibilities

*and an effective system for ensuring the transmission of information. It shall include compliance with the requirements laid down in Articles 42 to 48.*

*The system of governance shall be subject to regular internal review.*

*2. The system of governance shall be proportionate to the nature, scale and complexity of the operations of the insurance or reinsurance undertaking.*

*3. Insurance and reinsurance undertakings shall have written policies in relation to at least risk management, internal control, internal audit and, where relevant, outsourcing. They shall ensure that those policies are implemented.*

*Those written policies shall be reviewed at least annually. They shall be subject to prior approval by the administrative or management body and be adapted in view of any significant change in the system or area concerned.*

*3a. Insurance and reinsurance undertakings shall take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To this end the undertaking shall employ appropriate and proportionate systems, resources and procedures.*

*4. The supervisory authorities shall have appropriate means, methods and powers for verifying the system of governance of the insurance and reinsurance undertakings and for evaluating emerging risks identified by those undertakings which may affect their financial soundness. The Member States shall ensure that the supervisory authorities have the powers necessary to require that the system of governance be improved and strengthened to ensure compliance with the requirements set out in Articles 42 to 48.*

**2.3. Article 42 - Fit and proper requirements for persons who effectively run the undertaking or have other key functions**

*1. Insurance and reinsurance undertakings shall ensure that all persons who effectively run the undertaking or have other key functions meet at all times the following requirements:*

*(a) their professional qualifications, knowledge and experience are adequate to enable sound and prudent management (fit);*

*(b) they are of good repute and integrity (proper).*

*2. Insurance and reinsurance undertakings shall notify the supervisory authority of any changes to the identity of the persons who effectively run the undertaking or are responsible for other key functions, along with all information needed to assess whether any new persons appointed to manage the undertaking are fit and proper.*

*3. Insurance and reinsurance undertakings shall notify their supervisory authority if any of the persons mentioned in paragraphs 1 and 2 have been replaced because they no longer fulfil the requirements referred to in (...) paragraph 1.*

## 2.4. Article 43 - Risk management

*1. Insurance and reinsurance undertakings shall have in place an effective risk management system comprising strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report, on a continuous basis the risks, on an individual and aggregated level, to which they are or could be exposed, and their interdependencies.*

*That risk management system shall be well integrated into the organisational structure and in the decision making processes of the insurance or reinsurance undertaking. (...)*

*2. The risk management system shall cover the risks to be included in the calculation of the Solvency Capital Requirement as set out in Article 101(4) as well as the risks which are not or not fully included in the calculation thereof.*

*It shall cover at least the following areas:*

*(a) underwriting and reserving;*

*(b) asset – liability management;*

*(c) investment, in particular derivatives and similar commitments;*

*(d) liquidity and concentration risk management;*

*(dbis) operational risk management;*

*(e) reinsurance and other risk mitigation techniques.*

*The written policy on risk management referred to in Article 41(3) shall comprise policies relating to points (a) to (e) of the second subparagraph of this paragraph.*

*3. As regards investment risk, insurance and reinsurance undertakings shall demonstrate that they comply with Chapter VI, Section 6.*

*4. Insurance and reinsurance undertakings shall provide for a risk management function which shall be structured in such a way as to facilitate the implementation of the risk management system.*

*5. For insurance and reinsurance undertakings using a partial or full internal model approved in accordance with Articles 110 and 111 the risk management function shall cover the following additional tasks:*

*(a) to design and implement the internal model;*

*(b) to test and validate the internal model;*

*(c) to document the internal model and any subsequent changes made to it;*

*(d) to inform the administrative or management body about the performance of the internal model, suggesting areas needing improvement, and up-dating that body on the status of efforts to improve previously identified weaknesses;*

*(e) to analyse the performance of the internal model and to produce summary reports thereof.*

2.5. Article 45 - Internal control

*1. Insurance and reinsurance undertakings shall have in place an effective internal control system.*

*That system shall at least include administrative and accounting procedures, an internal control framework, appropriate reporting arrangements at all levels of the undertaking and a (...) compliance function.*

*2. The compliance function shall include advising the administrative or management body on compliance with the laws, regulations and administrative provisions adopted pursuant to this Directive. It shall also include an assessment of the possible impact of any significant changes in the legal environment on the operations of the undertaking concerned and the identification and assessment of compliance risk.*

2.6. Article 46 - Internal audit

*1. Insurance and reinsurance undertakings shall provide for an effective (...) internal audit function.*

*2. (...)*

*The internal audit function shall (...) include an evaluation of the adequacy and effectiveness of the internal control system and other elements of the system of governance (...).*

*The internal audit function shall be objective and independent from the operational functions.*

*Any findings and recommendations of the internal audit shall be reported to the administrative or management body which shall determine what actions shall be taken with respect to each of the internal audit findings and recommendations and shall ensure that these actions are carried out.*

2.7. Article 47 - Actuarial function

*1. Insurance and reinsurance undertakings shall provide for an effective actuarial function to undertake the following:*

*(a) to coordinate the calculation of technical provisions;*

*(b) to ensure the appropriateness of the methodologies and underlying models used as well as the assumptions made in the calculation of technical provisions;*

*(c) to assess the sufficiency and quality of the data used in the calculation of technical provisions;*

- (d) to compare best estimates against experience;*
  - (e) to inform the administrative or management body of the reliability and adequacy of the calculation of technical provisions;*
  - (f) to oversee the calculation of technical provisions in the cases set out in Article 81;*
  - (g) to express an opinion on the overall underwriting policy;*
  - (h) to express an opinion on the adequacy of reinsurance arrangements;*
  - (i) to contribute to the effective implementation of the risk management system referred to in Article 43, in particular with respect to the risk modelling underlying the calculation of the capital requirements set out in Chapter VI, Sections 4 and 5 and the assessment referred to in Article 44.*
- 2. The actuarial function shall be carried out by persons with sufficient knowledge of actuarial and financial mathematics and able where appropriate, to demonstrate their relevant experience and expertise with applicable professional and other standards.*

## **2.8. Article 48 – Outsourcing**

- 1. Member States shall ensure that, when insurance and reinsurance undertakings outsource (...) functions or any insurance or reinsurance activities, the undertakings remain fully responsible for discharging all of their obligations under this Directive.*
- 2. Outsourcing of critical or important operational functions or activities shall not be undertaken in such a way as to lead to any of the following:*
  - (a) impairing materially the quality of the governance system of the undertaking concerned;*
  - (b) increasing unduly the operational risk;*
  - (c) impairing the ability of the supervisory authorities to monitor the compliance of the undertaking with its obligations;*
  - (d) undermining continuous and satisfactory service to policyholders.*
- 3. Insurance and reinsurance undertakings shall, in a timely manner, notify the supervisory authorities prior to the outsourcing of critical or important functions or activities as well as of any subsequent material developments with respect to those activities.*

2.9. Article 49 - Implementing measures

*The Commission shall adopt implementing measures to further specify the following:*

*(1) the elements of the systems referred to in Articles 41, 43, 45 and 46, and in particular the areas to be covered by the asset – liability management and investment policy, as referred to in Article 43(2), of insurance and reinsurance undertakings;*

*(2) the functions referred to in Articles 43, 45, 46 and 47;*

*(3) the requirements set out in Article 42 and the functions subject thereto;*

*(4) the conditions under which outsourcing may be performed.*

*Those measures designed to amend non-essential elements of this Directive by supplementing it, shall be adopted in accordance with the regulatory procedure with scrutiny referred to in Article 304(3).*

### **3. Advice**

#### **3.1. General Governance Requirements**

##### **Explanatory text**

3.1. Article 41(1) of the Level 1 text states:

*Member States shall require all insurance and reinsurance undertakings to have in place an effective system of governance which provides for a sound and prudent management of the business.*

*That system shall at least include an adequate transparent organisational structure with a clear allocation and appropriate segregation of responsibilities and an effective system for ensuring the transmission of information. It shall include compliance with the requirements laid down in Articles 42 to 48.*

*The system of governance shall be subject to regular internal review.*

3.2. It is important that undertakings ensure an organisational culture that enables and supports the effective operation of the system of governance. This requires an appropriate "tone at the top" with the administrative or management body and senior management providing appropriate organisational values and priorities.

3.3. The undertaking's system of governance should:

- a) Establish, implement and maintain effective cooperation, internal reporting and communication of information at all relevant levels;
- b) Be robust with a clear and well-defined organisational structure that has well-defined, clear, consistent and documented lines of responsibility across the organisation;
- c) Ensure that the members of the administrative or management body possess sufficient professional qualifications, knowledge and experience in the relevant areas of the business to give adequate assurance that they are collectively able to provide a sound and prudent management of the undertaking;
- d) Ensure it employs personnel with the skills, knowledge and expertise necessary for the proper discharge of the responsibilities allocated to them;
- e) Ensure all personnel are aware of the procedures for the proper discharge of their responsibilities;
- f) Establish, implements and maintains decision-making procedures;
- g) Ensure that any performance of multiple tasks by individuals does not and is not likely to prevent the persons concerned from discharging any particular function soundly, honestly and professionally;

- h) Establish information systems that produce sufficient, reliable, consistent, timely and relevant information concerning all business activities, the commitments assumed and the risks to which the undertaking is exposed;
  - i) Maintain adequate and orderly records of its business and internal organisation;
  - j) Safeguard the security and confidentiality of information, taking into account the nature of the information in question;
  - k) Introduce clear reporting lines that ensure the prompt transfer of information to all persons who need it in a way that enables them to recognise its importance; and
  - l) Establish and maintain adequate risk management, compliance, internal audit and actuarial functions, the characteristics of which are set out below.
- 3.4. Sound and prudent management of the business implies among other things a consistent application of risk management and internal control practices throughout the entire organisational structure of the undertaking. In order to support this goal, consideration should be given to drawing up and implementing a code of conduct for all staff.
- 3.5. Undertakings should ensure that any potential source of conflicts of interest is identified and procedures are established so that those involved with the implementation of the strategies and policies understand where conflicts of interest could arise and how these should be addressed, e.g. by establishing additional controls.
- 3.6. Undertakings should adopt an overall remuneration policy that is in line with its business strategy, risk profile and objectives. It should avoid potential incentives for unauthorised or unwanted risk taking. The remuneration policy should cover the undertaking as a whole and contain specific arrangements that take into account the respective roles of the administrative or management body and persons who have key functions.
- 3.7. Undertakings have to ensure that the system of governance is internally reviewed on a regular basis. To this purpose they have to determine the appropriate frequency of the reviews taking into account the nature, scale and complexity of their business and assign responsibility for the review.
- 3.8. In order to allow an adequate revision of the system of governance appropriate reporting procedures encompassing at least all key functions should be established. The reports to be produced shall encompass an assessment of the effectiveness of the system of governance and should contain suggestions for improvements. They should be presented to the administrative or management body at least annually, according to the principle of proportionality, and discussions on any challenge provided or improvements suggested should be documented as appropriate. Suitable feedback loops should exist to ensure follow-up actions are continuously undertaken and recorded.
- 3.9. In particular the report(s) mentioned in the previous paragraph should include the conclusions drawn from the own risk and solvency assessment and should include all relevant information on the risks the undertaking faces in the short and long term and to which it is or could be exposed.

- 3.10. CEIOPS does not intend to require or set any requirements on the format, content or structure of the report(s) to be produced.
- 3.11. Article 41(2) of the Level 1 text states:
- The system of governance shall be proportionate to the nature, scale and complexity of the operations of the insurance or reinsurance undertaking.*
- 3.12. The proportionality requirement applies to every element of the system of governance. It is the responsibility of the administrative or management body to ensure that the undertaking's organisational structure delivers a system of governance proportionate to the nature, scale and complexity of the risks it faces in its business activities.
- 3.13. Subject to national law requirements an undertaking's administrative or management body should consider whether a committee structure is appropriate and if so, what its mandate and reporting lines should be. For example, it could consider forming audit, risk, investment or remuneration committees to address these important issues.
- 3.14. Undertakings should ensure that the administrative or management body meets its responsibility for a robust system of governance that works effectively by taking the necessary measures to provide for an efficient running of the risks identified by the risk management function. Evidence of effective challenge and oversight by the administrative or management body should be documented.
- 3.15. Regarding the fulfilment of the internal audit function it should be noted that this cannot be combined with other operational duties or functions. According to Article 46(3) of the Level 1 text, the internal audit function shall be objective and independent from the operational functions. In effect this means that in the view of the majority of CEIOPS' members<sup>2</sup>, the internal audit function – in contrast to the other functions explicitly mentioned in the Level 1 text – needs to be a separate unit or an individual without other duties within the undertaking unless the function is outsourced. As stated in its advice to the European Commission on the Principle of Proportionality<sup>3</sup>. CEIOPS holds that, in order for this requirement not to create an unreasonable burden for undertakings with low risk profiles, these undertakings would not have to provide for a permanently operating function as part of their organisation but could commission a qualified party to execute these tasks.

---

<sup>2</sup> One Supervisory Authority holds that considering the principle of proportionality it is possible that the internal audit function is exercised by two members of the administrative or management body provided the undertaking ensures that neither audits their own specific areas of responsibility.

<sup>3</sup> See CEIOPS' Advice to the European Commission on the Principle of Proportionality in the Solvency II Framework Directive proposal, CEIOPS-DOC-24/08, May 2008, [http://www.ceiops.eu/media/docman/public\\_files/publications/submissionstotheec/AdviceProportionality.pdf](http://www.ceiops.eu/media/docman/public_files/publications/submissionstotheec/AdviceProportionality.pdf).

3.16. Article 41(3) of the Level 1 text states:

*Insurance and reinsurance undertakings shall have written policies in relation to at least risk management, internal control, internal audit and, where relevant, outsourcing. They shall ensure that those policies are implemented.*

*Those written policies shall be reviewed at least annually. They shall be subject to prior approval by the administrative or management body and be adapted in view of any significant change in the system or area concerned.*

3.17. The policies on risk management, internal control, internal audit and, where relevant, outsourcing, shall clearly set out the relevant responsibilities, goals, processes and reporting procedures to be applied, all of which shall be in line with the undertaking's overall business strategy.

3.18. Proper implementation of the written policies requires ensuring that all staff members are familiar with the policies relevant for their area of activities.

3.19. CEIOPS interprets the requirement for prior approval by the administrative or management body to apply to any changes with regard to the content of the policies.

3.20. As a rule an annual review would be considered sufficient, unless the system or area concerned undergo significant change.

3.21. Article 41(3a) of the Level 1 text states:

*Insurance and reinsurance undertakings shall take reasonable steps to ensure continuity and regularity in the performance of their activities, including the development of contingency plans. To this end the undertaking shall employ appropriate and proportionate systems, resources and procedures.*

3.22. Undertakings shall develop and document contingency plans to ensure the business disruption and/or possible losses are limited if there is an unforeseen interruption to their systems and procedures. These might for example arise from natural catastrophes such as floods or earthquakes, terrorist attacks, serious fires, a breakdown of the IT systems or a pandemic that affects a large number of employees. Undertakings shall regularly identify the risks for which contingency plans should be in place taking into account the areas where they consider themselves to be especially vulnerable.

3.23. The plans shall be regularly tested and updated to ensure that they are and remain effective, and communicated to the relevant management and staff.

### **CEIOPS' advice**

3.24. The undertaking's system of governance shall:

- a) Establish, implement and maintain effective cooperation, internal reporting and communication of information at all relevant levels within the undertaking;

- b) Be robust with a clear and well-defined organisational structure that has well-defined, clear, consistent and documented lines of responsibility across the organisation;
- c) Ensure that the members of the administrative or management body possess sufficient professional qualifications, knowledge and experience in the relevant areas of the business to give adequate assurance that they collectively are able to provide a sound and prudent management of the undertaking;
- d) Ensure it employs personnel with the skills, knowledge and expertise necessary for the proper discharge of the responsibilities allocated to them;
- e) Ensure all personnel are aware of the procedures for the proper discharge of their responsibilities;
- f) Establish, implements and maintains decision-making procedures;
- g) Ensure that any performance of multiple tasks by individuals does not and is not likely to prevent the persons concerned from discharging any particular function soundly, honestly and professionally;
- h) Establish information systems that produce sufficient, reliable, consistent, timely and relevant information concerning all business activities, the commitments assumed and the risks to which the undertaking is exposed;
- i) Maintain adequate and orderly records of its business and internal organisation;
- j) Safeguard the security, integrity and confidentiality of information, taking into account the nature of the information in question;
- k) Introduce clear reporting lines that ensure the prompt transfer of information to all persons who need it in a way that enables them to recognise its importance; and
- l) Establish and maintain adequate risk management, compliance, internal audit and actuarial functions.

3.25. Undertakings should ensure that any potential source of conflicts of interest is identified and procedures are established so that those involved with the implementation of the strategies and policies understand where conflicts of interest could arise and how these should be addressed, e.g. by establishing additional controls.

3.26. The policies on risk management, internal control, internal audit and, where relevant, outsourcing, shall clearly set out the relevant responsibilities, goals, processes and reporting procedures to be applied, all of which should be in line with the undertaking's overall business strategy.

3.27. The undertaking shall regularly identify the risks for which contingency plans should be in place taking into account the areas where they consider themselves to be especially vulnerable.

3.28. The plans shall be regularly tested and updated to ensure that they are and remain effective, and communicated to the relevant management and staff.

## 3.2. Fit and Proper Requirements

### Explanatory text

3.29. Article 42 of the Level 1 text states:

*Insurance and reinsurance undertakings shall ensure that all persons who effectively run the undertaking or have other key functions meet at all times the following requirements:*

*(a) Their professional qualifications, knowledge and experience are adequate to enable sound and prudent management (fit);*

*(b) They are of good repute and integrity (proper).*

*Insurance and reinsurance undertakings shall notify the supervisory authority of any changes to the identity of the persons who effectively run the undertaking or are responsible for other key functions, along with all information needed to assess whether any new persons appointed to manage the undertaking are fit and proper.*

*Insurance and reinsurance undertakings shall notify their supervisory authority if any of the persons mentioned in paragraphs 1 and 2 have been replaced because they no longer fulfil the requirements referred to in paragraph 1.*

3.30. The provisions of Article 42(1) apply to all persons who effectively run the undertaking. These are not limited to the members of the administrative or management body, but could include other persons such as senior managers<sup>4</sup>.

3.31. The other "key functions" are those considered critical or important in the system of governance and include risk management, compliance, internal audit and actuarial functions. Other functions may be considered key functions according to the nature, scale and complexity of an undertaking's business or the way it is organised.

3.32. Undertakings need to establish who the persons that effectively run the undertaking are and which functions they consider key for their business including those set out in the previous paragraph. When deciding on the persons falling under the provisions of Article 42, the nature, scale and complexity of the risks inherent in the business of the undertaking should be taken into account as well as the way the undertaking is organised.

3.33. Undertakings shall notify the supervisory authority which persons effectively run the undertaking and which, if any, other key function holders are identified for the undertaking.

3.34. What is required by each key function holder by way of professional qualifications, knowledge and experience depends on the function, as well as on the nature, scale and complexity of the business.

---

<sup>4</sup> In general terms, senior management could include persons employed by the undertaking who are responsible for high level decision making and implementing the strategies devised by and the policies approved by the administrative or management body.

- 3.35. Apart from qualifications that enable them to discharge the duties of their specific area of responsibility the members of the administrative or management body should, collectively, be able to provide for the sound and prudent management of the undertaking.
- 3.36. Regarding the propriety requirement, all persons subject to Article 42 should each be proper. The proportionality principle does not result in different standards in the case of the propriety requirement, since the repute and integrity of the persons who effectively run the undertaking or hold key functions should always be on the same adequate level irrespective of the nature, scale and complexity of the business or of the undertaking's risk profile.
- 3.37. In order to ensure that all persons subject to Article 42 are proper and have the professional qualifications, knowledge and experience necessary to competently discharge their responsibilities, the undertaking needs to have in place appropriate documented policies and processes for assessing fitness and propriety. CEIOPS expects to develop criteria for assessing such policies and processes on Level 3.
- 3.38. The Level 1 text requires undertakings to notify the supervisory authority whenever the identity of persons effectively running the undertaking or responsible for other key functions changes.
- 3.39. CEIOPS understands the scope of persons for whom information is to be submitted to enable the supervisory authority to assess their fitness and propriety to be the same as the scope of the notification requirement. This implies, as a minimum, sufficient information to enable the supervisory authority to assess the fitness and propriety of persons who effectively run the undertaking and are responsible for "other key functions" as defined in paragraph 3.31, and may in addition include information regarding the fitness and propriety of persons responsible for key functions other than those defined in paragraph 3.31, depending on the nature, scale and complexity of the business.
- 3.40. CEIOPS will develop detailed guidance for assessing fitness and propriety on Level 3 taking into account existing 3L3 work in this area.
- 3.41. Undertakings are required to notify their supervisory authority after a person subject to Article 42 has been replaced because they no longer fulfil the fitness and propriety requirements. CEIOPS expects to harmonise the particulars of this notification process on Level 3.

### **CEIOPS' advice**

- 3.42. Undertakings shall have in place documented policies and procedures to ensure that all persons subject to Article 42 are fit and proper.
- 3.43. Key functions are those considered important and critical in the system of governance and include risk management, compliance, internal audit and actuarial functions. Other functions may be considered key functions according to the nature, scale and complexity of an undertaking's business or the way it is organised.

3.44. Undertakings shall notify the supervisory authority of the persons who effectively run the undertaking and which, if any, other key function holders are identified for the undertaking.

### **3.3. Risk Management System**

#### **Explanatory text**

3.45. Article 43(1) of the Level 1 text states:

*Insurance and reinsurance undertakings shall have in place an effective risk management system comprising strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report, on a continuous basis the risks, on an individual and aggregated level, to which they are or could be exposed, and their interdependencies.*

*That risk management system shall be well integrated into the organisational structure and in the decision making process of the insurance or reinsurance undertaking.*

3.46. Risk management is a continuous process that should be used in the implementation of the undertaking's overall strategy and should allow an appropriate understanding of the nature and significance of the risks to which the undertaking is exposed. The administrative or management body is responsible for ensuring that the implemented risk management system is suitable, effective and proportionate to the nature, scale and complexity of the risks inherent in the business.

3.47. To underline the importance of risk management and increase accountability, undertakings should designate a member of the administrative or management body to oversee the risk management function and ensure the development and on-going maintenance of an effective risk management system within the undertaking that is effective and proportionate to the nature, scale and complexity of the risks inherent in the business. CEIOPS expects that at least in large undertakings and undertakings with more complex risk profiles a Chief Risk Officer (CRO) is appointed.

3.48. The administrative or management body is also responsible for the approval of any periodic revision of the main strategies and business policies of the undertaking in terms of risk management.

3.49. CEIOPS understands "strategies" as high level plans that are developed by the administrative or management body and are further specified via policies and business plans to ensure implementation in day-to-day business. "Policies" are internal guidelines established by senior management in line with the relevant strategies to outline the framework that staff has to take into account when exercising their responsibilities.

3.50. The risk management system needs to be documented and communicated to relevant management and staff to ensure it is embedded within the business.

3.51. An effective risk management system covers all material risks and requires at

least the following:

- a) A clearly defined and well documented risk management strategy that includes the objectives, key principles, risk appetite and assignment of responsibilities across all the activities of the undertaking and is consistent with the undertaking's overall business strategy;
- b) Adequate written policies that include a definition and categorisation of the risks faced by the undertaking, by type, and the levels of acceptable risk limits for each risk type, implement the undertaking's risk strategy, facilitate control mechanisms and take into account the nature, scope and time horizon of the business;
- c) Appropriate processes and procedures which enable the undertaking to identify, assess, manage, monitor and report the risks it is or might be exposed to;
- d) Appropriate reporting procedures and feedback loops that ensure that information on the risk management system, which is coordinated and challenged by the risk management function is continuously monitored and managed by all relevant staff and the administrative or management body;
- e) Reports that are submitted to the administrative or management body by the risk management function on the material risks faced by the undertaking and on the effectiveness of the risk management function;
- f) An appropriate own risk and solvency assessment (ORSA) process<sup>5</sup>.

3.52. The risk management system shall be integrated into the organisational structure of the undertaking and into its decision making processes. Good integration includes, in particular, that the risk management system should be supported by a suitable internal control system. The design and operational effectiveness of the risk management system to identify, measure, and monitor risks the undertaking is exposed to shall be regularly evaluated and reported by the risk management function.

### **CEIOPS' advice**

3.53. An effective risk management system requires at least the following:

- a) A clearly defined and well documented risk management strategy that includes the risk management objectives, key principles, risk appetite and assignment of risk management responsibilities across all the activities of the undertaking and is consistent with the undertaking's overall business strategy;
- b) Adequate written policies that include a definition and categorisation of the risks faced by the undertaking, by type, and the levels of acceptable risk

---

<sup>5</sup> See CEIOPS' Issues Paper on the Own Risk and Solvency Assessment, CEIOPS-IGSRR-09/08, May 2008, [http://www.ceiops.eu/media/docman/public\\_files/consultations/IssuesPaperORSA.pdf](http://www.ceiops.eu/media/docman/public_files/consultations/IssuesPaperORSA.pdf).

limits for each risk type, implement the undertaking's risk strategy, facilitate control mechanisms and take into account the nature, scope and time horizon of the business and the risks associated with it;

- c) Appropriate processes and procedures which enable the undertaking to identify, assess, manage, monitor and report the risks it is or might be exposed to;
- d) Appropriate reporting procedures and feedback loops that ensure that information on the risk management system, which is coordinated and challenged by the risk management function is continuously monitored and managed by the administrative or management body.
- e) Reports that are submitted to the administrative or management body by the risk management function on the material risks faced by the undertaking and on the effectiveness of the risk management function;
- f) A suitable own risk and solvency assessment (ORSA) process.

## **Areas to be covered by the risk management system**

### **Explanatory text**

3.54. Article 43(2) and (3) of the Level 1 text states:

*2. The risk management system shall cover the risks to be included in the calculation of the Solvency Capital Requirement as set out in Article 101(4) as well as the risks which are not or not fully included in the calculation thereof.*

*It shall cover at least the following areas:*

- (a) underwriting and reserving;*
- (b) asset – liability management;*
- (c) investment, in particular derivatives and similar commitments;*
- (d) liquidity and concentration risk management;*
- (dbis) operational risk management;*
- (e) reinsurance and other risk mitigation techniques.*

*The written policy on risk management referred to in Article 41(3) shall comprise policies relating to points (a) to (e) of the second subparagraph of this paragraph.*

*3. As regards investment risk, insurance and reinsurance undertakings shall demonstrate that they comply with Chapter VI, Section 6.*

3.55. Article 49(1) requires the Commission to adopt implementing measures specifying amongst others the risk management system and in particular the

areas to be covered by the asset-liability management and investment policies of undertakings, as referred to in Article 43(2). CEIOPS considers the Level 1 text to be quite clear with regard to the areas to be covered by risk management. Undertakings have to establish a risk management system that includes all relevant risks they might be exposed to whether they are covered by the areas explicitly referred to in Article 43(2) or not. CEIOPS does however propose that risks whose importance has been highlighted by the current financial crisis be taken into account on Level 2 in order to ensure that they receive due consideration by undertakings.

- 3.56. Concerning the written policies that need to be established in relation to points (a) to (e) of the second subparagraph of Article 43(2), this Paper only focuses on the asset-liability management and investment policies as these are of crucial importance for an effective risk management and are specifically singled out for implementing measures by Article 49 of the Level 1 text. CEIOPS intends to cover supervisory expectations on the contents of the other written policies in future Level 3 guidance on the system of governance.
- 3.57. The risk management system of the undertaking should cover not only the risks included in the SCR, as per Article 101(4) of the Level 1 text, but also all other risks that may be considered materially relevant in the context of the undertaking's business.
- 3.58. In this Paper CEIOPS does not follow the risk categorisation of the standard formula but rather addresses the areas to be covered at a minimum by the risk management system as prescribed by Article 43(2) first subparagraph.

Credit risk management is addressed additionally in the paper together with the potentially most relevant "other risks" an undertaking may be exposed to, e.g. strategic and reputational risk. CEIOPS expects to elaborate further on these and possibly on more "other risks" not mentioned here, in its Level 3 guidance.

### ***Risk areas specifically identified in Article 43(2)***

- 3.59. The risk management system is required to include at least the following areas:

#### **- Underwriting and reserving**

##### **Explanatory text**

- 3.60. Underwriting risk refers to the risk of loss, or of adverse change in the value of insurance liabilities, due to inadequate pricing and reserving assumptions.
- 3.61. Underwriting and reserving risk includes the fluctuations in the timing, frequency and severity of insured events, relative to the expectations of the undertaking at the time of underwriting. This risk can also refer to fluctuations in the timing and amount of claims settlements.

- 3.62. A proper strategy for underwriting and reserving risk should include at least:
- a) The classes and characteristics of the insurance business (i.e. the type of insurance risk) the undertaking is willing to accept;
  - b) The undertaking's exposure to specific risk concentrations;
  - c) Internal underwriting limits;
  - d) The adequacy of premium income to cover expected claims and expenses;
  - e) The investment policy;
  - f) Reinsurance and other risk mitigation strategies and their effectiveness; and
  - g) The identification of the risks arising from all its insurance obligations, including embedded options and guaranteed surrender values in the products, and the resulting capital requirements of its exposures.
- 3.63. Suitable processes and procedures should be in place to ensure the reliability, sufficiency and adequacy of both the statistical and accounting data to be considered both in the underwriting and reserving processes.
- 3.64. The undertaking should ensure that all policies and procedures established for underwriting and reserving are applied by all distribution channels of the undertaking insofar as they are relevant for them.
- 3.65. The processes to be established should include reliable methods for evaluation of the methods chosen, e.g. back-testing of the methods used against statistical data such as the run-off of claims provisions.
- 3.66. The undertaking should have in place adequate claims management procedures which should cover the overall cycle of claims: reception, assessment, procession and settlement, complaints and dispute settlement and reinsurance recoverables.

### **CEIOPS' advice**

- 3.67. Suitable processes and procedures should be in place to ensure the reliability, sufficiency and adequacy of both the statistical and accounting data to be considered both in the underwriting and reserving processes.
- 3.68. The undertaking should ensure that all policies and procedures established for underwriting and reserving are applied by all distribution channels of the undertaking insofar as they are relevant for them.
- 3.69. The undertaking should have in place adequate claims management procedures which should cover the overall cycle of claims: reception, assessment, procession and settlement, complaints and dispute settlement and reinsurance recoverables.

## **- Asset-liability management**

### **Explanatory text**

- 3.70. Asset-liability management (ALM) is the management of a business in such a way that decisions on assets and liabilities are coordinated in order to manage the exposure to the risk associated with the variation of their economic values.
- 3.71. Along with the investment strategy, an ALM strategy should describe how financial and insurance risks will be managed in an asset-liability framework in the short, medium and long term. The ALM strategy should be linked to market risk and liquidity risk management.
- 3.72. The ALM strategy should usefully have regard to at least:
- a) The structure of the asset-liability approach, including the time horizon;
  - b) The portfolio of assets and liabilities, including obligations to pay bonuses to policyholders;
  - c) The stress tests to be performed to ascertain of adverse movements in the undertaking's investment portfolio and asset-liability positions;
  - d) A validation of parameters and hypotheses by comparison with earlier observations (back-testing); and
  - e) The interaction between the ALM policy and the investment policy.
- 3.73. When choosing from the different ALM techniques available for measuring risk exposure, an undertaking should rely on measurement tools that are consistent with the risk characteristics of the lines of business and its risk tolerance. The undertaking should also take into account its ALM objectives and the sophistication of its management information system.
- 3.74. In order to provide for the effective management of assets and liabilities, the undertaking should ensure appropriate and continuing liaison between the different areas within its business involved in the ALM.
- 3.75. The ALM framework should not only recognise the interdependence between assets and liabilities but also take into account the correlation of risks between different asset classes and the correlations between different products and business lines.
- 3.76. Undertakings should also have regard to any off-balance sheet exposures that they may have.
- 3.77. The undertaking should have effective procedures for monitoring and managing the asset-liability positions and to ensure that investment activities and asset positions are appropriate to the risk profile of its liabilities.
- 3.78. When introducing new products, the undertaking should consider how these affect the management of assets and liabilities.

## **Policy on asset-liability management**

- 3.79. The undertaking shall develop written ALM policies that especially take into account the interrelation with other types of risks, such as liquidity and underwriting risks, and establish ways to manage the possible effect of options embedded in the insurance products.
- 3.80. Hence, the ALM policy shall provide for:
- a) A structuring of the assets that ensures the undertaking holds sufficient cash and diversified marketable securities of an appropriate nature, term and liquidity to meet its obligations as they fall due;
  - b) A plan to deal with unexpected cash outflows; and
  - c) The identification of mitigation techniques and their impact on embedded options, and the assessment of the possible effects these can have throughout the life of the insurance policies.
- 3.81. The undertaking shall tailor its ALM policies to the needs of different product lines and combine the ALM policies appropriately in order to optimise the overall ALM management.

## **CEIOPS' advice**

- 3.82. The undertaking shall develop written ALM policies that especially take into account the interrelation with other types of risks, such as liquidity and underwriting risks, establish ways to manage the possible effect of options embedded in the products, provide for a structuring of the assets that ensures the undertaking holds sufficient cash and diversified marketable securities of an appropriate nature, term and liquidity to meet its obligations as they fall due.
- 3.83. The undertaking shall tailor its ALM policies to the needs of different product lines and combine the ALM policies appropriately in order to optimise the overall ALM management.
- 3.84. The ALM framework should not only recognise the interdependence between assets and liabilities but also take into account the correlation of risks between different asset classes and the correlations between different products and business lines.
- 3.85. Undertakings should also have regard to any off-balance sheet exposures that they may have.

## **- Investment, including derivatives and similar commitments**

### **Explanatory text**

- 3.86. Investments are subject to market risk. Market risk is the risk of loss, or of adverse change in the financial situation, resulting directly or indirectly from

fluctuations in the level and in the volatility of market prices of assets, liabilities and financial instruments.

- 3.87. Undertakings shall, according to the "prudent person" principle as specified in Article 130(2) of the Level 1 text, only invest in assets and instruments which they can properly monitor, manage and control. This requires them to identify assets and investments that are appropriate for them to fulfil the "prudent person" principle.
- 3.88. Hence undertakings must thoroughly understand the products they want to invest in, and for complex products should preferably use in risk management models that consider all relevant variables.
- 3.89. Further, special management monitoring and controls should be established for complex investments activities where the (re)insurance undertaking is taking on a higher risk profile.
- 3.90. An undertaking should consider all risks arising from its investments and their relationship with its liabilities that are significant in terms of their potential impact on the economic value of its operations.
- 3.91. If the risks arising from the investments are not adequately covered by the standard formula quantitative limits and asset eligibility criteria may in the future be developed under Level 2 by the Commission in order to address those risks. In any case undertakings should appropriately identify and assess these risks under their ORSA.
- 3.92. Undertakings need to be more aware of the risks embedded in the assets they are buying. This is particularly important in the case of complex structured products. In this regard it is not sufficient that the undertaking defines quantitative limits on assets as the undertaking still has to consider what risks are included in these complex products.
- 3.93. On that basis, CEIOPS would rather evoke the Prudent Person principle and believes that the restrictive use of quantitative limits remains appropriate under the Solvency II regime. Supervisors would expect to find investment policies in place, including internal limits settled by the undertakings, both on volume and on types of assets with the aim of managing risks in an appropriate manner and protect the interests of policyholders.
- 3.94. In order to ensure a proper risk management of investments, the undertaking shall develop a detailed investment strategy that should usefully at least have regard to:
  - a) The financial market environment (including historic and anticipated future environment);
  - b) Its solvency position;
  - c) Liquidity risk;
  - d) Concentration risk;
  - e) Credit risk;

- f) Asset and liability considerations, including interrelation with the asset–liability management strategy;
- g) Asset classes and strategic asset allocation;
- h) Conditions under which the undertaking can pledge or lend assets;
- i) The amount of delegated limits by management level;
- j) The use of derivatives, asset-backed securities, collateralised debt obligations, hedge funds or any other financial instrument with similar characteristics;
- k) The link between market risk and other risks in highly adverse scenarios (e.g. a pandemic);
- l) The independent and appropriate valuation of its investment assets;
- m) Procedures to monitor the performance and review the strategy when necessary; and
- n) Additional constraints to the investment strategy, such as e.g. P&L targets.

3.95. Special management, monitoring and control procedures and appropriate independent valuation of the undertaking’s investment assets is of crucial importance in relation to investments that are not quoted in a market, especially in relation to complex structured products.

3.96. Where mark to model valuation is applied undertakings should devote sufficient resources, both in terms of quality and quantity, to model approval and review, independent price verification and stress testing, as well as to internal control processes. On a regular basis, undertakings should assess the need to develop back-up valuation models for complex or potentially illiquid instruments.

3.97. Undertakings need to have access to basic expertise in order to understand, monitor and steer structured products and their embedded risks. Also, the undertaking needs procedures to evaluate hidden and non-standard risks associated with these products, especially new concentration risks that may not be obvious.

3.98. Undertakings should understand and be able to evaluate their own investments according to Solvency II valuation principles and should not depend solely on the valuation provided by the financial institution that has initially priced that investment or on a rating assigned by a rating agency.

3.99. Regarding holdings of derivative products or any other financial instrument with similar characteristics<sup>6</sup> (“similar commitments”) such as e.g. asset-backed securities, collateralised debt obligations and hedge funds, the investment strategy shall clearly identify:

- a) Goals and strategies of the use of derivatives and similar commitments and the way they contribute to an efficient portfolio management;

---

<sup>6</sup>In the context of derivatives, CEIOPS interprets the expression “similar commitments” to refer to financial instruments whose attendant risks are sometimes difficult to determine and whose proper management requires specific expertise.

- b) The evaluation of the strategy to use this type of products;
  - c) The principles of liquidity risk management for derivatives and similar commitments, including stress tests;
  - d) The principles of risk management with regard to derivatives and similar commitments.
- 3.100. Exposure limits for counterparty credit risk and risk class for derivatives and similar commitments should be integrated into the overall limits set out in the undertaking's investment strategy.
- 3.101. When undertakings invest in SPVs<sup>7</sup>, either their own SPVs or those established by other insurance undertakings, the following principles should be considered, taking into account the requirements and guidelines set out in CEIOPS Consultation Paper on Special Purpose Vehicles<sup>8</sup>:
- a) Special ALM procedures should be established as these assets may expose the undertaking to both asset risk (credit spread, market concentration risk, etc.) and to insurance risk as well (if the SPV was established by another (re)insurance undertaking). Specific stress tests may be constructed, namely CAT scenarios; and
  - b) Special attention should be given to assets issued by ISPV with whom the undertaking has reinsurance contracts established (self securitisation).

### **Policy on investment, including derivatives and similar commitments**

- 3.102. Compliance with the "prudent person" principle as stipulated according to Article 130(1) of the Level 1 text includes that an investment policy shall be defined based on the rules and procedures that a competent, prudent and expert manager would apply in order to pursue the investment strategy.
- 3.103. The investment policy shall ensure that the undertaking holds assets with sufficient values and enough liquidity to meet all liabilities and enable payments as they fall due. The assets should also be appropriate so that the policyholders are not exposed to undue risk.
- 3.104. The investment policy shall take into account the undertaking's business, its overall risk tolerance levels, the solvency position, the long-term risk-return requirements and its underlying exposure (gross and net of offsetting transactions).
- 3.105. When undertakings use derivative products, asset-backed securities and collateralised debt obligations, hedge funds or any other financial instrument with similar characteristics the investment policy shall take into account the goals and strategies of their use and the way they contribute to an efficient portfolio management, as well as procedures to evaluate the strategy to use this

---

<sup>7</sup> This means an SPV according to Article 13 (22) of the Level 1 text.

<sup>8</sup> See Consultation Paper No.36 "Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Special Purpose Vehicles (CEIOPS-CP-36/09, 26 March 2009), <http://www.ceiops.eu/content/view/14/18/>.

type of products and the principles of risk management to be applied.

- 3.106. In its policy on investment the undertaking shall also consider how to prudently manage liquidity risk, in the short as well as in the medium and long term, taking into account the investment strategy, overall underwriting strategy and claims management.
- 3.107. The investment policy shall include internal quantitative limits on assets.

### **CEIOPS' advice**

- 3.108. The undertaking shall define its investment policy in line with what a competent, prudent and expert manager would apply in order to pursue the investment strategy.
- 3.109. The investment policy shall take into account the undertaking's business, its overall risk tolerance levels, the solvency position and the long-term risk-return requirements and its underlying exposure (gross and net of offsetting transactions).
- 3.110. Special management procedures, monitoring and controls should be established for complex investment activities where the undertaking is taking on a higher risk profile.
- 3.111. When undertakings use derivative products or any other financial instrument with similar characteristics, such as asset-backed securities, collateralised debt obligations or hedge funds, the investment policy shall take into account the goals and strategies of their use and the way they contribute to an efficient portfolio management as well as procedures to evaluate the strategy to use this type of products and the principles of risk management to be applied.
- 3.112. In its policy on investment the undertaking shall also consider how to prudently manage liquidity risk in the short as well as in the medium and long term, taking into account the investment strategy, overall underwriting strategy and claims management.
- 3.113. The investment policy shall include quantitative limits on assets.

### **- Liquidity risk management**

#### **Explanatory text**

- 3.114. Liquidity risk refers to the risk that undertakings are unable to realise investments and other assets in order to settle their financial obligations when they fall due.
- 3.115. Liquidity in this context is the availability of funds, or certainty that funds will be available without significant losses, to honour all cash outflow commitments (both on and off-balance sheet) as they fall due. These commitments are generally met through cash inflows, supplemented by assets readily convertible

to cash.

- 3.116. It is the undertaking's responsibility to have sound liquidity management practices which cover both short and long term considerations. Short term liquidity, or cash management, covers the day-to-day cash requirements under normally expected or likely business conditions. Liquidity considerations over a long term need to be assessed in a way which recognises the possibility of various unexpected and potentially adverse business conditions (stress tests and scenario analyses) where asset values may not be realised for current market values.
- 3.117. The undertaking shall have in place a liquidity contingency plan that includes:
- a) The continuous monitoring of the undertaking's debt position;
  - b) The identification of the available financing options, including reinsurance, the negotiation of credit lines, committed borrowing facilities and intra-group financing;
  - c) A regular review and testing of these options, both in normal and adverse situations.
- 3.118. In order to ensure a proper risk management of the liquidity risk the undertaking should develop a detailed strategy that should usefully have regard to at least:
- a) The level of mismatch between the cash inflows and the cash outflows of both assets and liabilities;
  - b) The level of mismatch of the expected cash flows of direct insurance and reinsurance;
  - c) The total liquidity needs in the short and medium term including an appropriate buffer for liquidity shortfall;
  - d) The level and monitoring of liquid assets, including a quantification of potential costs or financial losses arising from an enforced realisation;
  - e) The cost of financing and the identification of other financing tools and the associated costs; and
  - f) Projections of cash outflows arising from the insurance activity, such as claims, lapses or surrenders, and evaluation of the uncertainty of timing and amount of the insurance liabilities.

### **CEIOPS' advice**

3.119. It is the undertaking's responsibility to have sound liquidity management practices which cover both short term and long term considerations and include stress test and scenario analyses.

3.120. The undertaking shall have in place a liquidity contingency plan that includes:

- a) The continuous monitoring of the undertaking's debt position Analysis of the undertaking's debt capacity;

- b) Identification of the available financing options, including reinsurance, the negotiation of credit lines, committed borrowing facilities and intra-group financing;
- c) A regular review and testing of these options, both in normal and adverse situations.

## **Concentration risk management**

### **Explanatory text**

- 3.121. Concentration risk means all risk exposures with a loss potential which is large enough to threaten the solvency or the financial position of undertakings.
- 3.122. Such exposures may be caused for example by credit risk, market risk, underwriting risk, liquidity risk, other risks, or a combination or interaction of those risks by counterparty, industry or geographical area.
- 3.123. As part of the approach to concentration risk, the undertaking should develop a detailed strategy that, at a minimum, should take account of:
- a) Policies on underwriting;
  - b) Investments; and
  - c) Reinsurance and other risk mitigation techniques.
- 3.124. Concentration risk can arise in both the assets and liabilities sides of the balance sheet of the undertaking, as well as in off-balance sheet items and can originate from a series of sources, including geographical areas, (entity or group) counterparties, economic sectors, types of products, providers of services, reinsurance and cumulative exposures in the insurance contracts (both explicit and embedded).
- 3.125. In order to properly manage concentration risk undertakings shall define relevant sources of risk concentration like the relevant sectors and geographical areas to be taken into account. Undertaking shall make use of internal limits, thresholds or similar concepts that are appropriate with regard to their overall risk management.
- 3.126. Undertakings need to have in place adequate procedures and processes for the active monitoring and management of concentration risk to ensure that it stays within established policies and limits and mitigating actions can be taken as necessary. The monitoring of concentration risk shall include an analysis of possible contagion lines.
- 3.127. Where it is proportionate to the nature, scale and complexity of an undertaking's risk profile it should consider common or correlating underlying factors in order to identify correlations in the probability of defaults or risks crystallizing.

## **CEIOPS' advice**

- 3.128. In order to properly manage concentration risk undertakings shall define the relevant sources of risk concentration like the relevant sectors and geographical areas to be taken into account. Undertakings shall make use of internal limits, thresholds or similar concepts that are appropriate with regard to their overall risk management.
- 3.129. Undertakings need to have in place adequate procedures and processes for the active monitoring and management of concentration risk to ensure that it stays within established policies and limits and mitigating actions can be taken as necessary. The monitoring of concentration risk shall include an analysis of possible contagion lines.

## **Operational risk management**

### **Explanatory text**

- 3.130. While defining the requirements for the management of operational risk, CEIOPS has taken into account the main conclusions that were achieved as a result of the questionnaire on operational risk that was presented to undertakings in the context of the QIS4 exercise. These conclusions, as published in the QIS4 Report<sup>9</sup>, are presented in Annex A.
- 3.131. Operational risk refers to the risk of loss arising from inadequate or failed internal processes, or from personnel and systems, or from external events.
- 3.132. As set out in Article 101 of the Level 1 text, this definition includes legal risk, but excludes risks arising from strategic decisions and reputation risk. The definition does not preclude undertakings from articulating what constitutes operational risk differently for the purposes of the undertakings' operational risk policies and procedures.
- 3.133. The undertaking should have a well-documented assessment and management system for operational risk, with clear responsibilities assigned.
- 3.134. The administrative or management body should be aware of the major categories and exposures of the undertaking's operational risks as a distinct risk category that should be managed, and should approve, implement and periodically review the undertaking's operational risk management framework.

This framework should include:

- a) An undertaking-wide definition of operational risk. Without prejudice to the definition given above, undertakings shall articulate what constitutes operational risk for the purposes of their policies and procedures;
- b) Effective processes to identify, assess, mitigate, manage, monitor and

---

<sup>9</sup> CEIOPS' Report on its fourth Quantitative Impact Study (QIS4) for Solvency II, CEIOPS-SEC-82/08, November 2008, <http://www.ceiops.eu/media/files/consultations/QIS/CEIOPS-SEC-82-08%20QIS4%20Report.pdf>.

report the operational risks the undertaking is, or might be, exposed to and adequate internal control mechanisms; and

- c) The arrangements, processes and mechanisms detailed above should be comprehensive and proportionate to the nature, scale and complexity of the undertaking's activities.

3.135. In order to ensure a proper risk management of operational risk, the undertaking should develop a detailed strategy that should usefully take into account:

- a) The entire activities and internal processes in place in the undertaking, including any IT system supporting them;
- b) The operational risk events it is or might be exposed to and the way to mitigate them;
- c) The need for an early warning system that allows for an effective intervention.

3.136. The undertaking shall implement an effective process to regularly identify, document and monitor exposure to operational risk and track relevant operational risk data, including near misses and interrelation between risks.

3.137. CEIOPS would subject to the principle of proportionality expect undertakings to systematically collect operational risk data in an internal data base.

3.138. Effective operational risk identification should consider the undertaking's business environment and internal control factors, including:

- a) Internal factors, such as the undertaking's structure, the nature of its activities, products and processes, the quality of its human resources, organisational changes and employee turnover; and
- b) External factors, including changes in the industry, the legal environment and technological developments that could adversely affect the achievement of the undertaking's objectives and its operational risk profile.

3.139. In order to better manage the operational risks the undertaking is exposed to, notably through the analysis and projections of values, the identification of operational risk events should also comprise its categorisation<sup>10</sup>.

3.140. In addition to identifying its exposure to high severity events, the undertaking should assess its vulnerability to these risks through stress and scenario testing. Over time such assessments must be validated and re-assessed through comparison to actual loss experience to ensure their reasonableness.

3.141. The operational risk management framework needs to be closely integrated into the risk management processes of the undertaking. Its output must be an integral part of the process of monitoring and controlling the undertaking's

---

<sup>10</sup> One example of an operational risk categorisation that is widely used by (re)insurance undertakings is the one proposed by Operational Risk Insurance Consortium (ORIC, see footnote 15), which is based on the Capital Requirements Directive. However, every undertaking should be free to choose the operational risk categorisation that best suits its needs and risk exposures/profile.

operational risk profile.

- 3.142. The undertaking should have a well-documented assessment and management system for operational risk, with clear responsibilities assigned for the system.

### **CEIOPS' advice**

- 3.143. The undertaking should have a well-documented assessment and management system for operational risk, with clear responsibilities assigned.
- 3.144. The administrative or management body should be aware of the major aspects of the undertaking's operational risks as a distinct risk category that should be managed, and should approve, implement and periodically review the undertaking's operational risk management framework.
- 3.145. The undertaking shall implement an effective process to regularly identify, document and monitor exposure to operational risk and track relevant operational risk data, including near misses and interrelation between risks.
- 3.146. The operational risk management framework needs to be closely integrated into the risk management processes of the undertaking. Its output must be an integral part of the process of monitoring and controlling the undertaking's operational risk profile.

### **Reinsurance and other risk mitigation techniques**

#### **Explanatory text**

- 3.147. Reinsurance and alternative risk transfer (ART) techniques may enable the undertaking to prudently manage and mitigate in particular the insurance specific risk. However, they also carry new potential risks, such as the risk of counterparty default.
- 3.148. Reinsurance and ART management is an ongoing process that may be used to keep the undertaking's risks within the scope of the preset risk tolerance levels. Such arrangements can consist of traditional reinsurance, involving the transfer of insurance risk through conventional carriers and products, as well as non-traditional (or financial<sup>11</sup>) reinsurance, contingent loans and securitisations which are both addressed in CEIOPS' advice on reinsurance management<sup>12</sup>.
- 3.149. A reinsurance management strategy shall be defined and properly documented. Undertakings should identify who is responsible for monitoring the reinsurance

---

<sup>11</sup> Financial or finite reinsurance is a generic term that is used to describe an entire spectrum of reinsurance arrangements that transfer limited risk relative to aggregate premiums that could be charged under the contract. Although there is no accepted global definition, a typical transaction may include, but need not be limited to, provisions for aggregating risk, for aggregating limits of liabilities, for aligning the interests of undertakings, and for explicitly recognising the time value of money.

<sup>12</sup> See Answers to the European Commission on the second wave of Calls for Advice in the framework of the Solvency II project, CfA 12, [http://www.ceiops.eu/media/files/publications/submissionstotheec/Doc07\\_05-AnswersEC2ndwaveSII.pdf](http://www.ceiops.eu/media/files/publications/submissionstotheec/Doc07_05-AnswersEC2ndwaveSII.pdf)

arrangements, which control mechanisms are in place and what reporting lines are established.

- 3.150. As part of their reinsurance management strategy, undertakings should have adequate procedures and processes for placing appropriate reinsurance programs. The level of sophistication for these processes and procedures should be proportionate to the nature, scale and complexity of the undertaking's portfolio.
- 3.151. The undertaking's reinsurance management strategy should usefully have regard to the following considerations:
- a) Identification of the level of risk transfer appropriate to the undertaking's approach to risk;
  - b) What types of reinsurance arrangements are most appropriate to limit risks to the undertaking's insurance risk profile;
  - c) Principles for the selection of reinsurance counterparties;
  - d) Procedures for assessing the creditworthiness and diversification of reinsurance counterparties;
  - e) Concentration limits for credit risk exposure to reinsurance counterparties and appropriate systems for monitoring these exposures; and
  - f) Provision for adequate liquidity management to deal with any timing mismatch between claims' payments and reinsurance recoveries.
- 3.152. The reinsurance management strategy should include provisions to regularly review the procedures and processes established in order to ensure that they remain efficient and effective and take into account relevant changes in the risk profile of the undertaking.
- 3.153. Notwithstanding the requirement for an overall reinsurance management strategy, any use of alternative risk transfer (ART) should in addition:
- a) Identify the rationale for using ART;
  - b) Ensure that ART arrangements include genuine risk transfer;
  - c) Identify the risks to be covered by ART arrangements;
  - d) Ensure that ART arrangements fully reflect all the risks that are to be covered;
  - e) Identify the counterparties to be used and evaluate the credit risk associated with these operations; and
  - f) Identify the procedures for ongoing monitoring of the arrangements with a review to be undertaken at least on an annual basis.
- 3.154. With regard to special purpose vehicles these are only recognised as risk mitigation techniques, i.e. lead to a reduction of the undertaking's capital requirements or technical provisions, if the conditions to be fulfilled for the special purpose vehicle to be authorised according to Article 209 of the Level 1

text are being met. While a lack of authorisation does not prevent the undertaking from making use of a special purpose vehicle by way of de facto risk reduction if this is deemed appropriate, the risks arising from such an arrangement need to be taken into account in the ORSA.

- 3.155. Undertakings have to assess the effectiveness of all risk mitigation techniques employed, whether they use reinsurance, SPV, derivatives or any other techniques, in order to ensure that they meet their risk mitigation objectives. The undertaking has to document the assessment and to introduce changes to the risk mitigation as necessary to improve its effectiveness.
- 3.156. As SPVs differ from reinsurance undertakings the Level 1 text (Article 209) requires that additional Level 2 requirements should be provided for the authorisation and supervision of the SPVs. CEIOPS has therefore, in parallel to this Paper, developed Advice on Level 2 implementing measures on a regime for SPVs that protects policyholders of undertakings while at the same time not preventing innovation in the insurance industry.
- 3.157. When undertakings use SPVs the following principles should be considered taking into account the requirements and guidelines set out in CEIOPS Paper on Special Purpose Vehicles<sup>13</sup>:
- a) The fully funded requirement should be continuously monitored by the undertaking through its system of governance. The maximum reinsurance credit taken by an undertaking for an SPV should be capped at an amount equal to the lower value of the aggregate maximum liability transferred and the aggregate value of the assets of the SPV. Any fall in the value of the assets within the SPV should be mirrored by a corresponding fall in the reinsurance asset within the undertaking;
  - b) Any remaining risk (credit, market, liquidity, operational risk or 'burn-through' that may occur if the insured cost were to exceed the maximum amount payable by the SPV) from the SPV should be fully taken into account in the undertaking through its risk management system and also taken into account within the calculation of its regulatory capital requirements. The undertaking should be particularly aware of any residual insurance risk arising from the SPV if there were losses in excess of those envisaged at the time of authorisation. These losses above the funding provided would revert back to the undertaking.
  - c) There should be an alignment of interests between the undertaking and the SPV to ensure, for example:
    - i. that claims management processes in the undertaking operate effectively;
    - ii. that a discipline on the underwriting of risks within the undertaking is provided, i.e. the undertaking can not just transfer risks it may not have fully understood or properly managed to an SPV; and
    - iii. that the SPV is established and subsequently run in an appropriate manner for all the interested parties.

---

<sup>13</sup>See Consultation Paper No. xxx "Draft CEIOPS' Advice for Level 2 Implementing Measures on Solvency II: Special Purpose Vehicles (CEIOPS-CP-xx/09, 26 March 2009), <http://www.ceiops.eu/content/view/14/18/>.

This alignment could be achieved by the undertaking retaining an investment through a convertible loan note or a lower rated security in the SPV or the undertaking retaining some of the risks reinsured on its balance sheet. Where any assets or rights of an SPV are held or controlled by the undertaking those assets must be separately identified by the undertaking. This provides the undertaking with a vested interest in the operations of the SPV which may also make it a more attractive investment, as investors have confidence the undertaking retains an interest in the risk being reinsured to the SPV.

Full disclosure must be provided by the undertaking to all relevant parties on how the interests are aligned, and any relationship between the parties. In these circumstances, regulatory capital relief should be reduced from this alignment. Such actions may have the economic effect of reducing the level of reinsurance cover or increasing the risks covered by the solvency capital requirement, and the supervisory authority should be confident this has been properly taken into account.

### **CEIOPS' advice**

3.158. As part of their reinsurance management strategy, undertakings should have adequate procedures and processes for the selection of suitable reinsurance programs. The level of sophistication for these processes and procedures should be proportionate to the nature, scale and complexity of the undertaking's operations.

3.159. The undertaking's reinsurance strategy should usefully have regard to the following considerations:

- a) Identification of the level of risk transfer appropriate to the undertaking's approach to risk;
- b) What types of reinsurance arrangements are most appropriate to limit risks to the undertaking's insurance risk profile;
- c) Principles for the selection of reinsurance counterparties;
- d) Procedures for assessing the creditworthiness and diversification of reinsurance counterparties;
- e) Concentration limits for credit risk exposure to reinsurance counterparties and appropriate systems for monitoring these exposures; and
- f) Provision for adequate liquidity management to deal with any timing mismatch between claims' payments and reinsurance recoveries.

3.160. The requirement for an overall reinsurance management strategy, any use of alternative risk transfer (ART) should in addition:

- a) Identify the rationale for using ART;
- b) Ensure that ART arrangements include genuine risk transfer;

- c) Identify the risks to be covered by ART arrangements;
- d) Ensure that ART arrangements fully reflect all the risks that are to be covered;
- e) Identify the counterparties to be used and evaluate the credit risk associated with these operations; and
- f) Identify the procedures for ongoing monitoring of the arrangements with a review to be undertaken at least on an annual basis.

3.161. When undertakings use SPV's the following principles should be considered taking into account the requirements and guidelines set out in CEIOPS Consultation Paper on Special Purpose Vehicles:

- a) The fully funded requirement should be continuously monitored by the undertaking through its system of governance;
- b) Any remaining risk from the SPV should be fully taken into account in the undertaking through the its risk management system and also taken into account within the calculation of its regulatory capital requirements;
- c) There should be an alignment of interests between the undertaking and the SPV.

### ***Some other risks to be considered***

#### **Credit risk management**

##### **Explanatory text**

3.162. Credit risk refers to the risk of loss or of adverse change in the financial position resulting, directly or indirectly, from fluctuations in the credit standing of issuers of securities, counterparties and any debtors to which undertakings are exposed, in the form of counterparty default risk, or spread risk, or market risk concentrations. This risk is not explicitly mentioned in Article 43(2) of the Level 1 text, but included in the calculation of the SCR.

3.163. Credit risk is a function of exposure at default and probability of default. A credit risk management strategy should, at a minimum, focus on these elements both in isolation and on the correlations between them.

3.164. The undertaking should ensure that the credit risk exposure is sufficiently diversified. It should have a process of credit risk management to ensure that exposure to any counterparty is limited so that no single exposure would threaten the undertaking's solvency position.

3.165. The process of risk management should be capable of identifying and mitigating any credit risk in relation to internally defined limits.

3.166. The undertaking should be alert to changes in credit ratings through regular

appropriate and proportionate monitoring processes, and capable of evaluating probabilities of default even where exposures are unrated. Exposure to speculative grade assets should be prudent and undertakings facing larger credit risk exposures should be capable of hedging credit risk via derivatives to protect against a protracted fall in credit quality or turn in the credit cycle.

- 3.167. Undertakings should be aware that intra group exposures give rise to credit risk as any other external exposure does. The undertaking should be able to demonstrate that it is not overly reliant on any counterparty, regardless of whether it lies within the same group.
- 3.168. The following other risks not explicitly mentioned in Article 43 of the Level 1 text should be considered in particular due to the potential impact their crystallisation could have on the business of the undertaking:
- a) Strategic risk; and
  - b) Reputational risk.

### **CEIOPS' advice**

- 3.169. The process of risk management should be capable of identifying and mitigating any credit risk in relation to internally defined limits.
- 3.170. The undertaking should be alert to changes in credit ratings through regular appropriate and proportionate monitoring processes, and capable of evaluating probabilities of default even where exposures are unrated. Exposure to speculative grade assets should be prudent and undertakings facing larger credit risk exposures should be capable of hedging credit risk via derivatives to protect against a protracted fall in credit quality or turn in the credit cycle.

### **Strategic risk**

#### **Explanatory text**

- 3.171. Strategic risk is defined as the risk of the current and prospective impact on earnings or capital arising from adverse business decisions, improper implementation of decisions, or lack of responsiveness to industry changes.
- 3.172. Strategic risk is a function of the incompatibility between two or more of the following components: the undertaking's strategic goals, the business strategies developed and the resources deployed to achieve these goals, and the quality of implementation and the economic situation of the markets the undertaking operates in.
- 3.173. The resources needed to carry out business strategies are both tangible and intangible. They include communication channels, operating systems, delivery networks, and managerial capacities and capabilities. The undertaking's internal characteristics should be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental changes.

3.174. The overall strategy of the undertaking should incorporate its risk management practices. In this sense, the undertaking should have a process for setting strategic high-level objectives and translating these into detailed shorter-term business and operation plans.

### **Reputational risk**

#### **Explanatory text**

- 3.175. Reputational risk is defined as the risk of potential loss to an undertaking through deterioration of its reputation or standing due to a negative perception of the undertaking's image among customers, counterparties, shareholders and/or supervisory authorities. To that extent it may be regarded as less of a separate risk, than one consequent on the overall conduct of an undertaking.
- 3.176. The administrative or management body of the undertaking should be aware of potential reputational risks it is exposed to and the correlation with all other material risks.
- 3.177. The undertaking should pay great attention to understanding and recognising key values affecting the reputation, considering expectations of the stakeholders and sensitivity of the marketplace.

### ***Risk management function***

#### **Explanatory text**

3.178. Article 43(4) and (5) of the Level 1 text states:

*4. Insurance and reinsurance undertakings shall provide for a risk management function which shall be structured in such a way as to facilitate the implementation of the risk management system.*

*5. For insurance and reinsurance undertakings using a partial or full internal model approved in accordance with Articles 110 and 111 the risk management function shall cover the following additional tasks:*

*(a) to design and implement the internal model;*

*(b) to test and validate the internal model;*

*(c) to document the internal model and any subsequent changes made to it;*

*(d) to inform the administrative or management body about the performance of the internal model, suggesting areas needing improvement, and up-dating that body on the status of efforts to improve previously identified weaknesses;*

*(e) to analyse the performance of the internal model and to produce summary reports thereof.*

- 3.179. The undertaking needs to establish a risk management function within its organisational structure that is proportionate to the scale, nature and complexity of risks inherent within the business. The embedding of the risk management function in the organisational structure of the undertaking and the associated reporting lines shall ensure that the function is objective and independent of the operational business.
- 3.180. The risk management function is responsible for the coordination across the undertaking of risk management activities.
- 3.181. The tasks of the risk management function include:
- a) Assisting the administrative or management body and other management in the effective operation of the risk management system, in particular by performing specialist analyses and performing quality reviews;
  - b) Monitoring the risk management system;
  - c) Maintaining an organisation-wide and aggregated view on the risk profile of the undertaking;
  - d) Reporting details on risk exposures and advising the administrative or management body with regard to risk management matters in relation to strategic affairs such as corporate strategy, mergers and acquisitions and major projects and investments; and
  - e) Identifying and assessing emerging risks.
- 3.182. The design and operational effectiveness of the risk management system to identify, measure, and monitor risks the undertaking is exposed to shall be regularly evaluated by the risk management function.
- 3.183. Article 43(5) requires the risk management function to take on board a set of additional tasks that relate to the use of partial or full internal models. By contrast the Level 1 text does not explicitly assign any task with regard to internal models to the actuarial function although the actuarial function may contribute to the effective implementation of the risk management system which includes the internal model. CEIOPS understands the Level 1 text to assign "ownership" of an internal model to the risk management function as opposed to e.g. operational business areas, staff working in a capital management or in a strictly actuarial capacity. The concept aims to ensure that the model is designed and maintained as an effective risk management tool and is more than a calculation kernel. Since the Level 1 text does not distinguish between different parts of the internal model CEIOPS interprets this to mean that the risk management function is responsible for the design, maintenance and monitoring, but this does not preclude the risk management function from calling upon expertise from other functions notably the actuarial.
- 3.184. Article 110(5) of the Level 1 text states that the supervisory authority shall give approval for use of an internal model in calculating the SCR only if they are satisfied that the systems of the undertaking for identifying, measuring, monitoring, managing and reporting risk are adequate. Undertakings who are seeking to apply for internal model approval need therefore to ensure that their risk management system is effective to ensure the model can be approved.

- 3.185. If the undertaking uses an internal model this is part of a comprehensive risk management system which should have adequate resources and structures to ensure that the internal model is and stays appropriate to the undertaking's risk profile.
- 3.186. In this context, the risk management function shall be responsible for the way in which the internal model is designed and integrated with the undertaking's internal risk management system and the day-to-day functions of the undertaking. It shall assess the internal model as a tool of risk management and as a tool to calculate the undertaking's SCR.
- 3.187. Article 114 states that the administrative or management body shall have responsibility for putting in place systems which ensure that the internal model operates properly on a continuous basis. As part of this process the risk management function should regularly test and validate the internal model with a view to identify weaknesses, to improve the model and to ensure that the model remains appropriate to the risk profile of the undertaking.
- 3.188. Documentation of the internal model, and any subsequent changes to it, should be owned by the risk management function so that these are explained in the context of the risk management system.
- 3.189. The information about the performance of the internal model that the risk management function is required to give to the administrative or management body according to Article 43(5)(d) should be properly documented. These reports should be tailored to the needs of the administrative or management body, enabling its members to understand all relevant facts and the implications following from them as a solid and reliable basis for necessary management decisions as well as in their role for being responsible for the on-going appropriateness of the design and operations of the internal model, and that the internal model continues to reflect the risk profile of the undertaking<sup>14</sup>.

### **CEIOPS' advice**

- 3.190. The undertaking shall embed the risk management function in the organisational structure and organise the associated reporting lines in a manner which ensures that the function is objective and not responsible for the results of operational business.
- 3.191. The tasks of the risk management function shall include:
- a) Assisting the administrative or management body and other management in the effective operation of the risk management system, in particular by performing specialist analyses and performing quality reviews;
  - b) Monitoring the risk management system;
  - c) Maintaining an organisation-wide and aggregated view on the risk profile of the undertaking; and

---

<sup>14</sup> CEIOPS' Consultation Papers expected in June 2009 will provide further details on Articles 114 and 118.

d) Reporting details on risk exposures and advising the administrative or management body with regard to risk management matters in relation to strategic affairs like corporate strategy, mergers and acquisitions and major projects and investments.

3.192. The risk management function shall be responsible for the way in which an internal model is integrated with the undertaking's internal risk management system and the day-to-day functions of the undertaking. It shall assess the internal model as a tool of risk management and as a tool to calculate the undertaking's SCR.

### **3.4. Internal Control**

#### **Explanatory text**

3.193. Article 45 of the Level 1 text states:

*1. Insurance and reinsurance undertakings shall have in place an effective internal control system.*

*That system shall at least include administrative and accounting procedures, an internal control framework, appropriate reporting arrangements at all levels of the undertaking and a compliance function.*

*2. The compliance function shall include advising the administrative or management body on compliance with the laws, regulations and administrative provisions adopted pursuant to this Directive. It shall also include an assessment of the possible impact of any significant changes in the legal environment on the operations of the undertaking concerned and the identification and assessment of compliance risk.*

3.194. A system of effective internal control is a critical component of undertaking management and a foundation for the safe and sound operation of undertakings. Internal control is not a procedure or policy performed at a certain point in time, but rather a set of continually operating processes involving the administrative or management body and all level of personnel.

3.195. There are different frameworks in force for the internal control system. The Level 1 text does not prescribe any specific approach and CEIOPS has no expectation that undertakings prefer any specific framework.

3.196. In CEIOPS' view, an effective internal control system, as envisaged in the Level 1 text, shall comprise a coherent, comprehensive and continuous set of mechanisms designed to secure at least the following:

- a) Effectiveness and efficiency of the undertaking's operations in view of its risks and objectives;
- b) Availability and reliability of financial and non-financial information; and
- c) Compliance with applicable laws, regulations and administrative provisions.

- 3.197. Internal control is defined as a process affected by an organisation's structure, work and authority flows, people and management information systems, designed to help the organisation accomplish specific goals or objectives<sup>15</sup>.
- 3.198. The internal control system should be suitable to the individual characteristics of each undertaking, such as the degree of centralisation, delegation of authority and the capacity and effectiveness of the information technologies, in particular taking into account the scale, nature and complexity of the business. The activities of the undertaking should determine how strong different features of the internal control framework need to be.
- 3.199. The internal control system should ensure that an undertaking's systems, whether manual or based on information technology, are appropriate to the undertaking's strategies and data needs and consistent with the nature and complexity of its activities.
- 3.200. Appropriate administrative procedures shall be defined and implemented for the main activities within the undertaking in order to ensure well-ordered and efficient operations, to reduce mistakes in the handling of business and to support compliance with applicable rules and regulations. Examples of such administrative procedures include procedures for the implementation and maintenance of accounting policies and procedures which ensure that accounts give a true and fair view of an undertaking's assets and liabilities as well as its financial position, internal programmes, procedures and controls to combat money laundering and terrorist financing, and systems to deal with policyholders' claims and complaints.
- 3.201. An effective internal control system should comprise robust and efficient control activities at all levels of the undertaking. These should be implemented by the management in line with the strategies, business plans and goals set for the undertaking. As an integrated part of daily business, the control activities should be reviewed and documented on an on-going basis.

#### *Control environment*

- 3.202. The internal control system of the undertaking should be built upon a strong control culture which emphasises and demonstrates to all levels of personnel the importance of internal control.
- 3.203. A high level of integrity is an essential part of the control culture. In reinforcing integrity, undertakings should avoid policies and practices that may provide incentives for inappropriate activities.
- 3.204. As stated in Article 41(3) of the Level 1 text, the undertaking needs to implement a written policy on internal control that is approved by the administrative or management body. This should include the means by which senior management implement the internal control system to provide for and maintain the suitability and effectiveness of the internal control system.

---

<sup>15</sup> <http://www.coso.org/IC-IntegratedFramework-summary.htm>

- 3.205. The provision that calls for the regular internal review of the system of governance is necessarily applicable to that system.
- 3.206. The undertaking's systems should also take account of applicable data protection requirements, provide for appropriate security controls and should at least cover access to hardware, systems and data, so as to maintain the integrity of records and information and thereby protect the interests of policyholders. Managerial, operational and technical controls could also be included, as necessary.

#### *Control activities*

- 3.207. The daily control activities could, depending on the particular circumstances of the undertaking, include approvals, authorisations, verifications, reconciliations, management reviews, appropriate measurements applicable to each business area and unit, physical controls, checking for compliance with agreed exposure limits and operating principles/instructions and follow-up on non-compliance. The control activities should be proportionate to the risks coming from the controlled activities and processes.
- 3.208. Controls should also ensure that any areas of potential conflicts of interest are identified and managed appropriately.

#### *Communication*

- 3.209. Clear reporting and communication lines shall be set up. The reporting of the achievement of the main goals and material risks inherent in the business should be predefined. This applies particularly to the reporting to the administrative or management body.
- 3.210. Communication lines inside the undertaking should also encourage adverse reporting, particularly when flowing upwards, so as to avoid employees suppressing negative information and permit the jumping of reporting lines should the situation call for such action. Quality reports, timely reporting, accuracy, completeness and suggestions for improvements should be encouraged.

#### *Monitoring*

- 3.211. The monitoring mechanisms shall facilitate the understanding of the undertaking's situation and provide the administrative or management body with relevant information for the decision-making process. They should include procedures to detect deficiencies.
- 3.212. Ongoing monitoring should occur in the course of normal operations and should include regular management activities and actions taken by all personnel when performing their duties.
- 3.213. The effectiveness of the internal control system itself should be monitored on a

continuous basis, so that any deficiencies of the system can be identified and rectified in a timely manner.

### *Compliance function*

- 3.214. The compliance function within the undertaking is the administrative capacity for ensuring that all the actions of the undertaking comply with applicable laws and regulatory requirements.
- 3.215. Article 45(1) requires undertakings to have in place a compliance function as part of the internal control system. It should identify, assess, monitor and report the compliance risk exposure of the undertaking.
- 3.216. Compliance risk is defined as the risk of legal or regulatory sanctions, material financial loss or loss to reputation an undertaking may suffer as a result of not complying with laws, regulations and administrative provisions as applicable to its activities.
- 3.217. In order to assess the possible impact of significant changes in the legal environment that the undertaking operates in as well as identify and assess the compliance risk that could arise from such changes, the compliance function should monitor projected revisions of statutes and plans to introduce new regulation and assess their potential impact on the undertaking and monitor the relevant court decisions.
- 3.218. According to Article 45(2) the tasks of the compliance function requires as a minimum advising the administrative or management body on compliance with the applicable laws, regulations and administrative provisions adopted pursuant to the Level 1 text. The compliance function could also ensure that the undertaking complies with other applicable laws and regulations whether insurance specific or not.
- 3.219. In order to be able to perform its responsibilities effectively and with the appropriate authority the compliance function shall be given appropriate standing in the undertaking. To this purpose its responsibilities, its competences and reporting duties should be set out in the internal control policy or another formal document.
- 3.220. The compliance function should assess the appropriateness of the undertaking's compliance procedures and guidelines, follow up identified deficiencies promptly and make suggestions for improvements as necessary.
- 3.221. The compliance function shall be able to communicate on its own initiative with any staff member and to obtain access to any records necessary to allow it to carry out its responsibilities.
- 3.222. The intended compliance activities shall be set out in a compliance plan that ensures that all relevant areas of the undertaking are appropriately covered, taking into account their susceptibility to compliance risk.
- 3.223. The compliance function shall promptly report any major compliance problems it identifies to the administrative or management body.

## CEIOPS' advice

- 3.224. The internal control system shall secure the undertaking's compliance with applicable laws, regulations and administrative provisions and the effectiveness and efficiency of operations in view of its objectives as well as the availability and reliability of financial and non-financial information.
- 3.225. The undertaking shall be required to have in place a suitable control environment, appropriate control activities, effective information and communication procedures and adequate monitoring mechanisms.
- 3.226. The compliance function shall have appropriate standing within the undertaking. It shall be able to communicate on its own initiative with any staff member and to obtain access to any records necessary to allow it to carry out its responsibilities.
- 3.227. The intended compliance activities shall be set out in a compliance plan that ensures that all relevant areas of the undertaking are appropriately covered, taking into account their susceptibility to compliance risk.
- 3.228. The compliance function shall promptly report any major compliance problems it identifies to the administrative or management body.

## 3.5. Internal Audit

### **Explanatory text**

3.229. Article 46 of the Level 1 text states:

*1. Insurance and reinsurance undertakings shall provide for an effective internal audit function.*

*2. The internal audit function shall include an evaluation of the adequacy and effectiveness of the internal control system and other elements of the system of governance.*

*3. The internal audit function shall be objective and independent from the operational functions.*

*4. Any findings and recommendations of the internal audit shall be reported to the administrative or management body which shall determine what actions shall be taken with respect to each of the internal audit findings and recommendations and shall ensure that these actions are carried out.*

3.230. The internal audit function is an independent function within the organisation which examines and evaluates the functioning of the internal controls and all other elements of the system of governance as well as the compliance of activities with internal strategies, policies, processes and reporting procedures.

3.231. The internal audit function needs to be independent from the organisational

activities audited. In order to ensure this, the internal audit shall be given an appropriate standing within the organisation and shall carry out its assignments with impartiality. The principle of independence entails that the internal audit function operates under the direct control of the administrative or management body, reporting to this body or an audit committee.

- 3.232. To ensure the effectiveness of the internal audit function it is further necessary to endow the function with sufficient resources. With regard to the remuneration of the internal audit function the undertaking needs to ensure that the function is compensated according to its own objectives, not in relation to the performance of the business units it reviews.
- 3.233. The internal audit function shall be able to exercise its assignment without impairment in all areas of the undertaking and to this purpose have direct communication with all members of staff. It shall be free to express its opinion and to disclose its findings and appraisals to the whole administrative or management body.
- 3.234. The position/status of the internal audit function within the undertaking should be set up in a formal document by the administrative or management body or with its approval, e.g. in an internal audit charter or in an internal audit strategy document. This should at least cover the following aspects:
- a) Objective and scope of the internal audit function;
  - b) Status within the undertaking; and
  - c) Competences/tasks and responsibilities.
- 3.235. The internal audit function needs to be provided with a complete and unrestricted right to obtain information, which includes the prompt provision of all necessary information, the availability of all essential documentation and the ability to see into all activities and processes of the undertaking, relevant for the discharge of its responsibilities. It needs to be granted access to any records, files or data of the undertaking, including management information and the minutes of decision-making bodies whenever relevant for the performance of its tasks.
- 3.236. All business units should have an obligation to inform the internal audit function when control deficiencies are recognised, losses are sustained or there is a definite suspicion concerning irregularities. The internal audit function should define the appropriate parameters/triggers for this obligation.
- 3.237. When the complexity and extent of the risks do not justify entrusting the internal audit function to a full-time staff member, this function may be commissioned to a qualified third party.
- 3.238. The internal audit function should prepare an audit plan setting out the audit work to be undertaken in the upcoming business year(s). The audit plan should be based on a methodical risk analysis, taking into account all activities and the complete system of governance as well as expected developments of activities and innovations. On the basis of the result of this risk analysis, a plan, extending for several years depending on the scale and complexity of the activities, should be established.

- 3.239. In the planning of audit activities the internal audit function needs to ensure that all significant activities are reviewed within a reasonable period of time (audit cycle principle) and proper consideration should be given to how often important areas of the undertaking need to be scrutinised.
- 3.240. The audit plan should be realistic and detail the necessary resources and budget. It should be submitted for approval to the administrative or management body.
- 3.241. The audit activities should be complemented by an adequate follow-up procedure in order to keep track of remedial actions taken by management in areas where shortcomings were observed by the internal audit function.
- 3.242. Good practice suggests that the internal audit function should issue written reports and transmit these promptly to the managers of the audited units regardless of whether material shortcoming have been found. Reports should in any case be produced if deficiencies are identified in an audited area and also be transmitted to the administrative or management body in the case of major deficiencies. This notwithstanding, the internal audit function shall at least annually produce a written report on its finding to be submitted to the administrative or management body. The report shall cover at least any deficiencies with regard to the efficiency and suitability of the internal control system as well as major shortcomings with regard to the compliance with internal policies, procedures and processes. It shall include recommendations on how to remedy inadequacies and also specifically address, how past points of criticism and past recommendations have been followed up.
- 3.243. The internal audit function should also report to the administrative or management body on the achievement of the internal audit function's objectives, in particular, on the execution of the audit plan. As part of its supervisory task, the administrative or management body should regularly discuss the organisation, audit plan, audit programme, resources, activity reports and summary of recommendations and their implementation.
- 3.244. In order to permit a review of the effectiveness of the work of the internal audit function, audits should be documented in a way that makes it possible to retrace the audit procedures undertaken and the findings these produced.

### **CEIOPS' advice**

- 3.245. To ensure its independence from the organisational activities audited, the internal audit function shall have an appropriate standing within the organisation and carry out its assignments with impartiality. The internal audit function shall be able to exercise its assignments on its own initiative in all areas of the undertaking. It shall be free to express its findings and to disclose them and its appraisals to the whole administrative or management body.
- 3.246. The internal audit function shall have the complete and unrestricted right to obtain information, which includes the prompt provision of all necessary information, the availability of all essential documentation and the ability to look into all activities and processes of the undertaking, relevant for the discharge of its responsibilities, as required in the performance of its tasks, as well as having direct communication with any member of the undertaking's staff.

- 3.247. To ensure the effectiveness of the internal audit function, every activity and every unit of the undertaking shall fall within its scope. The function shall draw up an audit plan to determine its future auditing actions, taking a risk based approach in deciding its priorities.
- 3.248. The internal audit function shall at least annually produce a written report on its findings to be submitted to the administrative or management body. The report shall cover at least any deficiencies with regard to the efficiency and suitability of the internal control system as well as major shortcomings with regard to the compliance with internal policies, procedures and processes. It shall include recommendations on how to remedy inadequacies and also specifically address how past points of criticism and past recommendations have been implemented.

### **3.6. Actuarial Function**

#### **Explanatory text**

3.249. Article 47(1) of the Level 1 text states:

*Insurance and reinsurance undertakings shall provide for an effective actuarial function to undertake the following:*

- a) To coordinate the calculation of technical provisions;*
- b) To ensure the appropriateness of the methodologies and underlying models used as well as the assumptions made in the calculation of technical provisions;*
- c) To assess the sufficiency and quality of the data used in the calculation of technical provisions;*
- d) To compare best estimates against experience;*
- e) To inform the administrative or management body of the reliability and adequacy of the calculation of technical provisions;*
- f) To oversee the calculation of technical provisions in the cases set out in Article 81;*
- g) To express an opinion on the overall underwriting policy;*
- h) To express an opinion on the adequacy of reinsurance arrangements;*
- i) To contribute to the effective implementation of the risk management system referred to in Article 43, in particular with respect to the risk modelling underlying the calculation of the capital requirements set out in Chapter VI, Sections 4 and 5 and the assessment referred to in Article 44.*

3.250. The actuarial function as envisaged by the Level 1 text is not shaped on the position of the Responsible Actuary which has been introduced in a number of Member States. Nevertheless CEIOPS understands the establishment of an actuarial function to have been prescribed as a measure of quality assurance with a view to safeguarding that certain important undertakings' decisions can

be taken based on expert technical actuarial advice.

- 3.251. As the actuarial function does not exist in other Directives, CEIOPS' proposals for this topic are subject to an impact assessment. For that reason, this section is laid out differently, explaining the main options for each of the issues that were formally considered. It also sets out why CEIOPS has selected its preferred option for each issue. Annex B of this Paper also sets out in greater detail the issues and options considered, and how they satisfy the objectives for the Solvency II framework set by the Commission.
- 3.252. CEIOPS would welcome specific feedback from stakeholders on the options considered and the rationale set out in the Annex B, in particular where undertakings consider the impact of the options to be different from that set out.
- 3.253. With regard to the standards to be applied by the actuarial function in exercising its tasks, CEIOPS has considered the following options:

**Option 1:** The function should use technical standards developed by CEIOPS on Level 3.

**Option 2:** The function should rely on technical standards that are widely accepted in the industry and the profession.

**Option 3:** The function should rely on European technical standards to be developed and endorsed by a body of representatives of different stakeholders, including CEIOPS.

- 3.254. The actuarial profession is organised in national and international associations that issue guidelines on technical issues, effective on their own members.
- 3.255. CEIOPS understands that those associations have legitimacy and expertise to develop such standards. As the methodologies and practices from actuarial professional bodies are widely accepted in the industry, there is no reason not to consider them appropriate for supervisory purposes. However, CEIOPS also envisages a high level of convergence in the guidelines to be used, which is not compatible with the use of guidelines issued by national actuary associations.
- 3.256. CEIOPS believes that a European endorsement is necessary for two main reasons:
- a) CEIOPS should be able to express its views and concerns in relation to the guidelines;
  - b) Guidelines from an international association would only be mandatory to actuaries belonging to that association. However, being part of an association would not necessarily be a requirement for performing tasks/duties related to the actuarial function.
- 3.257. CEIOPS favours option 3 as it is of the opinion that a European body, which may be an existing body or a newly established body, should develop the guidelines to serve as a basis for the performance of the tasks/duties in the context of the actuarial function, since these should be developed at an European level in accordance with the Solvency II regime. This does not prevent national associations from continuing their existing role in their jurisdiction but consistency would need to be maintained.

- 3.258. The alternative is for CEIOPS to develop its own guidance on Level 3 which would not necessarily lead to more harmonisation in the use of methodologies than the endorsement of the guidance by a body where it is included. At this point in time CEIOPS does not see sufficient grounds for proposing to issue new standards itself. However, CEIOPS envisages that the endorsement process could be implemented via Level 3 guidance.
- 3.259. The actuarial function shall, in the exercise of its tasks, apply the European technical standards endorsed by the body referred above that allow an appropriate level of confidence regarding its findings.
- 3.260. CEIOPS considers the list of tasks for the actuarial function to be comprehensive as far as mandatory tasks are concerned. This does not, however, preclude the allocation of further duties to the actuarial function as the administrative or management body sees fit, provided this does not compromise the proper segregation of duties within the undertaking.
- 3.261. The actuarial function shall have access to the appropriate information systems that provide all necessary information, relevant for the discharge of its responsibilities.
- 3.262. Article 47(1) prescribes the mandatory tasks of the actuarial function. This list can be interpreted in different ways. CEIOPS has considered whether:

**Option 1:** It should be left to undertakings to decide on the scope of these tasks individually.

**Option 2:** The general scope of the tasks should be prescribed on Level 2 to some extent.

- 3.263. While leaving the decision to the undertakings would provide more flexibility for them in organising responsibilities and tailoring actuarial input to what they consider their individual needs, CEIOPS is concerned that not prescribing to some extent what is required in fulfilling the tasks listed in Article 47(1) could erode the intention of the Level 1 text to provide a certain level of expert technical advice through the actuarial function.
- 3.264. Furthermore CEIOPS believes that defining, although generally, the scope of the actuarial function's tasks could lead to a higher level of consistency and an increase in the quality of assurance of the outputs of this function across the EU.
- 3.265. In order to ensure a minimum level of actuarial input of sufficient quality for the administrative or management body to rely and base its decisions on, CEIOPS therefore favours the Option 2 approach where there are minimum tasks provided to the actuarial function but the undertaking is free to organise its internal operations as it sees fit so the actuarial function may be involved in other activities. Set out below is an explanation of the additional scope of the tasks that is a consequence of this option.
- 3.266. Article 47(1)(a) requires the actuarial function to coordinate the calculation of the technical provisions. In order to accomplish this task it should:
- a) Ensure that methodologies and procedures are applied to assess the sufficiency of technical provisions and to ensure that their calculation is consistent with the underlying principles;

- b) Assess the uncertainty associated with the estimates;
- c) Produce judgement whenever this is needed, making use of any relevant information and experience of the persons that are in charge of the function;
- d) Ensure that problems related to the calculation of technical provisions arising from insufficient data quality are solved and that the most appropriate alternatives to common methods applied are found, taking into consideration the principle of proportionality;
- e) Ensure that homogeneous risk groups for an appropriate assessment of the underlying risks are identified;
- f) Consult any relevant market information and ensure that it is integrated into the assessment of technical provisions;
- g) Compare and justify any material differences among the estimates for different years;
- h) Ensure that an appropriate assessment of options and guarantees embedded in liabilities is provided.

3.267. In relation to Article 47(1)(b), in order to ensure the appropriateness of the underlying methodologies and models, the actuarial function not only has to assess the general suitability of the methodology or underlying model for the calculation of technical provisions as such, but also has to decide whether they are appropriate for the specific lines of business of the undertaking, for the way the business is managed and for the available data.

3.268. While assessing the sufficiency and quality of the data under Article 47(1)(c), the actuarial function should have regard to the objectivity, reasonability and verifiability of management actions included in the calculation of technical provisions. It should also assess whether information technology systems used in actuarial procedures sufficiently support these procedures. However, the implementation of data auditing techniques is a task that should not be performed by the actuarial function but by the internal audit function.

3.269. The comparison of the best estimates against experience under Article 47(1)(d) requires the actuarial function to assess whether past best estimates have proved sufficient and to use the insights gained in this assessment to improve the quality of present best estimate calculations.

3.270. This analysis should also include comparisons between observed and expected values of the costs associated with technical provisions in order to produce conclusions on the appropriateness of the data used and the methodologies applied on their estimation. The results of these comparisons should be reported to the administrative or management body, given its relevance for the comprehension of the calculations performed and to support future decisions regarding this issue. It should be noted that the referred comparisons may be a practise of not only the actuarial function but the risk management function as well, and its area of application may be extended.

3.271. When it comes to Article 47(1)(e), informing the administrative or management body of the reliability and adequacy of the calculation of the technical provisions

is not limited to expressing an opinion on these points, including on the degree of uncertainty about the ultimate outcome and the circumstances that might lead to a significant deviation from the provisions made. The actuarial function must set out how it arrived at its opinion and clearly state and explain any concerns it may have as to the technical provisions being sufficient. As the reliability of the calculation of the technical provisions depends on adequate and good quality data, the assessment of the sufficiency and quality of the data used in the calculation is information that needs to be included when the administrative or management body is informed of the reliability and adequacy of the calculation.

- 3.272. The actuarial function should also assess the level of appropriateness, accuracy and completeness of the available data and convey recommendations on improving data quality, where appropriate. It may consider there is a need to introduce adjustments to the historical data, not because the data per se is considered inappropriate, but because it could be necessary to increase the level of its appropriateness for the purpose of the application of specific methodologies.
- 3.273. In this context the actuarial function should provide judgement as to how much credibility should be assigned to historical data and to prospective assumptions. This judgement has to be based notably on a careful analysis of the underlying liabilities, relevant market data, the undertaking's experience, especially with the portfolio concerned, and relevant qualitative information.
- 3.274. Reporting on the reliability of the technical provisions also includes informing the administrative or management body on the results of comparisons of the best estimates against experience and comments on the appropriateness of methodologies, underlying models and assumptions used.
- 3.275. Since the administrative or management body is ultimately responsible for the reliable and adequate calculation of the technical provisions the report must cover all information the administrative or management body needs to form its own opinion on the issue.
- 3.276. In the scope of the coordination of the calculation of technical provisions the actuarial function should as under Article 47(1)(f) oversee when a case-by-case approach should be followed, that is, when there is not sufficient quality of data to apply a reliable actuarial method. Also, it has to produce judgement to establish assumptions and to safeguard the accuracy of the results.
- 3.277. In relation to Article 47(1)(g) and (h), the actuarial function shall annually express an opinion on the overall underwriting policy and the adequacy of the significant reinsurance arrangements as well as expected cover under stress scenarios and report these views to the administrative or management body and senior management. In the provision of these opinions the actuarial function shall not only address possible deficiencies and the possible consequences these may have but also make constructive suggestions for improvements.
- 3.278. In CEIOPS' view the requirement on the actuarial function to express an opinion on the overall underwriting policy and the adequacy of the reinsurance arrangements does not imply that the actuarial function may not be involved in the original decisions on these issues. However, "justification" of decisions taken by the actuarial function or with its involvement requires more detailed explanations and a decided examination of other possible decision options.

- 3.279. Commenting on the “overall underwriting policy” does not require expressing views on every single policy but on the undertaking’s underwriting in general. The scope of the view expressed is determined by what is relevant information for the administrative or management body in reviewing the undertaking’s underwriting policies.
- 3.280. Regarding the overall underwriting policy, the opinion to be expressed by the actuarial function should at least include the following issues:
- a) Analysis of the sufficiency of the premiums<sup>16</sup> to cover future losses, notably taking into consideration the underlying risks, the impact of expenses directly associated with future claims and of unallocated loss adjustment expenses and the impact of embedded options and guarantees on future liabilities;
  - b) Considerations regarding inflation, legal risk, change of mix, anti-selection and adequacy of *bonus-malus* system(s) implemented in specific line(s) of business.
- 3.281. Regarding the overall reinsurance cover, the opinion to be expressed by the actuarial function should include an opinion on the adequacy of the reinsurance and other mitigation techniques strategy in relation to the underwriting policy and the adequacy of the calculation of the technical provisions arising from reinsurance.
- 3.282. In order to be able to provide its opinions in an independent fashion, the actuarial function should be constituted by persons who verify a sufficient level of independency between them in order to appropriately form their own actuarial view in the exercise of the functions tasks.
- 3.283. In considering the reporting of the actuarial function CEIOPS has looked into two possible options:

**Option 1:** Require annual reporting with definition on Level 2 of its structure and content

**Option 2:** Require annual reporting but leave the decision on the details up to the undertakings as stated in paragraph 3.10.

- 3.284. In forming and formulating its own actuarial view the actuarial function shall be objective and free from influence of other functions or the administrative or management body.
- 3.285. The actuarial function shall at least annually produce written reports on the mandatory tasks performed that document the steps that have been undertaken, clearly state any shortcomings identified and give recommendations as to how the deficiencies could be remedied.
- 3.286. The reports should be submitted to the administrative or management body of the undertaking, which should document the decisions to be taken in view of the

---

<sup>16</sup> CEIOPS believes that the actuarial function should be aware if the firm is underwriting at a loss for example and the consequences for doing so.

findings and recommendations of the actuarial function.

- 3.287. CEIOPS considers the option of defining the structure and content of the report in Level 2 to be excessive. In effect the actuarial function should reflect the specificities of the undertaking and take into account the principle of proportionality. Furthermore CEIOPS does not intend to define the structure and content of any report of the system of governance and does not envisage a reason for doing it in the case of the actuarial function. Consequently, CEIOPS favours option 2.
- 3.288. Detailed monitoring should be undertaken regarding the measures implemented by the undertaking in the pursuit of the actuarial recommendations.
- 3.289. Article 43(5) sets out that the risk management function is responsible for a number of areas of the internal model. This aims to ensure that the model is seen as a widely-understood risk management tool within the business and not purely an 'actuarial model'. Even though the risk management function is responsible for the design, implementation, testing and validation of the internal model this does not preclude the actuarial function from assisting in these tasks where deemed appropriate as set out in Article 47(1)(i). Depending on the complexity of the risk management system, actuarial methods may need to be applied that call for a detailed understanding of statistical methods and the probabilities of insurance risks, such as mortality, morbidity, claims frequencies and severities, understanding and assessing the use of risk mitigation techniques and understanding volatility and adverse deviation.
- 3.290. An effective risk management system requires input from the actuarial function (e.g. in the quantification and modelling of risks). This is not limited to a contribution to the ORSA or an internal model, if any, but includes also an involvement in e.g. asset-liability management, and risk mitigation arrangements.
- 3.291. The fact that the actuarial function shall "contribute to the effective implementation of the risk management system", and that according to Article 43(4) the risk management function shall facilitate the implementation of the risk management system, does not imply that both functions should be organised as different organisational units. A full or partial integration of these functions is acceptable.
- 3.292. Article 47(2) of the Level 1 text states:

*The actuarial function shall be carried out by persons with sufficient knowledge of actuarial and financial mathematics and able where appropriate, to demonstrate their relevant experience and expertise with applicable professional and other standards.*

- 3.293. It is incumbent upon the undertaking to make sure that persons charged with actuarial tasks have the relevant qualifications, experience and knowledge of applicable standards. CEIOPS does not envisage a specific university degree or training as a prerequisite for adequately fulfilling the actuarial function; in particular a person carrying out the relevant tasks does not need to acquire the occupational title of "actuary" in jurisdictions where such a title is available. The actuarial function requires an understanding of the stochastic nature of insurance and the risks inherent in assets and liabilities, including the risk of a mismatch between assets and liabilities, as well as an understanding of the use

of statistical models.

- 3.294. In order to be considered sufficient, the level of knowledge should be commensurate with the sophistication of the methodologies and techniques appropriately employed by the undertaking. Undertakings which under a risk-based approach may use relatively simple calculation methods, do not have an internal model or a complex risk management system and rely on elementary reinsurance arrangements, may require a comparatively lower level of knowledge in actuarial and financial mathematics in the person(s) carrying out the actuarial function. The undertaking shall be able to demonstrate to the supervisor that the applied methodologies and techniques are adequate having regard to the specificities of the undertaking.

### **CEIOPS' advice**

- 3.295. The actuarial function shall rely on European technical standards to be developed and endorsed by a body of representatives of different stakeholders, including CEIOPS.
- 3.296. The actuarial function shall have access to the appropriate information systems that provide all necessary information, relevant for the discharge of its responsibilities.
- 3.297. In coordinating the calculation of the technical provisions the actuarial function shall at a minimum:
- a) Apply methodologies and procedures to assess the sufficiency of technical provisions and to ensure that their calculation is consistent with the underlying principles;
  - b) Assess the uncertainty associated with the estimates;
  - c) Produce judgement whenever this is needed, making use of any relevant information and experience of the persons that are in charge of the function;
  - d) Ensure that problems related to the calculation of technical provisions arising from insufficient data quality are solved and that the most appropriate alternatives to common methods applied are found, taking into consideration the principle of proportionality;
  - e) Ensure that homogeneous risk groups for an appropriate assessment of the underlying risks are identified;
  - f) Consult any relevant market information and ensure that it is integrated into the assessment of technical provisions;
  - g) Compare and justify any material differences among the estimates for different years;
  - h) Ensure that an appropriate assessment of options and guarantees embedded in liabilities is provided.

- 3.298. In order to ensure the appropriateness of the underlying methodologies and models used in the calculation of the technical provisions, the actuarial function not only has to assess the general suitability of the methodology or underlying model for the calculation of technical provisions as such, but also has to decide whether they are appropriate for the specific lines of business of the undertaking, for the way the business is managed and for the available data.
- 3.299. While assessing the sufficiency and quality of the data used in the calculation of the technical provisions, the actuarial function should have regard to the objectivity, reasonability and verifiability of management actions included in the calculation of technical provisions. It should also assess whether information technology systems used in actuarial procedures sufficiently support these procedures.
- 3.300. The comparison of the best estimates against experience requires the actuarial function to assess whether past best estimates have proved sufficient and to use the insights gained in this assessment to improve the quality of present best estimate calculations.
- 3.301. In the scope of the coordination of the calculation of technical provisions the actuarial function should as under Article 47(1)(f) oversee when a case-by-case approach should be followed, that is, when there is not sufficient quality of data to apply a reliable actuarial method. Also, it has to produce judgement to establish assumptions and to safeguard the accuracy of the results. This analysis should also include comparisons between observed and expected values of the costs associated with technical provisions in order to produce conclusions on the appropriateness of the data used and the methodologies applied on their estimation.
- 3.302. Informing the administrative or management body of the reliability and adequacy of the calculation of the technical provisions is not limited to expressing an opinion on these points, including on the degree of uncertainty about the ultimate outcome and the circumstances that might lead to a significant deviation from the provisions made. The actuarial function must set out how it arrived at its opinion and clearly state and explain any concerns it may have as to the technical provisions being sufficient.
- 3.303. The actuarial function should oversee when a case-by-case approach to the calculation of technical provisions should be followed, that is, when there is not sufficient quality of data to apply a reliable actuarial method. Also, it has to produce judgement to establish assumptions and to safeguard the accuracy of the results.
- 3.304. Regarding the overall underwriting policy, the opinion to be expressed by the actuarial function should at least include the following issues:
- a) Sufficiency of the premiums to cover future losses, notably taking into consideration the underlying risks (including underwriting risks), the impact of expenses directly associated with future claims and of unallocated loss adjustment expenses and the impact of embedded options and guarantees on future liabilities;
  - b) Considerations regarding inflation, legal risk, change of mix, anti-selection and adequacy of *bonus-malus* system(s) implemented in specific line(s) of business.

- 3.305. Regarding the overall reinsurance arrangements, the opinion to be expressed by the actuarial function should include an opinion on the adequacy of the reinsurance and other mitigation techniques strategy in relation to the underwriting policy and the adequacy of the calculation of the technical provisions arising from reinsurance.
- 3.306. The comparison of the best estimates against experience requires the actuarial function to assess whether past best estimates have proved sufficient and to use the insights gained in this assessment to improve the quality of present best estimate calculations.
- 3.307. This analysis shall also include comparisons between observed and expected values of the costs associated with technical provisions in order to produce conclusions on the appropriateness of the data used and the methodologies applied on their estimation. The results of these comparisons should be reported to the administrative or management body.
- 3.308. In forming and formulating its own actuarial view the actuarial function shall be objective and free from influence of other functions or the administrative or management body. In order to be able to provide its opinions in an independent fashion, the actuarial function should be constituted by persons who verify a sufficient level of independency between them in order to appropriately form their own actuarial view in the exercise of the function's tasks.
- 3.309. The actuarial function shall at least annually produce written reports to be submitted to the administrative or management body. The reports shall document the tasks that have been undertaken, clearly state any shortcomings identified and give recommendations as to how the deficiencies could be remedied

## **3.7. Outsourcing**

### **Explanatory text**

3.310. Article 48(1) of the Level 1 text states:

*Member States shall ensure that, when insurance and reinsurance undertakings outsource operational functions or any insurance or reinsurance activities, the undertakings remain fully responsible for discharging all of their obligations under this Directive*

3.311. Outsourcing in the context of the Level 1 text means an arrangement of any form between an insurance or reinsurance undertaking and a service provider, whether a supervised entity or not, by which that services provider performs a process, a service or an activity, whether directly or by sub-outsourcing, which would otherwise be performed by the insurance or reinsurance undertaking by itself.

3.312. Therefore the Level 1 text refers to the full or partial provision by a third party (service provider) of any process, service or activity that an undertaking would otherwise perform in the course of its business itself. A service provider may be

authorised, it may be an entity from the same group as the undertaking (internal outsourcing) or not and it may be located inside the EU as well as outside.

- 3.313. In principle all functions and activities of a (re)insurance undertaking can be outsourced. The exceptions are core management functions as this would be incompatible with the undertaking remaining fully responsible for discharging its obligations.
- 3.314. An undertaking may outsource directly or indirectly via a third party (sub-outsourcing). Outsourcing does not prevent an undertaking from giving guidelines or instructions in individual cases as to how the outsourcing is to be performed.
- 3.315. Not every provision of a function or service to an undertaking by a service provider will fall within the meaning of outsourcing above. Hiring a specialist consultant to provide one-off technical advice does not constitute outsourcing, though it may become so if the undertaking subsequently relies on that consultant to manage an internal function or service, e.g. when it is installed or becomes fully operational. CEIOPS would expect to elaborate further on what might or might not constitute outsourcing in Level 3 guidance.
- 3.316. The undertaking should develop a written policy regarding outsourcing which should be approved by the administrative or management body.
- 3.317. The undertaking's outsourcing policy should include considerations of the impact of outsourcing on its business and the reporting and monitoring arrangements to be implemented when an outsourcing contract has been agreed. The policy should be regularly assessed and updated, with any necessary changes implemented.
- 3.318. As the undertaking remains fully responsible for all outsourced functions and activities it needs to include in its risk management systems and controls a process for monitoring and reviewing the quality of the service provided. It is not sufficient for the service provider itself to have internal controls and a risk management system that covers the services performed. In order to ensure effective control of outsourced activities and manage the risks associated with the outsourcing, the undertaking needs to maintain in-house the competence and ability to assess whether the service provider delivers according to contract.

- 3.319. Article 48(2) of the Level 1 text states:

*Outsourcing of critical or important functions or activities shall not be undertaken in such a way as to lead to any of the following:*

*(a) Impairing materially the quality of the governance system of the undertaking concerned;*

*(b) Increasing unduly the operational risk;*

*(c) Impairing the ability of the supervisory authorities to monitor the compliance of the undertaking with its obligations;*

*(d) Undermining continuous and satisfactory service to policyholders.*

- 3.320. CEIOPS believes that critical or important functions with regard to the provisions of the Level 1 text include the key functions of an undertaking's system of governance and all functions within the undertaking that are fundamental to carry out its core business, e.g. design, pricing and design of insurance products, investment of assets, portfolio management or claims handling.
- 3.321. The provision by a third party of functions such as legal opinions or specialised training is not considered by CEIOPS as critical or important for the purposes of the Level 1 text. This is because, even if they could be considered outsourcing under certain specific circumstances, they do not form part of an undertaking's core business.
- 3.322. When choosing a service provider for any critical or important functions or activities the undertaking has to carry out all necessary steps to see that:
- a) A detailed examination is performed of the potential service providers' ability and capacity to deliver the required functions or activities satisfactorily, taking into account the undertaking's objectives and needs;
  - b) The service provider has adopted all means to ensure that no explicit or potential conflicts of interest with the undertaking impair the needs of the outsourcing undertaking;
  - c) It enters into a written agreement with the service provider which clearly allocates the respective rights and obligations of the undertaking and the service provider;
  - d) The general terms and conditions of the outsourcing agreement are authorised and understood by the undertaking's administrative or management body;
  - e) The outsourcing does not represent a breach of any data protection regulation or any other laws; and
  - f) The service provider is subject to the same provisions that are applicable to the undertaking regarding the safety and the confidentiality of the information related to its clients.
- 3.323. The examination to be performed should allow the undertaking to understand the main risks that might arise from the outsourcing, identify the most suitable strategies for the mitigation/management of these risks and ensure that the service provider has the ability, capacity and any authorisation required by law to perform the outsourced activities reliably and professionally. The conclusions should be documented and reviewed by the undertaking at any time it is considered relevant.
- 3.324. The written agreement to be concluded between the undertaking and the service provider should clearly state the following requirements:
- a) The duties and responsibilities of both parties involved;
  - b) The service provider's commitment to comply with all applicable laws, regulatory requirements and guidelines and to cooperate with the undertaking's supervisors in connection with the outsourced function or activity;

- c) That the service provider can only terminate the contract with a period sufficiently long to enable the undertaking to find an alternative solution;
- d) That the undertaking has the right to terminate the arrangement for the outsourcing with a reasonable period of notice if for any reason the services rendered should prove to be inadequate;
- e) That the undertaking reserves the right to information about the outsourced activities and the service provider's performance of the outsourcing as well as a right to issue general guidelines and individual instructions as to what is to be taken into account when performing the outsourced functions or activities;
- f) That the service provider shall protect any confidential information relating to the undertaking and its clients;
- g) That the undertaking, its external auditor and the supervisory authority competent for its supervision will have effective access to all information related to the outsourced functions or activities, as well as to the service provider's business premises if an on-site inspection or audit is to be performed;
- h) That the supervisory authority has the right to directly address questions to the service provider.

3.325. If the service provider is located outside the Member State of the undertaking the written agreement to be established should also include provisions on the resolution of any disputes between the undertaking and the service provider, namely regarding the jurisdiction that proceedings are subject to.

3.326. The outsourcing agreement should also determine whether sub-outsourcing is possible. If this is the case, the agreement between the service provider and the sub-service provider(s) needs to regulate the conditions which apply and must not affect the service provider's responsibilities under the outsourcing agreement with the undertaking. Generally the service provider must ensure the quality of the sub-service provider in the same way the undertaking is to make sure the service provider is able to render satisfactory services. The undertaking also has to maintain the rights and powers of the supervisory authority with regard to the sub-outsourced activities. The undertaking remains responsible for ensuring the outsourced activity is satisfactorily performed, including the terms of the sub-outsourcing contract.

3.327. The ownership of any intellectual work rendered by the service provider, e.g. in the case of software development, should be made clear in the outsourcing agreement, both in case of cancellation or contract expiration.

3.328. Irrespective of the service provider's risk management obligation to establish suitable contingency plans, the undertaking needs to consider in its own contingency planning the possibility of having to face an emergency situation or business disruption arising from a failure or a problem of the service provider.

3.329. The undertaking should ensure that the service provider discloses any developments that may have a material impact on its ability to carry out the outsourcing including any adverse effect from new laws or regulations introduced in its home country and any material changes to its financial

resources or its risk profile.

- 3.330. In case of internal outsourcing, i.e. where the service provider is in the same group as the undertaking, some of the requirements may be applied more flexibly. The examination of the service provider may be less detailed provided the undertaking's administrative or management body has greater familiarity with the service provider and if the undertaking has sufficient control over, or can influence the actions of, the service provider.
- 3.331. Internal outsourcing may potentially pose a lower level of risk to an undertaking but it is unlikely to pose no risk at all. Hence the undertaking should assess whether and to what extent it should rely on functions and activities provided. A written agreement must always exist, stipulating the duties and responsibilities of both parties. However, this could assume the form of a service level agreement.
- 3.332. It should be noted that, in common with other directives, e.g. the Capital Requirements Directive (CRD) and the Markets in Financial Investments Directive (MiFID), the Solvency II Level 1 text applies to an undertaking and not its group. While the supervisory review process may take into account a group as a whole and the extent to which an entity within the group provides a service or function for other undertakings in the same group, the obligations remain with the individual undertaking as it is the authorised entity. While an undertaking may delegate to another group member the carrying out of services or functions, it cannot absolve itself of responsibility for them.
- 3.333. To ensure that the outsourcing of any critical or important functions or activities does not lead to a material impairment of the quality of the undertaking's governance system:
- a) The undertaking must ensure that the service provider has in place an adequate risk management and internal control system;
  - b) The outsourced activities must be adequately included in the undertaking's risk management and internal control system; and
  - c) The undertaking must establish a contractual right to information about the outsourced activities and a contractual right to issue instructions concerning the outsourced activities.
- 3.334. In order to ensure against an undue increase of operational risk, when outsourcing critical or important functions or activities the outsourcing undertaking should:
- a) Verify that the service provider has adequate financial resources to take on the additional tasks the undertaking plans to delegate and to properly and reliably discharge its duties towards the undertaking and that the staff of the service provider is chosen on the basis of criteria that give reasonable assurance that they are sufficiently qualified and reliable;
  - b) Verify that the service provider properly isolates and identifies the information, documentation and assets belonging to the undertaking and its clients in order to protect their confidentiality; and
  - c) Make sure the service provider has adequate contingency plans in place to

deal with emergency situations or business disruptions and has periodic testing of backup facilities where that is necessary having regard to the function, service or activity outsourced.

3.335. In order to ensure that the outsourcing of critical or important functions or activities does not impair the ability of the supervisory authorities to monitor the compliance of the undertaking with its obligations under the Level 1 text must comply with Article 38 of the Level 1 text and must ensure:

- a) The service provider's cooperation with the supervisory authorities of the undertaking in connection with the outsourced functions or activities;
- b) The undertaking, its auditors and the relevant supervisory authorities have effective access to data related to the outsourced functions or activities; and
- c) The supervisory authorities have a right of access to the business premises of the service provider and are able to exercise this right.

3.336. CEIOPS considers that a written agreement between an undertaking and its service provider containing the requirements set out in paragraph 3.324, in particular g) and h), will ensure compliance with Article 38. Such a written agreement will also ensure that, irrespective of whether or not a service provider is located in the EU, the undertaking's supervisory authorities will be able to monitor the undertaking's compliance with its obligations.

3.337. As part of good management practice, CEIOPS expects an undertaking to monitor continuously whether its service provider is in compliance with all the terms of their written agreement. If, for example, a service provider is subsequently unwilling to cooperate with the undertaking's supervisory authorities, the undertaking should terminate the outsourcing agreement. In this, context, where a service provider is located outside the EU, undertakings should pay particular attention to whether the service provider's regulator and /or local laws and regulations might restrict access to information about the outsourced activity or function or to the service provider's premises.

3.338. Article 48(3) of the Level 1 text states:

*Insurance and reinsurance undertakings shall, in a timely manner, notify the supervisory authorities prior to the outsourcing of critical or important functions or activities as well as of any subsequent material developments with respect to those activities.*

3.339. CEIOPS envisages that the critical or important activities which involve notification requirements in case of outsourcing will be identified consistently across the Member States when the Level 1 text is implemented into national law. It also expects supervisors to be endowed with the necessary powers to intervene if the outsourcing arrangements give rise to concerns about a possible non-compliance with Article 48 or Article 38(1)(b) or any of the conditions for outsourcing the Commission may adopt by way of implementing measures pursuant to Article 49(4).

3.340. Article 38(3) requires undertakings to notify supervisory authorities in a timely manner prior to the outsourcing of critical or important functions or activities. This does not imply that the supervisor has to approve or authorise the

outsourcing. Rather the prior notification presents an opportunity for the supervisor to discuss concerns with the undertaking if the outsourcing appears not to comply with the provisions of the Directive and to object if supervisory concerns cannot be dispelled. Accordingly, CEIOPS interprets “in a timely manner” to constitute a period of time sufficient for the supervisor to examine the proposed outsourcing before it comes into force. This could be at least six weeks before the outsourcing is due to come into effect.

- 3.341. Subsequent material developments that entail further notification requirements are all developments that are relevant for supervisory purposes, i.e. any circumstances that may give supervisors reason to reassess the compliance with the Directive or implementing measure requirements or adversely affect the undertaking’s ability to deliver its service to policyholders. This could in particular apply to material changes in the outsourcing arrangements, a change of service provider or major problems with the performance of the service provider, such as e.g. non-performance on account of business disruption, non-compliance with applicable laws and regulations, serious and repeated infringements of guidelines, inadequate risk management, insufficient granting of access to data and information or anything else that causes significant dissatisfaction to the undertaking or policyholders about the service.
- 3.342. Taking into consideration the requirements that have to be met, particularly those in respect of the written agreement between an undertaking and its service provider, CEIOPS believes that these notification arrangements are suitably flexible and that different notification arrangements for service providers located inside the EU as opposed to outside the EU are not necessary.

### **CEIOPS’ advice**

- 3.343. The undertaking’s outsourcing policy shall include considerations of the impact of outsourcing on its business and the reporting and monitoring arrangements to be implemented in case of outsourcing. The policy shall be regularly assessed and updated with any necessary changes implemented.
- 3.344. If an undertaking and the service provider are members of the same group, the undertaking may take into account the extent to which it controls the service provider or has the ability to influence its actions.
- 3.345. Critical or important functions with regard to the provisions of the Level 1 text include the key functions of an undertaking’s system of governance and all functions within the undertaking that are fundamental to carry out its core business.
- 3.346. When choosing a service provider for any critical or important functions or activities the undertaking shall undertake all necessary steps to ensure that:
- a) A detailed examination is performed of the potential service provider’s ability and capacity to deliver the required functions or activities satisfactorily, taking into account the undertaking’s objectives and needs;
  - b) The service provider has adopted all means to ensure that no explicit or potential conflict of interests with the undertaking impairs the needs of the undertaking;

- c) It enters into a written agreement with the service provider which clearly allocates the respective rights and obligations of the undertaking and the service provider;
- d) The general terms and conditions of the outsourcing agreement are authorised and understood by the undertaking's administrative or management body;
- e) The outsourcing does not represent a breach of any data protection regulation or any other laws; and
- f) The service provider subjects to the same provisions that are applicable to the undertaking regarding the safety and the confidentiality of the information related to its clients.

3.347. The written agreement to be concluded between the undertaking and the service provider should clearly state the following requirements:

- a) The duties and responsibilities of both parties involved;
- b) The service provider's commitment to comply with all applicable laws, regulatory requirements and guidelines and to cooperate with the undertaking's supervisors in connection with the outsourced function or activity;
- c) That the service provider can only terminate the contract with a period sufficiently long to enable the undertaking to find an alternative solution;
- d) That the undertaking has the right to terminate the arrangement for the outsourcing with a reasonable period of notice if for any reason the services rendered should prove to be inadequate;
- e) That the undertaking reserves the right to information about the outsourced activities and the service provider's performance of the outsourcing as well as a right to issue general guidelines and individual instructions as to what is to be taken into account when performing the outsourced functions or activities;
- f) That the service provider shall protect any confidential information relating to the undertaking and its clients;
- g) That the undertaking, its external auditor and the supervisory authority competent for its supervision will have effective access to all data related to the outsourced functions or activities, as well as to the service provider's business premises if an on-site inspection or audit is to be performed;
- h) That the supervisory authority has the right to directly address questions to the service provider.

3.348. To ensure the outsourcing of any critical or important functions or activities does not lead to a material impairment of the quality of the undertaking's governance system:

- a) The undertaking must ensure that the service provider has in place an adequate risk management and internal control system;

- b) The outsourced activities must be adequately included in the undertaking's risk management and internal control system; and
- c) The undertaking must establish a contractual right to information about the outsourced activities and a contractual right to issue instructions concerning the outsourced activities.

## 4. Annexes

### Annex A: Main conclusions taken out from the QIS 4 OpRisk questionnaire

While developing the implementing measures to be applied in the context of the management of operational risk, CEIOPS has taken into account the main findings from the operational risk section of the QIS4 exercise, namely the ones on the qualitative questions, published in October 2008, which were:

- The average per country of the percentage of the **operational risk capital charge** to the total SCR ranged from 5% to 10%;
- 47% of the respondents felt that the operational risk charge is **adequately designed**, while 53% of respondents thought it was not adequately designed;
- One Member State responded that the operational risk charge as currently calibrated in the standard formula understates the operational risk requirement as set by the undertakings' own **internal model** sometimes by more than half;
- In relation to the **formula**, respondents stated that:
  - The standard formula is too simplistic, since it is not risk sensitive, and rewards low pricing and reserving;
  - The consideration of 100% correlation with other risks is not appropriate;
  - The formula does not take into account the quality of the operational risk management processes of each undertaking, nor does it encourage the development of good risk management practices;
  - The maximum of 30% of the BSCR for the capital charge is considered too high;
  - The formula does not reflect the wide spectrum of operational risks that can materialise within an undertaking;
- The main suggestions to **remedy the perceived deficiencies** in the standard formula were:
  - The operational risk charge should be calculated as a percentage of the BSCR or the SCR;
  - The operational risk charge should be more sensitive to operational risks management;
  - The operational risk charge should be based on the entity-specific operational risk sources and the quality of the operational risk management process and the internal control framework;
  - Diversification benefits and risk mitigation techniques should be

considered;

- Regarding the qualitative questions posed about operational risk management systems, the responses indicated that there is a **wide range of practices** currently followed by undertakings, with some indicating that they have stochastic modelling techniques to quantify capital requirements for operational risk and others had yet to even start collecting and categorising operational risk losses. For example, 39% of respondents stated that they capture operational risk loss events and most of these then attempt to quantify these loss events;
- Among the undertakings that categorise the operational risk events, the most **common categorisation** used is the one proposed by the Operational Risk Insurance Consortium (**ORIC**<sup>17</sup>), which is based on the categorisation established by the Capital Requirements Directive (Basel II). A number of undertakings however stated that they used their own categorisation.

## **Annex B: Actuarial Function – Issues and options considered**

See separate Excel file.

---

<sup>17</sup> The Operational Risk Insurance Consortium (ORIC) is a partnership established between the Association of British Insurers (ABI) and the software company SAS that intends to provide a high-quality database cataloguing operational risk loss events. ORIC members receive, on a quarterly basis, information on losses due to failed people, processes, systems or external events, by both monetary amount and narrative description. To feed the database, individual firms have to submit their own data on operational risk, with total anonymity.