

# Issues Paper

## Risk Management and Other Corporate Issues

*CEIOPS publishes the following Issues Paper on "Risk Management and Other Corporate Issues" to inform CEIOPS' possible further work and any wider discussion.*

*Comments are welcome, although not required as for CEIOPS' Consultation Papers. CEIOPS will not provide feedback to comments. It will take them into account in its future work.*

*Please send any comments to CEIOPS by email ([Secretariat@ceiops.org](mailto:Secretariat@ceiops.org)) by 17 October 2007, indicating the reference "CEIOPS-PII-11/07".*

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

1.	Introduction.....	3
2.	General requirements.....	3
2.1.	Organisational structure .....	4
2.2.	Fit and proper .....	5
2.3.	Risk management system .....	6
2.4.	Internal control system .....	7
2.5.	Actuarial function .....	9
2.6.	Formalisation of the systems.....	10
3.	Strategic risk .....	11
4.	Insurance specific risk .....	12
4.1.	Product design and pricing.....	13
4.2.	Selling .....	13
4.3.	Provisioning.....	14
4.4.	Claims management .....	14
4.5.	Reinsurance and alternative risk transfer .....	15
5.	Market risk, including Asset-Liability Management .....	18
6.	Credit risk .....	21
7.	Concentration risk .....	23
8.	Liquidity risk .....	24
9.	Operational risk.....	26
10.	Reputational risk .....	29
11.	Correlation effects .....	30

## **1. Introduction**

1. As part of its preparation for future work under the Solvency II project, CEIOPS has on its own initiative developed high level principles and minimum qualitative requirements, which could form the basis for a risk and governance structure of undertakings.
2. The principles and minimum requirements would apply to solo insurance and reinsurance undertakings as well as to group undertakings (undertakings).
3. This paper sets out some of those principles. The paper represents the direction of CEIOPS' initial thinking on these issues.
4. It is not a formal CEIOPS Consultation Paper. Its purpose is to inform possible further work by CEIOPS in defining fundamental requirements for all undertakings, identifying potential options in the light of forthcoming Level 2 implementing measures, and also to inform any wider discussion, including on a 3 Level 3 basis.

## **2. General requirements**

1. Undertakings should have in place a robust system of governance, which provides for sound and prudent management of the business, including outsourced activities.
2. That system shall at least include an adequate organisational structure with well defined, transparent, consistent and enforced reporting lines, allocation of responsibilities and appropriate segregation thereof.
3. Undertakings shall take reasonable steps to ensure continuity and regularity in their operational performance. To this end the undertaking shall employ appropriate systems, resources and procedures, including contingency plans.
4. The system of governance shall be proportionate to the nature, scale and complexity of the operations of the undertaking.
5. The system of governance shall be subject to regular internal review. The review should be carried out by internal audit, external service provider or any other party commissioned to execute it by the administrative or management body. The administrative or management body should approve the review and decide if any actions are needed.
6. Undertakings shall have written policies in place including on risk management, internal control and, where relevant, outsourcing which clearly set out the strategies, processes and reporting procedures applied.
7. Those written policies shall be reviewed at least annually. They shall be subject to prior approval by the administrative or management body and be adopted before any significant change in the system or area concerned.

### Proportionality principle and function definition

8. A function is an administrative capacity to undertake particular tasks. A function may be undertaken by permanent or temporary staff of an undertaking or by way of outsourcing.
9. Unless otherwise specified, undertakings may freely determine administrative arrangements for fulfilling the necessary functions in accordance with their available resources, having regard to the nature, scale and complexity of their operations. It follows that in small undertakings more than one function may be carried out by one person – as long as these are not incompatible –, or by way of outsourcing.
10. All undertakings must have an adequate internal control system. The application of proportionality, in this context, means that where additional functions are specified, such as the actuarial function, compliance function or internal audit function, undertakings may freely determine their need for separate functions to achieve an adequate internal control system.
11. In the case of undertakings with a reduced level of business activity and a reduced dimension of risks associated to their business in which, due to the limitations of available resources, total segregation of duties is impracticable, additional control procedures shall be implemented that ensures an equivalent level of security.

### **2.1. Organisational structure**

12. The undertaking shall have a well-defined organisational structure that should support the implementation of efficient risk management and internal control systems, in order to ensure that the management and control of operations are undertaken in a sound and prudent manner.
13. The organisational structure must have a clear and objective definition of the reporting lines and responsibilities and include a suitable segregation of duties.

### Organisational culture

14. The organisational culture of the undertaking must ensure that there is coherence throughout the entire organisational structure as to the application of risk management and internal control practices, in order to ensure sound and prudent management of the undertaking's business.
15. In order to support development of an organisational culture consideration should be made regarding the need to draw up and implement a code of conduct.

### Information and communication systems

16. The organisational structure of the undertaking shall ensure the existence of suitable information systems and communication channels taking into consideration its activities, strategies, objectives and needs.

17. The information systems implemented shall be secure and produce reliable, consistent, high quality, sufficient, timely and relevant information concerning the business activity, the commitments assumed and the risks to which the undertaking is exposed.
18. Internal and external communication channels and reporting lines shall be defined in order to ensure effective communication throughout the organisation and ensure the timely and appropriate reporting of information to relevant levels within the undertaking and appropriate functions.

Administrative or management body' responsibilities on the organisational structure

19. The administrative or management body is responsible for ensuring that the organisational structure permits the undertaking to establish suitable governance mechanisms having regard to the scale, nature and complexity of its business activity.
20. The administrative or management body is responsible for ensuring compliance with the strategies, policies, objectives and guidelines defined in relation to the undertaking's organisational structure.

**2.2. Fit and proper**

21. Undertakings shall ensure that all persons who effectively run the undertaking or have other key functions, including independent non-executive directors, are at all times fit and proper. Their professional qualifications, knowledge and experience shall be sufficient and adequate to enable sound and prudent management (fit). Their repute, conduct and actions shall be such as to ensure that their integrity is to the highest standards (proper).
22. The qualifications that individual fitness entails will depend on the specific function a member of the administrative or management body is to hold. The members of the administrative or management body should also be collectively fit to run the company, i.e. as a whole, they should have all necessary qualifications.
23. The undertaking should identify the persons who run key functions and, based on pre-established criteria and minimum requirements, assess whether they are fit and proper.
24. The key functions identified should be disclosed.
25. The undertaking should establish necessary processes and procedures that ensure that persons running key functions are assessed before they are appointed. These processes should also ensure that confidential information concerning the fit and proper assessment is kept confidential.

### **2.3. Risk management system**

26. The rationale for insurance business is to take on risk. The management of that risk is a very important part of the operations of undertakings.
27. Risk management is a continuous process that should be used in the implementation of the strategy of the undertaking and which should allow an appropriate understanding of the nature and significance of the risks to which the undertaking is exposed.
28. The objective of risk management is to identify, evaluate, mitigate, monitor and control all material risks to which the undertaking is exposed, both at the internal and external levels.

#### Principles applicable to risk management systems

29. The risk management system shall be supported by a well-defined organisational structure and a suitable internal control system and shall be proportional to the scale and complexity of the business activity of the undertaking, taking into consideration the nature and specific characteristics of the risks that the undertaking currently assumes or intends to assume.
30. A suitable risk management system must take into consideration:
  - a) The risks directly associated with the insurance business;
  - b) The relevant risks that, while not directly associated with the insurance business, underlie this business activity.
31. The risk management system must take into consideration the insurance specific risks, market, credit, operational and liquidity risks and all other risks which, given the undertaking's specific situation, may become material, e.g. the fact of being part of a group<sup>1</sup>.

#### Administrative or management body's responsibilities on the risk management system

32. The administrative or management body has responsibility for approving the risk strategy for the undertaking. The administrative or management body shall be responsible for ensuring that a suitable and effective risk management system is implemented and monitored.
33. In the framework of a suitable risk management system, the administrative or management body is responsible for the approval of any periodic revision of the main strategic guidelines and business policies of the undertaking.
34. The administrative or management body shall ensure that the risks to which the undertaking is exposed are identified, evaluated and mitigated and shall provide for the existence of adequate mechanisms required to monitor and control such risks.

---

<sup>1</sup> Risk classifications in this Issues Paper are used for the Paper's purposes only. CEIOPS recognizes that international organisations such as IAA, IAIS and the Joint Forum have alternative interpretations of certain risks. CEIOPS also does not intend that classifications here anticipate negotiations for the final Framework Directive.

### Risk management function

35. The undertaking must establish a risk management function within its organisation structure that is suited to the scale, nature and complexity of the respective operations.
36. The risk management function must be performed in an objective and independent<sup>2</sup> manner in relation to the undertaking's operations.

### Risk modelling function

37. The internal model is part of a comprehensive risk management system, which must possess adequate resources and structures to ensure properly functioning processes.
38. For undertakings that submit partial or full internal model to be approved, a risk modelling function must be in place.
39. The risk modelling function should develop and document all features of the internal model.
40. This function should be responsible for the way in which the actuarial model is integrated with the internal risk management system. It should assess the internal model as a tool of risk management and as a tool to calculate the undertaking's SCR (solvency capital requirement). The linkage between the actuarial model and the risk management function, known also as 'use test', should be ensured by this function.

## **2.4 Internal control system**

41. Internal control comprises a coherent, comprehensive and continuous set of processes implemented by the administrative or management body and all other staff members of the undertaking with the objective of ensuring the following:
  - a) Effectiveness and efficiency of operations;
  - b) Availability and reliability of financial and non-financial information;
  - c) An adequate control of risks;
  - d) A prudent approach to business;
  - e) The efficiency of the risk management system, including, in particular, insurance risks, together with market, credit, liquidity and operational risks;
  - f) Compliance with legislation and other regulations as well as internal policies and procedures;
  - g) Compliance with other governance mechanisms defined by the administrative or management body.

---

<sup>2</sup> For example, the risk management function is often performed by an independent Chief Risk Officer (CRO).

### Principles applicable to the internal control system

42. The internal control system of the undertaking should be built upon an efficient risk management system and appropriate and clearly defined control activities, monitoring and reporting procedures, and should be supported by a suitable organisational structure.
43. An efficient internal control system demands an appropriate segregation of duties and clear reporting lines and responsibilities, both at individual level and between functions.
44. The internal control system should be tailored to the scale, nature and complexity of the business, to the predefined degree of centralisation and delegation of authority and to the capacity and effectiveness of the information technologies, and should be based on the risk tolerance level defined for each business area of the undertaking.

### Administrative or management body' responsibilities on the internal control system

45. The administrative or management body is responsible for approving an internal control strategy and establishing and maintaining a suitable and effective internal control system.
46. Within the framework of the internal control system, the administrative or management body is responsible for providing suitable direction to implement prudential control measures to ensure an appropriate and effective level of management and control of the undertaking so that its business activity is complying with legislation and other regulations in force.
47. The administrative or management body is responsible for promoting a high level of integrity and for establishing a culture within the company that emphasises and demonstrates to all levels of personnel the importance of internal control.
48. The administrative or management body are responsible for initiating the development, implementation, maintenance and monitoring of the internal control system and for ensuring its efficiency and suitability, in compliance with the strategies and guidelines established.
49. The administrative or management body are also responsible for ensuring that the undertaking's organisational and procedural controls function efficiently.

### Monitoring and revision of the internal control system

50. The undertaking must develop, implement and maintain appropriate monitoring mechanisms for the internal control system, in order to comply with defined policies and established procedures, as well as to ensure their effectiveness and suitability in light of the undertaking's business activity.
51. The mechanisms specified in the previous paragraph shall facilitate the understanding from a broad perspective of the undertaking's situation and provide the administrative or management body with relevant information for the decision-making process.

52. The administrative or management body shall periodically receive reporting on the monitoring of the undertaking's internal control system, including the identification of any faults and/or fragilities detected, either when evaluated on an isolated basis or in an aggregated manner.

#### Compliance function

53. Compliance risk is defined as the risk of legal or regulatory sanctions, material financial loss, or loss of reputation an undertaking may suffer as a result of its failure to comply with laws, regulations and administrative provisions.
54. The compliance function should identify, assess, advise, monitor and report on the compliance risk exposure.
55. The compliance function includes also advising the administrative or management body on compliance with the laws, regulations and administrative provisions. It may also include an assessment of the possible impact of any changes in the legal environment on the operations of the undertaking concerned and the identification and assessment of compliance risk.
56. In small undertakings the tasks of the compliance function may be performed within the internal control system or by the internal audit function.

#### Internal audit function

57. The internal audit function is an independent function that should identify and propose ways to improve the undertaking's operations. It should help the undertaking accomplish its objectives by bringing a systematic and disciplined approach to evaluating and improving the effectiveness of risk management, internal control and other governance functions and other processes and policies.
58. All undertakings shall have an internal audit function. Having regard to the scale, nature and complexity of the undertaking's activities, the same level of robustness of internal control can also be achieved by other arrangements like regular and/or systematic inspections and assessments made by outsourced service providers or utilising internal group audit . Depending on the scale, nature and complexity of the activities of the undertaking, the internal audit function should report to an audit committee established by the administrative or management body.
59. The internal audit function shall have sufficient authority in order to perform its competencies in an objective and independent manner, and should not have a direct link to the undertaking's operational functions that will be subject to evaluation.

### **2.5 Actuarial function**

60. The undertaking shall establish and maintain an actuarial function. The actuarial function requires an understanding of the stochastic nature of

insurance and the risks inherent in assets and liabilities, including the risk of mismatch between assets and liabilities, and in the use of statistical models.

61. Actuarial methods are used to assess risks, determine the adequacy of premiums (tariffs) and establish technical provisions for both life and non-life insurance. These methods include a detailed understanding of the probabilities of insurance risks (e.g. mortality, morbidity, claims frequencies and severities), the use of statistical methods, the use of discounted cash flows, understanding and assessing the use of risk mitigation techniques and an understanding of volatility and adverse deviation.
62. The actuarial function should make an assessment of:
  - a) The overall underwriting policy;
  - b) The claims management procedures;
  - c) The appropriateness of the methodologies and underlying models used, as well as the assumptions made in the calculation of technical provisions;
  - d) The sufficiency and quality of the data used in the calculation of technical provisions;
  - e) The objectivity, reasonability and verifiability of management actions included in the calculation of technical provisions;
  - f) The overall investment policy and management;
  - g) The overall reinsurance, and other risk mitigation techniques, policy and management;
  - h) IT systems used in actuarial procedures, namely from the actuarial point of view.
63. The actuarial function assessment does not imply a formal approval or the take over of the responsibility for the issues assessed.
64. The actuarial function must produce an annual report with the findings and recommendations to the administrative or management body. This report must be drawn up with clarity and suitable objectivity, in order to comply with the obligation to provide information.
65. Detailed monitoring should be undertaken regarding the measures implemented by the undertaking in the pursuit of the actuarial recommendations.

## **2.6 Formalisation of the systems**

66. The undertaking shall formalise in specific documentation the main risk management and internal control policies, strategies and procedures.
67. The documentation specified in the previous paragraph shall identify clearly and in detail the systems that have been implemented for the identification, assessment, mitigation, monitoring and control of the risks, together with the specific control activities implemented within the framework of the internal control system.

### **3. Strategic risk**

#### Background

1. 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.
2. Strategic risk is a function of the compatibility of an undertaking's strategic goals, the business strategies developed to achieve those goals, the resources deployed against these goals, and the quality of implementation.
3. 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 must be evaluated against the impact of economic, technological, competitive, regulatory, and other environmental changes.

#### High level principles

4. The undertaking should have a process for setting strategic-high-level objectives and translating these into detailed shorter-term business and operation plans.
5. The administrative or management body of the undertaking should approve and oversee the undertaking's strategic goals, objectives (including risk management objectives), corporate culture and behaviour.

#### Minimum requirements

6. Strategic goals, objectives, corporate culture, and behaviour should be effectively communicated and consistently applied throughout the undertaking. Strategic direction and organisational efficiency should be enhanced by the depth and technical expertise of the administrative or management body.
7. Management information systems employed at the undertaking should effectively support strategic direction and initiatives.
8. Strategic initiatives should be well conceived and supported by appropriate communication channels, operating systems, and service delivery networks. The initiatives should be supported by capital for the foreseeable future and pose only nominal possible effects on earnings volatility.
9. Strategic initiatives should be supported by sound due diligence and strong risk management systems. It should be possible to reverse decisions with little difficulty and manageable costs.
10. Risk management practices should be an integral part of the overall strategic planning. The quality of risk management should be consistent with the strategic issues confronting the undertaking.

11. Exposures to different risk and businesses should reflect strategic goals that are not overly aggressive and are compatible with developed business strategies.

#### **4. Insurance specific risk**

##### Background

1. Underwriting risk means the risk of loss, or of adverse change in the value of insurance liabilities, resulting from potential expense overruns due to inadequate pricing and provisioning assumptions.
2. The life underwriting risk is the risk arising from the undertaking of life insurance contracts. The Solvency Capital Requirement standard formula covers the following risks:
  - a) Mortality risk;
  - b) Longevity risk;
  - c) Disability - morbidity risk;
  - d) Life expense risk;
  - e) Revision risk;
  - f) Lapse risk; and
  - g) Life catastrophe risk.
3. The non-life underwriting risk is the risk arising from the undertaking of non-life insurance contracts. The Solvency Capital Requirement standard formula covers the following risks:
  - a) Premium and reserve risk; and
  - b) Non-life catastrophic risk.
4. A proper execution of the processes of product design and pricing, selling, provisioning, claims management and reinsurance management is a very important tool to identify, evaluate, mitigate, monitor and control these risks.
5. Product design and pricing risk is the exposure to financial loss resulting from transacting insurance and annuity business where the costs and liabilities assumed in respect of a product line exceed the expectation in pricing of that product line.
6. After selling the products, the valuation of technical provisions and a proper management of claims is also a fundamental part of the risk management system.
7. Reinsurance, as a risk mitigation technique, enables the undertaking to prudently manage and/or mitigate the underwriting risk.

## **4.1. Product design and pricing**

### High level principles

8. The undertaking must establish an underwriting policy, which is adequate to the scale, nature and complexity of its business.
9. Sound product design and pricing involves prudently managing the risk/premium relationship of each product and controlling product risk.
10. The basis of an effective product design and pricing risk management program is the identification of the existing and potential risks of the products commercialised.

### Minimum requirements

11. A comprehensive product design and pricing management program should:
  - a) Identify current and new product lines, significant pricing changes, or product changes which require an adjustment in the price charged;
  - b) Develop product design and pricing policies to effectively manage and control those product lines.
12. An undertaking should develop and implement comprehensive procedures and information systems to effectively monitor and control product development and pricing. These procedures should define criteria to identify and report potential problems, followed by appropriate corrective action.

## **4.2. Selling**

### High level principles

13. The undertaking should establish proper procedures of risk identification and selection to be applied at the time of acceptance of the insurance contracts.
14. The undertaking must ensure that all sellers of insurance products, whether they are employees or intermediaries, apply the procedures defined.

### Minimum requirements

15. The undertaking should ensure that all policies and procedures established for pricing and provisioning, especially in what regards data collection, are applied by all distribution channels of the company.
16. The undertaking should establish one policy on different commissions levels and discounts to be applied by different distribution channels.
17. Proper monitoring and control procedures should be implemented in order to ensure that all requirements are complied with by the intermediaries.

### **4.3. Provisioning**

#### High level principles

18. A proper valuation of technical provisions is essential for an effective management of the underwriting policy or for asset-liability management (ALM).
19. The management of technical provisions is an ongoing process that is required to ensure that the technical provisions are adequate for covering the obligations towards the policyholders.

#### Minimum requirements

20. Suitable controls, systems and procedures should be in place to ensure the reliability, sufficiency and adequacy of both the statistical and accounting data to be considered in the valuation of technical provisions.
21. The data should be complete, e.g. for claims provisions all claims reported should be introduced in the systems. The undertaking must be able to explain the methodologies applied in collecting the data used to calculate the technical provisions, including how data has been checked and how data irregularities have been dealt with.
22. It should be ensured that all responsibilities, including options embedded in the products, are taken into account, and that the products are well understood.
23. For provisions to be established, reliable back-testing of the methods used against statistical data such as the run-off of claims reserves must be carried out in a proper form and in line with approved procedures.
24. To support the adequate valuation of technical provisions, resources in terms of staff, equipment and software allocated in IT should be appropriate, both in quality and quantity, for ensuring that the systems and controls are effective and reliable at all times. Strict internal controls should be in place, in particular in the cases where algorithms are used to process data under computing systems.
25. Models based upon commercial software modelling packages require the modeller to be assured that the vendor has done significant testing of his/her product and has in place procedures to monitor and improve the products' accuracy.
26. Models developed in-house must be thoroughly tested through a rigorous and systematic process to ensure that the results are properly determined and make appropriate use of the input data.

### **4.4. Claims management**

#### High level principles

27. An undertaking should have in place adequate claims management mechanisms in order to protect it from paying higher claims than

framed in its contractual obligations under the insurance policy that could threaten its solvency position.

28. The claims management should cover the overall cycle of claims: reception, assessment, processing and settlement and complaints and dispute settlement.
29. The undertaking should establish internal procedures to deal with claims in a timely manner.
30. Claims should be paid according to the relevant law and insurance terms and conditions.
31. Claims should be paid without any undue delay. All claimants should be treated fairly. The claims should not be handled by someone who could have any conflict of interest.

#### Minimum requirements

32. The undertaking should ensure that the policyholder/claimant/beneficiary knows how to report a claim. The undertaking should provide the information necessary to help on the claims reporting process.
33. The undertaking should have a claims management function that is as accessible as possible for the policyholder/claimant/beneficiary. If an intermediary is the initial contact, claims should be sent to the undertaking within an appropriate time period.
34. When assessing claims, the undertaking should take into account all relevant factors according to the insurance terms and conditions of the contract.
35. Regular internal audits should be carried out for all claims not settled.
36. In cases of no or partial claims payment, the policyholders should be informed in writing of the reasons underlying.
37. The undertaking should establish a process to deal with complaints and dispute settlement.

### **4.5. Reinsurance and alternative risk transfer**

#### Background

38. Reinsurance management is an ongoing process that may be used to keep the undertaking's risks at an acceptable level through appropriate reinsurance arrangements. 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) reinsurance, which are both addressed in the CEIOPS' advice on reinsurance management (CfA 12).
39. Reinsurance management includes the specification, implementation, monitoring, reporting and control of reinsurance arrangements.
40. Reinsurance management plays an important role in an undertaking and in its risk profile. Using traditional and/or financial reinsurance

(finite reinsurance), an undertaking can reduce risk, stabilise its solvency levels, use available capital more efficiently and expand underwriting capacity. Both the solvency and liquidity of an undertaking could be jeopardised in the event of deficiencies in the reinsurance arrangements, especially in non-life insurance.

41. 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 not be limited to, provisions for aggregating risk, for aggregating limits of liabilities, for aligning the interests of insurers and reinsurers, and for explicitly recognising the time value of money.

#### High level principles

42. The undertaking should develop policies and procedures that enable it to prudently manage the use of reinsurance, including both the risks transferred and the risks arising from reinsurance, namely credit risk.
43. The reinsurance management includes the risk management and internal control procedures related to reinsurance operations and should, at least, take into account the following procedures:
  - a) Monitor the implementation of the overall reinsurance management strategy;
  - b) Verify the retention limits established;
  - c) Monitor reinsurance documentation;
  - d) Monitor whether the risk is effectively transferred;
  - e) Monitor reinsurance recoverables; and
  - f) Monitor the creditworthiness of each reinsurer.
44. The reinsurance policies and procedures shall identify:
  - a) Monitoring programs;
  - b) Lines of responsibilities and controls implemented.

#### Minimum requirements

45. The reinsurance management policies and procedures shall, among other things:
  - a) Regarding the strategic reinsurance management:
    - i. Identify the overall risk tolerance limits of the undertaking;
    - ii. Identify the maximum net risk to be retained, appropriate to the established risk tolerance limits;
    - iii. Set types of reinsurance arrangements that the undertaking considers appropriate to its type of business and risk profile, with particular reference to long-tail liabilities;
    - iv. Define policies in the event that the matching of the undertaking's underwriting and its reinsurance programme

cannot be obtained at all times, e.g. counter-measures, as well as clear links to other areas affected by the change or (partial) loss of reinsurance cover in the case that reinsurance contracts cannot be renewed to accord with current terms/conditions or because of a reinsurer's default;

- v. Set limits on the amount and type of insurance that will be automatically covered by reinsurance (e.g. treaty reinsurance);
- vi. Identify the process of monitoring, reviewing and amending the reinsurance management strategy in response to changes in the risk profile of the undertaking or in the market conditions;

b) Regarding the operational reinsurance management:

- i. Identify, for all lines of business, the maximum foreseeable amount of reinsurance protection that will have to be purchased from individual reinsurers, based on the difference between the total amount of gross business the undertaking expects to be able to write and the amount of business that can actually be written on the basis of its available capital;
- ii. Identify, for all lines of business, whether there is sufficient capacity available on the reinsurance market to cover the amount of reinsurance protection required;
- iii. Set criteria for acquiring facultative reinsurance cover;
- iv. Set principles for the selection and monitoring of reinsurers with particular attention to the creditworthiness of the reinsurers, the diversification of the reinsurance cover.
- v. Provide for the maintenance of an up-to-date register of reinsurers, as approved by the administrative or management body, including the maximum level of exposure for each reinsurer. This register shall be available to the supervisory authority on request;
- vi. Set principles for the management of liquidity risk related to the time interval between the payment of insurance claims and the amounts being recovered from the reinsurer.

46. Notwithstanding the definition for the overall reinsurance management strategy, the ART (alternative risk transfer) strategy, which should be implemented and documented by senior management, shall also:

- a) Identify the rationale for using ART;
- b) Ensure that ART arrangements include genuine risk transfer before they may result in a change in the SCR;
- 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;

- f) Identify the procedures for ongoing monitoring of the arrangements with a review to be undertaken at least on an annual basis; and
- g) Demonstrate that the ART arrangements are appropriate in relation to the risks to be covered.

## **5. Market risk, including Asset-Liability Management**

### Background

1. *Market risk* means the risk of loss, or of adverse change in the financial situation, resulting from fluctuations in the level and in the volatility of market prices of assets, liabilities and financial instruments, either directly or indirectly.
2. Market risk is the risk associated with adverse changes in the value of the assets held by an undertaking, and can be split into:
  - a) Interest rate risk;
  - b) Equity risk;
  - c) Property risk;
  - d) Currency risk;
  - e) Spread risk;
  - f) Other risks (e.g. market risk concentrations and counterparty default risk).
3. Interest rate risk is the sensitivity of asset and liability values to changes in the term structure of interest rates or interest rate volatility.
4. The expected cash flows of the liabilities are, in addition to interest rate risk, affected by the life underwriting risk. This risk affects both the valuation and the expected duration of the liabilities, which has to be taken into account when the interest rate risk is evaluated.
5. Equity risk arises from the level or volatility of market price for equities. Exposure to equity risk refers to all assets and liabilities whose value is sensitive to changes in equity prices.
6. Property risk arises from the level or volatility of market prices of real estate.
7. Currency risk arises from the level or volatility of currency exchange rates.
8. Spread risk is the part of risk originating from assets that is explained by the volatility of credit spreads over the risk-free curve.
9. Asset Liability Management risk is the risk of mismatch between the liabilities and the assets covering them.

### High level principles

10. The undertaking should develop strategies, policies and procedures that enable it to prudently manage all the market risks, including asset-liability management risk.
11. The strategies, policies and procedures referred in the previous paragraph should enable the undertaking to properly identify, evaluate, mitigate, monitor and control, in particular, the risks not covered by the standard formula and the proper level of capital to hold in relation to those risks.
12. The strategies, policies and procedures referred above shall:
  - a) Identify the monitoring programs;
  - b) Identify the chain of responsibilities;
  - c) Define the process of approval, implementation, monitoring and control of investment decisions;
  - d) Define the frequency and format of internal reporting.

### Minimum Requirements

13. In order to ensure a proper risk management of the market risk the undertaking should develop an investment strategy that shall clearly identify:
  - a) The strategic allocations (the determination of the asset allocation, including ALM considerations - i.e. asset mix across the main investment categories);
  - b) The return to be targeted and the way in which insurers exercise their discretion with regard to with-profits life business;
  - c) The allocation limits by counterparty, business sector, geography, type of instrument and currency;
  - d) The use of financial derivatives as part of the general portfolio management process or of structured products that have the economic effect of derivatives and securities lending;
  - e) The admitted investments and any restrictions imposed on the investment policy;
  - f) The methodology, benchmarks and frequency of performance measurement and analysis;
  - g) The degree of sensitivity to investment risks, including matching, risk margins, and capital requirements; the results of the use of quantitative tools in previous years (e.g. stress tests and/or scenarios) shall also be reflected in the investment policy;
  - h) The extent to which the holding of some types of assets is ruled out or restricted where, for example, the sale of the asset could be difficult due to the illiquidity of the market or where independent (i.e. external) verification of pricing is not available;
  - i) Key staff involved in investment activities;

- j) The framework for reporting on asset positions;
  - k) The nature of any outsourcing and requirements for the safekeeping of assets (custodial arrangements);
  - l) The strategies on the use of voting rights owned; and
  - m) How to proceed internally when new asset classes or financial derivatives become part of the investment portfolio.
14. Concerning, in particular, derivative products, asset-backed securities and collateralised debt obligations, hedge funds or any other financial instrument with similar characteristics, the investment strategy shall clearly identify:
- a) Goals and strategies of the use of those products;
  - b) Evaluation of the strategy to use this type of products;
  - c) Principles of risk management used;
  - d) The level of leverage of the products;
  - e) The payoff structure of the investment;
  - f) Calculation of shocks;
  - g) The use of speculative management techniques, namely in the case of hedge funds;
  - h) The total amount of possible loss (Value at Risk).
15. An investment policy should be defined, based on rules and procedures that a wise, prudent and expert manager would apply in order to pursue the investment strategy, in line with the interests of the insured and to obtain an income appropriate to the incurred risk and liabilities covered. Along with the investment management policy, an asset-liability policy shall be drawn up, describing how financial and insurance risks will be managed in an asset-liability framework both short and long term.
16. The asset liability management strategy shall clearly identify:
- a) The structure of the asset-liability approach, including the time horizon;
  - b) The underlying modelled portfolio of assets and liabilities and their developments;
  - c) The setting up of target functions and/or cause-effects relations;
  - d) The stress tests to be performed, including the identification of parameters;
  - e) The setting up of priority lists regarding desired characteristic key ratios;
  - f) A validation of parameters and hypotheses by confrontation with earlier observations (backtesting);
  - g) The connection between the asset-liability management policy and the investment policy and their interaction;
  - h) All areas where the undertaking is committed to pay bonuses to the

policyholders.

17. The undertaking should especially take into account the interrelation with other types of risks, such as liquidity risk, insurance specific risk and risks posed by options embedded in new and in-force policies; in this regard:
  - a) It should structure its assets so that it has sufficient cash and diversified marketable securities to meet its obligations as they fall due and should have a plan to deal with unexpected cash outflows;
  - b) It should identify ways to mitigate the impact of the embedded options, while ensuring that policyholders are treated fairly, and assess the possible effects these can have throughout the life of the insurance policies.

## 6. Credit risk

### Background

1. *Credit risk* means the risk of loss, or of adverse change in the financial situation, resulting 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.
2. The credit risk exposure arises from financial transactions of the undertaking with asset issuers, debtors, intermediaries, policyholders or reinsurers.
3. The credit risk exposure plays an important role in an undertaking's financial viability and in its risk profile.
4. Credit risk management includes the definition, implementation, monitoring, reporting and control of the credit exposure and should be adequate to the nature and scale of the undertaking.

### High level principles

5. The undertaking should develop policies and procedures that enable it to prudently manage credit risk in accordance with the strategy.
6. These policies and procedures should:
  - a) Identify the level, quality and diversification defined as acceptable according to the undertaking's risk profile;
  - b) Identify internal limits defined for the credit exposure to:
    - i. One counterparty or a group of counterparties;
    - ii. Assets and transactions intra-group;
    - iii. Individual assets and sectors;
    - iv. Geographic regions;
  - c) Identify mitigation techniques used;
  - d) Explain the valuations methods used to assess the risk, and

- evaluate the mitigation techniques used;
- e) Identify the monitoring and review programs, lines of responsibilities and controls implemented.

#### Minimum requirements

- 7. The policies and procedures referred above should cover at least the following areas:
  - a) Valuation of the credit risk exposure;
  - b) Levels of concentration;
  - c) Monitoring process.
- 8. The policies must at least identify the methodology used to assess the credit risk.
- 9. The methodology used should:
  - a) Allow the identification of the types and sources of credit risk to which the undertaking is exposed;
  - b) Be adequate to the nature of the transactions, distinguishing between transactions where the credit risk is taken in order to achieve a return and transactions where credit exposure arises as a consequence;
  - c) Take into account direct and indirect exposures, including synthetic exposures arising from derivatives.
- 10. The evaluation of the adequacy of the exposure and diversification levels should consider:
  - a) Different types of exposures to one single counterparty;
  - b) Relations between counterparties if the default of one counterparty has an influence on the probability of default of another;
  - c) Any environmental or market situations that can influence the credit quality of the counterparties.
- 11. In the identification of internal limits the undertaking should take into consideration:
  - a) The goals, maturity and characteristics of the transaction;
  - b) Type of credit risk involved;
  - c) An evaluation and monitoring on an ongoing basis of the creditworthiness of the counterparties;
  - d) The size of the exposure;
  - e) The collateral, if any.

## 7. Concentration risk

### Background

1. *Concentration risk* means all risk exposures with a loss potential which is large enough to threaten the solvency or the financial position of undertakings; such exposures may be caused by credit risk, market risk, underwriting risk, liquidity risk, other risks, or a combination or interaction of those risks.
2. A risk concentration is an exposure with the potential to produce significant losses for the entity. Concentration risk can be defined as the risk of loss arising from a concentrated position or exposure.
3. Concentration risk can arise in both the assets and liabilities sides of the undertaking, as well as in off-balance sheet items.
4. Concentration risk can arise from a series of sources, including:
  - a) Geographical areas;
  - b) Counterparties, either groups or entities;
  - c) Economic sectors;
  - d) Types of products (both on the assets and liabilities sides);
  - e) Providers of services;
  - f) Reinsurance;
  - g) Cumulative exposures in the insurance contracts (both explicit and embedded);
  - h) Catastrophes.

### High level principles

5. The undertaking shall have in place clear policies and procedures to prudently manage and control concentration risk. These policies and procedures should be embedded in its risk management systems, in line with the global strategy.
6. As part of this approach to concentration risk, the undertaking should have a policy on underwriting, on investments, and on reinsurance, that deals with concentrations, including correlated concentrations.
7. Such policies and procedures should be approved by the administrative or management body, and applied by the senior management of the undertaking, and should be consistent with its policy on solvency.

### Minimum requirements

8. The undertaking should have in place the appropriate processes to identify, measure and manage concentration risk, taking into account the following aspects:
  - a) It should identify its exposures to a single counterparty, either entity or group of entities, a type of risk within a geographic area, a single economic sector, a single reinsurer or provider of services;
  - b) Once these exposures have been identified, they should be

measured taking into account potential correlations in order to adequately determine the possible impact these risks may have on the undertaking's solvency position. Stress tests and scenario analysis should be carried out to determine the potential impact of concentrations;

- c) After having identified and measured risks derived from concentration, the undertaking should manage them in line with the strategies and plans established by the administrative or management body and senior management, deciding on accepting them, transferring and/or mitigating them. Mitigation techniques should be analysed so that they do not generate other types of concentrations. Diversification should play a key role in terms of managing concentration risk.
9. In the context of its total risk profile, as well as its risk policies, the undertaking should establish internal thresholds or limits, consistent with its policy on capital and risk. The procedures to operate above these thresholds, as well as the conditions to do so, should be established and documented.
10. The undertaking should monitor, on an ongoing basis, its concentrations and the potential risks within, both present and future. Such monitoring procedures should be embedded in its risk management system. The undertaking should check the consistency of the results with the content of the policies and procedures implemented. Special monitoring should be carried out concerning positions authorised in excess of the limits or thresholds previously set.
11. Whenever deficiencies are detected, the undertaking should take appropriate steps to respond to this situation. Such measures may include, e.g. adjustments to limits or thresholds, changes in the investment or underwriting policies to fit in with the policies implemented, transfers of risks, allocation of extra capital, and contingency plans.
12. When performing its own risk and solvency assessment, the undertaking should analyse the amount of capital needed to cover concentration risks in line with its own policies.

## **8. Liquidity risk**

### Background

1. *Liquidity risk* means the risk that undertakings are unable to realise investments and other assets in order to settle their financial obligations when they fall due.
2. Liquidity is the availability of funds, or certainty that funds will be available, 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. The risk of illiquidity increases if principal and interest cash flows

related to assets, liabilities and off-balance sheet items are mismatched.

3. The liquidity profile of an undertaking is a function of both its assets and liabilities.
4. The uncertainty of the timing and amount of the cash outflows related to the insurance activity may affect the capacity of the undertaking to comply with its responsibilities or may force it to incur an additional cost in obtaining liquidity by selling assets.

#### High level principles

5. The undertaking should develop policies and procedures that enable it to prudently manage the liquidity risk.
6. The policies and procedures should:
  - a) Have regard to the investment strategy, the global underwriting strategy and the claims management;
  - b) Clearly differentiate the operational (short term) from the strategic (medium and long term) liquidity management.

#### Minimum requirements

7. It is the undertaking's responsibility to have sound liquidity management practices which cover both operational and strategic considerations. Operational liquidity, or cash management, covers the day-to-day cash requirements under normally expected or likely business conditions. Strategic liquidity considers liquidity needs on a longer-term basis and recognises the possibility of various unexpected and potentially adverse business conditions. Strategic liquidity is a key consideration of asset-liability management because of its potential effect on the ultimate viability of the undertaking.
8. The undertaking should be aware of the ways in which its activities can affect its liquidity risk profile, and how outside influences may affect its liquidity position. It should consider not only its current liquidity risk, but how existing activities may affect its liquidity risk profile in the future; it should also consider the implications of new products or business lines.
9. The liquidity management requires a planning that foresees the future liquidity needs having regard to not only the insurance activity but also future economic, market, politics or regulatory trends.
10. The policies and procedures should at least include:
  - a) Identification of the liquidity risk exposure;
  - b) Regarding the strategic liquidity management:
    - i. Predictions of economic, market, political, regulatory or other changes that might have an impact on the policyholder behaviour;
    - ii. The level of mismatch between the expected cash flows from the assets and liabilities under normal market conditions and under stressed or extreme situations, namely in case of catastrophe;

- iii. The level of mismatch between the expected cash flows from direct insurance and reinsurance under normal market conditions and under stressed or extreme situations, namely in case of catastrophe;
  - iv. The total needs of liquidity in a medium and long term;
  - v. The financial situation and the credit quality of the undertaking in the medium and long term;
  - vi. Description of the strategy to mitigate the liquidity risk;
  - vii. Description of the liquidity contingency plan, including any stress tests.
- c) Regarding the operational liquidity management:
- i. The level of mismatch between the cash inflows and the cash outflows of both assets and liabilities;
  - ii. The level of mismatch of the expected cash flows of direct insurance and reinsurance;
  - iii. The total liquidity needs in the short term (next 30 days), including probable liquidity flaws;
  - iv. The level of liquid assets, including a quantification of eventual costs or financial losses arising from an unpredicted sale;
  - v. Identification of other financing tools, including reinsurance, debt capacity, bank lines of credit or intra-group financing;
  - vi. Predictions 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.
- d) Regarding the internal control system:
- i. Description of the processes in place to monitor and control the liquidity needs (including a list of liquidity key ratios);
  - ii. Definition of an alert system that should be activated when the limits are reached;
  - iii. The procedures to implement the contingency plan;
  - iv. The structure and the periodicity of the internal report.

## 9. Operational risk

### Background

1. *Operational risk* means the risk of loss arising from inadequate or failed internal processes, or from personnel and systems, or from external events, including legal risks. For the purposes of this Issues Paper, operational risk would exclude reputational risks and risks arising from strategic decisions.
2. Amongst the several operational risks that the undertaking can be exposed to, it should concentrate on, but not limit itself to, the risks

related to internal and external fraud, business process and practices, outsourcing arrangements, severe business continuity disruptions and money laundering practices.

#### High level principles

3. 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 and periodically review the undertaking's operational risk management framework. This framework should provide a firm-wide definition of operational risk and lay down the principles of how operational risk should be identified, assessed, mitigated, monitored, and controlled.
4. Administrative or management body should be responsible for implementing the operational risk management framework approved. The framework should be consistently implemented throughout the whole organisation, and all levels of staff should understand their responsibilities with respect to operational risk management.
5. The administrative or management body should ensure that insurance activities are conducted by qualified staff with the necessary experience, technical capabilities and access to resources. Management should ensure that the undertaking's operational risk management policy has been communicated to staff at all levels in units that incur material operational risks.
6. The undertaking should identify and assess the operational risk inherent in all material products, activities, processes and systems. The undertaking should also ensure that before new products, activities, processes and systems are introduced or undertaken, the operational risk inherent in them is subject to adequate assessment procedures.

#### Minimum requirements

7. An effective risk identification should consider both internal factors (such as the undertaking's structure, the nature of its activities, the quality of its human resources, organisational changes and employee turnover) and external factors (such as changes in the industry and technological advances) that could adversely affect the achievement of the undertaking's objectives and its operational risk profile. In addition to identifying the most potentially adverse risks, the undertaking should assess its vulnerability to these risks.
8. The undertaking should have policies, processes and procedures to manage material operational risks. It should periodically review its risk limitation and control strategies and should adjust its operational risk profile accordingly using appropriate strategies, in light of its overall risk appetite and profile. For this purpose, the undertaking should consider the following aspects:
  - a) It should have documented IT strategies and procedures, as well as checks on systems security, data integrity, new systems testing, and backup facilities. The undertaking should also have a policy for data access, distribution and communication security; compliance

with that policy should be monitored regularly;

- b) It should have policies and procedures for developing and maintaining outsourcing partnerships, including a comprehensive process for identifying potential outsourcing service providers, implementing contingency plans and exit strategies and monitoring outsourcing arrangements;
  - c) All outsourcing arrangements should be subject to a formal and comprehensive written agreement covering at least the responsibilities of both parties and a qualitative description of the services. The insurance undertaking should establish supervisory authority access to relevant data held by the outsourcing service provider and the right for the supervisory authority to conduct onsite inspections at an outsourcing service provider's premises should be incorporated into the outsourcing agreement;
  - d) It should have in place tested and updated contingency and business continuity plans to ensure its ability to operate on an ongoing basis and limit losses in the event of severe business disruption;
  - e) It should implement specific measures and procedures, including human resources hiring policies and staff training programmes, in order to minimize risk related to human resources (fraud, negligence, etc.);
  - f) It should have training programs for all staff, including administrative or management body, aiming to increase risk awareness. In addition to general operational risk trainings, special training should be available for staff exposed to external fraud (e.g. claims department);
  - g) It should incorporate, within its risk management and internal control systems, adequate procedures and mechanisms that aim at combating fraud and prevention of money laundering;
  - h) Where legally possible, the undertaking should participate in relevant databases where claims suspected to be fraudulent should be reported.
9. The undertaking should ensure that relationships with all customers and partners are approved by persons with the proper level of authority and that appropriate legal documentation is in place before any business commences. Whenever standardised documents are not used, contracts should be reviewed by legal counsel for appropriateness, enforceability, legality and, to the extent possible, uniformity within the undertaking. Similarly, legal counsel should review non-standard clauses that are introduced in standardised documents and addenda.
10. The undertaking should sell and advise customers on products that are clearly defined, well documented and part of the undertaking business. All advisory and selling activities should focus on the customers' interests. The undertaking should ensure that customers understand the advice, the product or service and the related risks.

11. The undertaking should implement a process to regularly monitor operational risk profiles and material exposures to losses including collecting data on operational risk losses.
12. There should be regular reporting of pertinent information that supports the proactive management of operational risk to the administrative or management body. The operational risk reports should contain internal financial, operational and compliance data, as well as external market information about events and conditions that are relevant to decision making. Reports should be distributed to appropriate levels of management and to areas of the undertaking on which areas of concern may have an impact. Reports should fully reflect any identified problem areas and should motivate timely corrective action on outstanding issues.
13. The frequency and content of operational risk reporting should be formally approved by the administrative or management body. The administrative or management body should ensure the ongoing appropriateness of the reporting framework. The frequency, content and format of reporting should depend on the recipient and on how the information will be used.

## **10. Reputational risk**

### Background

1. Reputational risk is defined as the risk of potential damage 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 regulatory authorities. To that extent it may be regarded as less of a separate risk, than one consequent on the overall conduct of an undertaking.

### High level principles

2. The administrative or management body of the undertakings should be aware of potential reputational risks it is exposed to and the correlation with all other material risks.
3. The undertaking should pay great attention to understanding and recognising key values affecting the reputation, expectations of the stakeholders and sensitivity of the market where they operate to loss of reputation or confidence.

### Minimum requirements

4. The undertaking should implement a reputational risk management program including activities aiming at increasing risk awareness within the organisation and a process of regular monitoring and analysis of the potential reputation risk it may face.
5. As a part of reputational risk management program, the undertaking should have adequate customers' complaints handling procedures with periodic reports to senior management on the nature, scale and frequency of complaints.

6. The undertaking should have a communications and public relations function that is involved in external communication concerning reputation-sensitive topics.
7. The undertaking should have detailed emergency scenarios in place for responding to any reputation loss. These emergency scenarios should be subject to regular review.
8. The undertaking should have training programs, including media training for senior management, administrative or management body to act/react in reputational risk incidents.

## **11. Correlation effects**

1. The administrative or management body should be aware of the correlations between the risks to which the undertaking is exposed.
2. The undertaking should develop policies and procedures that enable it to prudently evaluate the correlations between risks.
3. The policies and procedures should:
  - a) Have regard to the correlations matrix established in the Solvency Capital Requirement standard formula;
  - b) Have regard to specificities of the undertaking that may justify the use of a different correlations matrix.
4. This issue will be developed in detail under the Own Risk and Solvency Assessment requirements.