INTERNAL CONTROL FOR INSURANCE UNDERTAKINGS

COMMITTEE OF EUROPEAN INSURANCE AND OCCUPATIONAL PENSIONS SUPERVISORS
(CEIOPS)

December 2003

Madrid Working Group

Relationship of participants:

Chairman: Carlos Montalvo.

CEIOPS Secretariat: Philippe Vecchierini.

Austria: Teresa Bum; Gerlinde Taurer.

Belgium: Dirk DePaepe; Filip Leen; Vivianne Van Herzele.

Finland: Teija Korpiaho.

France: Silvain Merlus; Romain Passerot; Olivier Pequeux.

Germany: Jochen Wolf.

Iceland: Runar Gudmundsson.

Ireland: Siobhan O'Leary.

Italy: Elena Bellizzi.

Liechtenstein: Werner Furrer.

Luxemburg: Annick Felten.

The Netherlands: Jaap Turkesteen; Jan Peter Van der Does.

Norway: Morten Thorbjornsen; Ole-Jorgen Karlsen.

Portugal: Ana Cristina Santos.

Spain: Javier Bernaldo de Quirós; Miriam Blázquez; Lorenzo Esteban;
Fernando Laguna; Pablo Muelas; María Nuche; Dámaso Sanz.

United Kingdom: Simon Ashby; William Mc Donnell; Anna-Karin Saxena; Colin Tattersall.

European Commission: Pauline de Chatillon; Vesa Ronkainen; Henri-Olivier Fliche.

TABLE OF CONTENTS

1.A. EXECUTIVE SUMMARY

1.B. INTERNAL CONTROL PRINCIPLES

2. INTRODUCTION

a. Background

b. Objectives

c. Need for Internal Controls. Importance

d. Limitations

e. Legislation relating to jurisdictions

f. Working method

3. DEFINITION

a. Internal Control definition

b. Related concepts
   i. Corporate Governance definition
   ii. Internal Audit definition
   iii. Enterprise Risk Management definition

4. PRINCIPLES AND RECOMMENDATIONS

a. Control Culture
   i. Principle
   ii. Recommendations and Comments

b. Risk Assessment
   i. Principle
   ii. Recommendations and Comments

c. Control Activities and Segregation of Duties
   i. Principle
   ii. Recommendations and Comments

d. Information & Communication
    i. Principle
    ii. Recommendations and Comments

e. Information & Communication Technologies
    i. Principle
    ii. Recommendations and Comments

f. Monitoring
    i. Principle
    ii. Recommendations and Comments

5. SMALL ENTITIES

6. OUTSOURCING

7. REFERENCES

1. A EXECUTIVE SUMMARY

1.1 Since the last decade, international Insurance fora have intensified their efforts to develop a complete set of generally accepted and applicable principles and standards concerning insurance activities and their supervision. Such developments allow insurance undertakings to deal with the complexity and importance of private insurance, which is increasing both from a social and a financial perspective.

1.2 As a result, Internal Control has become a key concern, as insurance activities become ever riskier and more complex.

1.3 Aware of the importance of Internal Control, the Conference of European Insurance Supervisors agreed during its 118th Session, held in Bruges, to create a specialized Working Group with the task of producing a Framework on Internal Control for the Insurance sector.

1.4 The result of the work carried out by the group is this document, issued with the intention of creating an appropriate framework geared to both insurance undertakings and supervisory authorities. On the one hand, insurance undertakings have a common reference to be used as a solid basis for more detailed developments, and on the other hand supervisors may apply a common general approach when assessing and monitoring Internal Control systems implemented by insurance entities. As far as this document contributes to an effective application of adequate Internal Control procedures, the insurance industry will benefit from higher security standards, and both policyholders and shareholders will see their level of protection improved. Thus, the implementation of Internal Control procedures should not be seen as an additional burden for insurers, but as a direct and effective manner of adding value to their business activity, the financial sector and the Economy as a whole.

1.5 In this context, the main goals of this working group (WG) were:

1. The establishment of the main principles for insurance undertakings and supervisors when implementing and/or evaluating an internal control system.
2. The development and follow-up of the recommendations issued by the Brouwer Reports on Financial Stability (EFC/ECFIN/240/00, April 2000) and on Financial Crisis Management (EFC/ECFIN/251/01, April 2001).
3. The promotion of the knowledge of Internal Control among the Insurance sector.
4. Guidance on effective application of adequate Internal Control principles.

1.6 In view of the fact that this subject has already been, for the past last years, taken into consideration in other financing sectors, namely banking and investment services, and that a convergence approach is naturally expected in order to limit the risk of regulatory arbitrage between sectors, the papers produced in those frameworks were considered by the WG when producing this document on Internal Control applicable to insurance undertakings. Nevertheless, this document offers new ideas to the existing documents, both illustrating with insurance specific references the Internal Control principles applied cross-sectors, and

introducing differentiated topics rising from the specificities of insurance activities that were considered to deserve a differentiation.

1.7 The first step of the WG work was reaching a common definition of Internal Control. The WG agreed the following definition:

¨ Internal Control is a continuous set of processes carried out by an entity's board of directors, management and all personnel, designed to provide reasonable assurance of:

- *Effectiveness and efficiency of operations.*
- *Reliability of financial and non-financial information.*
- *An adequate control of risks.*
- *A prudent approach to business.*
- *Compliance with laws and regulations, and internal policies and procedures.*

Internal control should strengthen the internal operating environment of the company, thereby increasing its capability to deal with external (and internal) events and uncover possible flaws and deficiencies in processes and structures¨.

1.8 The common definition adopted includes the different objectives of Internal Controls. A delimitation process with Corporate Governance and Risk Management has been carried out, to set the differences as well as the existing links among them. Internal audit, although a part of internal control, has also deserved a detailed consideration.

- 1.9 The principles on Internal Control developed on this document should be of general application to all insurance undertakings, and should be used by the supervisory authorities when assessing the adequacy of the systems implemented.

1.10 A set of recommendations are included developing each of the principles, together with some examples.

1.11 The introduction of a common set of principles and recommendations at an European Economic Area (EEA) level, should increase convergence of supervisory practices, in line with the Brouwer recommendations on financial stability and financial crisis management. It should also expand on the London Working Group's report on Prudential Supervision of Insurance Undertakings analysis in order to provide a more in depth study of current and potential internal control tools available to supervisors.

1.12 The need for a specific analysis on small undertakings is a direct consequence of the fact that certain types of structures/demands just cannot be extended to every entity. Nevertheless, regardless of the size, every undertaking should have adequate administrative organisation and controls.

1.13 Practice demonstrates the importance of setting appropriate internal controls when outsourcing key functions. The working group, aware of this fact, has also included an individual chapter to deal with the subject.

1.14 In considering Internal Control systems, insurance undertakings have to be compliant with applicable national and EU legislation. Special attention should be paid to those situations

where the insurance undertaking is part, for example, of an Insurance Group (according to Directive 98/78, October the 27th, 1998) and/or a Financial Conglomerate (Directive 2002/87, December the 16th, 2002).

1.15 Finally, and given the fact that insurance activity evolves over time, Internal Control systems and supervision need to evolve too. Therefore, continuous revision and adaptation is a core idea, applicable both as an Internal Control principle and as a general approach whenever dealing with Internal Control. In the light of future steps, it is likely that this document will need continuous updating and development to encompass the market and social expectations.

1.B INTERNAL CONTROL PRINCIPLES

The following principles will be applicable to insurance undertakings' Internal Control:

1. CONTROL CULTURE

The board of directors 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. Management is responsible for the implementation of the internal control Culture and principles. All personnel need to understand their role in the internal control process and be fully engaged in the process.

2. RISK ASSESSMENT

In establishing and maintaining an effective system of internal control an insurance undertaking should regularly assess both the internal and external risks that it faces.

Assessment should include the identification and analysis (using quantitative and/or qualitative tools) of all the significant risks that an insurance company is exposed to, and act accordingly.

3. CONTROL ACTIVITIES AND SEGREGATION OF DUTIES

An adequate Internal Control system requires the implementation of effective and efficient Control Activities at all levels of the entity. They should be implemented by the management in line with the goals and strategies set up by the board of directors, and should involve all personnel. As an integrated part of daily business, these activities should be reviewed and recorded on an on-going basis.
An efficient Internal Control system demands an appropriate segregation of duties and clear lines of responsibilities, both at individual level and between functions.

4. INFORMATION & COMMUNICATION

Insurance Undertakings should have reliable information at all levels within their organisation, in order to define, achieve and review the objectives set by the board of directors, through effective decision making processes.
Internal Control systems should ensure the effectiveness of communication procedures. Such communication should be internal as well as external, and may include both formal and informal paths.

5. INFORMATION AND COMMUNICATION TECHNOLOGIES

Insurance Undertakings should implement Information and Communication Technology (ICT) systems appropriate to the activities they carry out, their strategies and needs. Security controls for the risks inherent in ICT should be established to effectively enhance management of those risks, allowing the insurance company to recognize both the potential benefits and the associated risks of such systems.

6. MONITORING

Insurance undertakings should implement appropriate systems to monitor their Internal Control's efficiency and effectiveness. Monitoring should be carried out on an ongoing basis, complemented with separate evaluations.
As an integral part of an internal control system, and in keeping with the diversity and complexity of the insurance undertaking's activity, there should be an effective and comprehensive internal audit carried out by operationally independent, appropriately trained and competent staff.

The internal audit function should be conducted through a professional audit program designed to provide reasonable assurance that Internal Control objectives are met. An effective internal audit function should also comprise a follow-up process on audit findings in order to assure that they are being adequately dealt with.

2. INTRODUCTION

2.1 Background

2.1.1 Undertakings have always had management, operational or decision making systems based upon diverse criteria, ranging from the unilateral will of a single owner to consensus of a board. Therefore, decisions and criteria have always had a cause and consequences, having in mind the compliance with the established objectives and the business plan, compelling adequate Internal Control systems to be a demand of the markets and the business itself.

2.1.2 The Insurance sector, along with the rest of the Financial sector, has faced significant changes in recent years, and such changes have brought new products and services, new tools, goals and objectives. Internal Control systems of the undertakings have to be adapted to better cope with this evolving scenario.
In addition, we are in an era of globalisation, with closer links among the different sectors, constant mergers and acquisition processes with an international scope. Such a situation needs to be taken into account when drafting a set of Internal Control principles, as we cannot leave aside what is being done in other markets or sectors. Financial Conglomerates can be seen as an example of the increasing importance of the relationship between the financial sectors.

2.1.3 Given the importance of Internal Controls in insurance undertakings, the Spanish supervisory authority prepared and presented to the Conference of Insurance Supervisors a Questionnaire on Internal Control and submitted it to all the delegations. The findings of the questionnaire on Internal Control showed the existence of differences in the treatment and development of Internal Control issues. It was agreed by member states that it would be appropriate to set up a specific Working Group on the subject, with the intention of developing at a supervisory level a framework of IC principles and recommendations for insurance undertakings and supervisory authorities.

2.1.4 Supervisors from most of the member states, including Austria, Belgium, Finland, France, Germany, Iceland, Ireland, Italy, Liechtenstein, Luxemburg, Netherlands, Norway, Portugal, Spain and the UK participated in this Working Group. Comments and contributions have also been received from Denmark, Greece and Sweden. In addition to member states, representatives from the Secretariat of the Conference, as well as the European Commission have attended the meetings.

2.2 Objectives

2.2.1 The goals established by this working group were:

2.2.1.1 To draw up a series of principles for insurance undertakings and supervisory authorities when assessing the undertaking's internal Control systems, allowing a consistent approach alongside the EEA.

2.2.1.2 To develop and follow-up on the recommendations issued by the Brouwer Reports on Financial Stability (EFC/ECFIN/240/00, April 2000) and on Financial Crisis Management (EFC/ECFIN/251/01, April 2001).

- With respect to the increased convergence of supervisory practices referred to in the Economic and Financial Committee (EFC) report on Financial Stability, the Working Group has: drafted a common set of principles on Internal Control for all insurance undertakings at a European level; shared concerns and experiences, and; shared supervisory toolkits, all with the intention of increasing convergence.

- Using the EFC report on Financial Crisis Management as a starting point, this document focuses on the following EFC recommendations: Internal Control principles deal with management information systems, which must be reliable, allowing for completeness, accuracy and transparency. It also requires internal and external risk assessment, including stress testing as a core tool on such assessment and preventive control of risks.

2.2.1.3 To promote awareness of Internal Control in the Insurance sector.

- Internal Control systems should help entities to improve performance both in favourable and unfavourable situations and conditions; execute the business plan; exploit business opportunities; mitigate adverse effects of both internal and external effects, creating an added value for the company.

- This document also aims to give insurance undertakings new guidelines for developing and improving their Internal Control systems. It therefore includes a series of recommendations for each of the different principles for Internal Control. The inclusion of such recommendations is fully compatible with the Working Group's intention not to impose any one method of running the insurance undertakings.

2.2.2 The content of this paper intends, through the effective application of the principles and recommendations included in it, to contribute in the creation of a playing field where all the stakeholders benefit from improved Internal Control systems.

2.3 Need for Internal Controls: importance

2.3.1 From the insurance sector point of view, Internal Control should be seen as an opportunity for the entities to improve their performance, both from an internal and an external perspective:

- Internally, good Internal Control systems lead to improved recognition, assumption and prevention of risks, which is of prime importance in a sector with the particularities of Insurance, which is about finding business opportunities in risks. Also competitiveness will be fostered by appropriate controls not only in the short but also in the long term. Finally, it will help reduce the impact of unexpected events, or even to avoid them altogether, for example by means of good early warnings or scenario testing.

- Externally, appropriate Internal Control systems will have a positive impact on policyholders (meaning better results for the undertaking), supervisors (essential in the Solvency II framework, as if supervisors are not satisfied with internal control of the undertaking is likely the insurer will be obliged to increase its solvency margin) and shareholders (meaning higher confidence and thus higher share value of the entity),

2.3.2 From a supervisory point of view, Internal Control is becoming increasingly important. The London Working Group's report on Prudential Supervision of Insurance Undertakings has highlighted the fact that many of the problems of the real cases analysed were either directly caused by inadequate Internal Controls, or underlying internal causes led to inadequate controls which in turn resulted in inappropriate risk decisions. Solvency II requires supervisory authorities to focus more on certain qualitative aspects, including Internal Control of the insurance entities.

2.4 Limitations

2.4.1 The main limitation concerning Internal Control is that, no matter how good a system is, it will only provide ¨reasonable assurance¨, not complete certainty that the insurance undertaking will withstand undesired events happening.

2.4.2 Together with this general assumption, the following aspects have to be taken into account in considering possible limitations to Internal Control systems:

- Internal Control is carried out by people, and will therefore be affected by human error. Good training programs, as well as an ethical component within the entity and its way of doing business can help mitigate this situation.
- Insurance companies are exposed to some risks that can be controlled as well as to some which are difficult to foresee. They are exposed not only to internal risks, but also to external ones. These risks may be compounded by the length of some insurance contracts, which may run for many years.
- A rigorous cost benefit analysis will help identify the most appropriate manner of implementing internal controls.

2.4.3 Internal Control will be implemented differently in different undertakings. This is of particular importance whenever we are focusing on a small entities approach.

2.5 Legislation relating to jurisdictions

When considering the role of the board of directors and the management in the Internal Control process, the working group has paid attention to the fact that there are different legislative and regulatory systems in EU countries and several models of corporate structure. Taking into account these differences, the terms "board of directors" and "management" used in this paper are functional labels denoting the decision making functions undertaken, not references to the formal legal structure of the organization. "board of directors" delineates the governing body that oversees the activities of and sets policy for the insurance company as a whole. "Management" means the senior personnel who run the company on a day to day basis. In any case, the duties must be clearly assigned to either the board of directors or the management, and must be effectively exercised in line with the underlying concept of the role of these two institutions.

2.6 Working Methods

2.6.1 The Working Group decided to focus on Internal Control, rather than expanding on other related issues already tackled in other documents and fora, for example Risk Management. Therefore this document does not include any classification or list of risks.

2.6.2 At a first stage, it was carried out a literature review of Internal Control, both in and outside Europe, across the financial and other sectors. Such an overview was necessary to help avoid undesired divergences from the existing approaches. It included a series of presentations on general Internal Control issues, mainly as a preparatory basis for the upcoming work. It also included the agreement on a common definition for internal Control as the necessary starting point for a common understanding of the subject.

2.6.3 In the second stage it aimed tackling insurance specific concerns, so that the document would deal with real insurance industry concerns and specialties allowing a better approach to Internal Control for insurance undertakings. To do so, the Group invited different undertakings and organizations (MAPFRE, AVIVA, ICEA) to explain how they were implementing their Internal Control systems and what their concerns were.

2.6.4 At the same time, the experts concentrated on Internal Control from a supervisory point of view, sharing knowledge, concerns and expertise to bottom out the different issues raised during the discussions.

2.6.5 The content of the document has been revised to adapt it to the upcoming situation, in particular to align it with phase II of the Solvency II project, as stated in the Commission's document MARKT/2539/03, recently issued. For this purpose, the outcomes of this document on Internal Control have been structured in different levels, in order to accommodate as far as possible future developments of Solvency II. Hence the document contains a first level of general principles on Internal Control applicable to insurance undertakings, followed by a second, more detailed level, including recommendations and a series of examples.

2.6.6 The Working Group split the work in six areas dealing with the different principles for Internal Control, putting together their findings for detailed discussion.

2.6.7 The Group, aware of the unique characteristics of the Insurance sector, also decided to pay particular attention to the situation of small entities, dedicating a chapter to this subject.

2.6.8 Building on work carried out in other fora, specifically the London Working Group, the Group decided to devote one chapter to the internal control of outsourcing.

2.6.9 The result of the work carried out by the group is this document, issued with the intention of creating an appropriate framework geared to both insurance undertakings and supervisory authorities.

3. DEFINITION

3.1 INTERNAL CONTROL

3.1.1 The Working Group began by setting out a common definition for Internal Control. Having considered the variety of existing definitions both at a legislative level and at an academic one, the Group decided that the concept should include a set of elements, such as: the idea of an interrelated series of processes as a whole; the responsibility and accountability of the board and management; the idea of strengthening the undertaking's structures providing tangible benefits for the company, as well as Internal Control's main objectives.

3.1.2 In this context, the Working Group has agreed on the following definition of Internal Control (IC):

¨Internal Control is a continuous set of processes carried out by an entity's board of directors, management and all personnel, designed to provide reasonable assurance of:

- *Effectiveness and efficiency of operations.*
- *Reliability of financial and non-financial information.*
- *An adequate control of risks.*
- *A prudent approach to business.*
- *Compliance with laws and regulations, and internal policies and procedures.*

Internal control should strengthen the internal operating environment of the company, thereby increasing its capability to deal with external (and internal) events and uncover possible flaws and deficiencies in processes and structures¨.

3.1.3 The following ideas can be extrapolated from the given definition:

- Set of processes: interrelated actions and decisions within the undertaking.
- Carried out by the board, management and all personnel: everyone in the undertaking will have an Internal Control responsibility appropriate to their role in the undertaking, and the board and management will be responsible for the establishment, maintenance and improvement of the Internal Control systems of the entity. In addition, Internal Control affects all personnel's work, decisions or assumptions, in their daily work and in the long term as well.
- Reasonable assurance: thus accepting the existence of a certain degree of uncertainty that cannot be completely controlled or absorbed by the undertaking. Accepting the idea that Internal Control systems have to be linked with the cost of carrying out control procedures, yet they have to guarantee a ¨reasonable¨ degree of confidence according to the nature and extent of risks taken on by the insurance undertaking.
- Internal Control systems are intended to help achieving certain goals & objectives, including the following:

    - Operational objective (effectiveness and efficiency of operations).
    - Information objective (reliability of financial and non-financial information).
    - Control objective (an adequate control of risks).
    - Management objective (a prudent approach to business).

- Compliance objective (compliance with laws and regulations, and internal policies and procedures).

3.2 RELATED CONCEPTS

3.2.1 Not only is there a variety of Internal Control definitions, but there are also some issues that are particularly closely linked to Internal Control, these are Internal Audit, Corporate Governance and Enterprise Risk Management. The boundaries are not always clearly established, however, these elements have their own identity.

3.2.2 These are the definitions given in other fora to the above elements:

3.2.2.1 Corporate Governance

Defined by the Organisation for Economic Co-Operation and Development (OECD) as a *¨set of relationships between a company's management, its board, its shareholders and other stakeholders. Corporate governance also provides the structure through which the objectives of the company are set, and the means of attaining those objectives and monitoring performance are determined. Good Corporate governance should provide proper incentives for the board and management to pursue objectives that are in the interests of the company and shareholders and should facilitate effective monitoring, thereby encouraging firms to use resources more efficiently¨.*

Taking into account that the board and management are responsible for establishing and maintaining an appropriate system of Internal Controls, Internal Control will be affected by the way the undertaking is managed, and therefore by Corporate governance. There is a link between Internal Control and the way an entity is managed, whether in a positive or a negative way, thus Internal Control should be seen as a core part of Corporate governance. In its case study analysis, the London Working Group found that poor management was a key underlying factor in the failure or near failure of many European insurance companies.

3.2.2.2 Internal Audit

The Institute of Internal Auditors defines Internal auditing as *¨an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control, and governance processes¨.*

The Internal Audit definition provides a clear idea of the links between it and Internal Control. It designates Internal Audit an essential assessment function as well as being central to increasing the effectiveness of the IC processes. While internal control is about helping a firm to meet its objectives, internal audit is about ensuring that its risk management and internal control systems are working properly. Given its importance, it is analysed in the Principles chapter.

3.2.2.3 Enterprise risk management

The Committee of Sponsoring Organizations on the Treadway Commission's (COSO) draft framework on Enterprise risk management defines it as *¨a process, effected by the entity's board*

of directors, management and other personnel, applied in strategy setting and across the enterprise, designed to identify potential events that may affect the entity, and manage risks to be within its risk appetite to provide reasonable assurance regarding the achievement of entity objectives¨.

Risk management is about understanding the nature (i.e. causes, effects, likelihood) and significance of the risks faced by a firm. It is also about deciding on acceptable levels for these risks and designing cost-effective control and or resilience strategies (i.e. strategies to help manage the impact of risk on the firm). The aim of the last stage is to ensure that the firm's risks are kept at an acceptable level.

Internal control is about understanding and controlling risk, as well as acting as a monitoring function. The primary purpose of internal control is to continuously evaluate whether a firm is meeting its objectives and to ensure that the board, managers and employees are all working to ensure the success of these strategies while keeping the level of risk at an acceptable level. In so doing a sound system of internal control should be able to reduce (but rarely eliminate) poor judgement in decision making; human error; the deliberate failure to follow control processes by employees and managers; and the impact of unexpected events.

Internal control and risk management are close complements. A firm should use its risk management systems to help assess potential opportunities and threats to its objectives. There are also many different risk management tools with the same purposes than Internal Control, such as loss prevention, loss reduction and risk financing tools, that may be used to ensure that the firm continues to meet its objectives.

4. PRINCIPLES AND RECOMMENDATIONS

4.1 CONTROL CULTURE

4.1.1 Principle

The board of directors 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. Management is responsible for the implementation of the Internal Control Culture and principles. All personnel need to understand their role in the internal control process and be fully engaged in the process.

4.1.2 Recommendations & Comments

4.1.2.1 In order to have adequate Internal Control systems, insurance undertakings should have an organisational Culture at all levels of the company that is conscious and aware of the importance of internal control. It is the responsibility of the board of directors and management to emphasise the importance of internal control through their actions and words. This includes the ethical values that the company displays in their business dealings, both inside and outside the organisation.

4.1.2.2 In considering their Internal Control systems, insurance undertakings have to be compliant with applicable national and EU legislation, both that which is specific to Insurance and that which is not.

4.1.2.3 In reinforcing integrity, insurance undertakings should avoid policies and practices that may inadvertently provide incentives or temptations for inappropriate activities.
Examples of such policies and practices, include remuneration and sanctions based on forward-looking factors (e.g. strategic success) rather than short-term profitability or growth indicators. This should be balanced by discouraging firms from increasing senior management's risk appetite by skewed rewards, i.e. huge bonuses for reaching ambitious targets but little penalty for under-achieving.
4.1.2.4 A good Internal Control Culture helps mitigate Reputation Risk. Reputation is the resulting image of the company, and relies on aspects such as relationship with customers, quality of services and products, transparency, as well as profit to shareholders.

4.1.2.5 All personnel within the insurance company have an Internal Control responsibility. It is therefore essential that all of them understand the importance of internal control and engage actively in the process according to their responsibilities and specific duties. Written codes of conduct should be drawn up. Responsibilities, accountability, procedures, information and reporting channels amongst others should be documented as appropriate.

4.1.2.6 Competence should reflect the knowledge and skills needed to accomplish different tasks. The board should decide on the overall guidelines to Human Resource policies and practices such as hiring, evaluating and compensating. Management should specify the competence levels, knowledge and skills for particular jobs (formal or informal job descriptions).

4.2 RISK ASSESSMENT

4.2.1 Principle

In establishing and maintaining an effective system of internal control an insurance undertaking should regularly assess both the internal and external risks that it faces. Assessment should include the identification and analysis (using quantitative and/or qualitative tools) of all the significant risks that an insurance company is exposed to, and act accordingly.

4.2.2 Recommendations & Comments

4.2.2.1 An insurance company's risk assessment activities should be proportionate to the size and complexity of its business. The company's approach to risk assessment should also be influenced by the nature of the risks that it faces.

4.2.2.2 An insurance company should assess:

- the risks that it is in the business of taking
  (for example, underwriting risk, provisioning risk and market risk);
- any other relevant risks that it is not in the business of taking, but which are a by-product of its business activities
  (for example, internal governance and control risk, business continuity risk, people risk).
- the business opportunities underlying the different risks assessed.

4.2.2.3 An insurance company should plan and document its risk assessment objectives, as well as the assumptions and methodologies that it intends to use when assessing its risks.

4.2.2.4 Risk identification includes the processes by which an insurance undertaking pinpoints its risk exposures, both internal and external. An insurance company should try to identify as many of its risks as is reasonably practical, with particular attention paid to significant risks. A significant risk is a risk whose consequences could pose serious obstacles to the achievement of not only an insurance company’s objectives, but also those of its supervisor, and policyholders. Potentially significant risks for the insurance sector include underwriting risk including provisioning risk, credit risk including reinsurance risk, market risk including interest rate risk, investment risk and ALM risk, and operational risk.

4.2.2.5 Attention should be paid to the different importance and incidence of risks for Life and Non Life and for different products.

4.2.2.6 Risk analysis is the process through which an insurance company is able to understand the nature of the risks that it faces, including how they come to exist, whether they can or should be controlled and how they can produce a loss or gain. This can include the qualitative analysis of risk (e.g. via the use of risk mapping or scorecards) as well as quantitative risk measurement using stress testing and other tools to determine the likelihood and value of potential gains or losses. When analysing its risks, an insurance company should also consider

the potential interrelationships that can exist amongst them. This means that an insurance company's risks should not only be evaluated individually but also on an aggregate basis.

4.2.2.7 Once an insurance company has identified and analysed its risks it should decide its tolerance for these risks and the extent to which it wants to assume them or not. The level of risk tolerance should be established by the board of Directors, and reviewed on a periodical basis, at least annually. Accountability for the degree of risk to be taken ought to be documented as appropriate. In the case of assuming risks, the company should ensure that it has appropriate arrangements in place to mitigate and or control them.

4.2.2.8 Risk assessment should be ongoing, with processes such as risk identification and analysis repeated as necessary. In addition, the whole assessment process should be benchmarked within the entity, and reviewed periodically, as new risks may appear, and existing ones may change.

4.2.2.9 An insurance company should create an appropriate culture and controls to support its risk assessment activities. This culture should encourage staff from all parts of the company to contribute to the identification and analysis of risk.

4.3 CONTROL ACTIVITIES AND SEGREGATION OF DUTIES

4.3.1 Principle

An adequate Internal Control System requires the implementation of effective and efficient Control Activities at all levels of the entity. They should be implemented by the management in line with the goals and strategies set up by the board of directors, and should involve all personnel. As an integrated part of daily business, these activities should be reviewed and recorded on an on-going basis.

An efficient Internal Control system demands an appropriate segregation of duties and responsibilities, both at individual level and between functions.

4.3.2 Recommendations & Comments

4.3.2.1 Control activities are defined as policies and procedures that help to ensure that management directives are carried out.
Such control activities will vary within insurance undertakings, since they have different goals, strategies, structures and risk appetite. As a result, a broad set of possibilities and a significant variety of activities may be used, tailored to the undertakings' necessities. Moreover, and whenever applicable, the control activities should be carried out in accordance with the insurance Group and Financial Conglomerate structure.

4.3.2.2 Control activities should be linked to the risk assessment processes, as long as they tackle those risks previously identified and analysed by the insurance undertaking. They should address efficiently the process of defining adequate limits for exposure to risk as well as policies and procedures aiming to adjust business activities to the strategic decisions the risk profile. concerning

4.3.2.3 In general, control activities should not only serve to detect but also to prevent problems.

4.3.2.4 Control activities should be carried out through all levels of the entity enhancing transparency of every business activity and involving the board of directors, the management and all other personnel of the company in those activities. References to the board of directors and management shall be considered in line with the content of paragraph 2.5, Legislation relating to jurisdictions.

- Board of directors

  a) The board of directors has overall responsibility for ensuring that an adequate and effective system of internal control is established and maintained.

  b) The board of directors is responsible for approving and periodically reviewing the overall business strategies and significant policies of the organisation as well as the organisational structure and the internal control strategy of the insurance company.

c) The board of directors should provide direction, guidance and suitable prudential oversight, ensuring that the insurance company is appropriately and effectively managed and controlled and assuring compliance with laws and regulations.

d) The board of directors is responsible for the supervision/evaluation of the company's performance, particularly of the management.

e) To accomplish its responsibilities, the board of directors should:

e1) Select and approve the management, ensuring its appropriate competence, knowledge, integrity, prudence and experience to fill the management position.

e2) Define the responsibilities and duties of the management.

e3) Define, approve and review the organisational structure, ensuring an adequate framework for internal control within the insurance company, to include arrangements for delegating responsibility and authority, proper decision making procedures and an adequate segregation of duties, both between functions and between individuals.

e4) Define, approve and review the company's personnel and human resources policies, ensuring its sufficiency and qualifications.

e5) Define, document and maintain internal control guidelines to serve as a basis for concerted control activities on all business levels, ensuring its implementation and compliance within the company.

e6) Define outsourcing policies and specific control guidelines regarding the outsourced functions, ensuring that particular attention is paid to any core functions outsourced.

e7) Define internal programmes, procedures and controls to combat money laundering and terrorist financing.

e8) Ensure that the management is monitoring the effectiveness of the internal control system.

e9) Request periodical reporting on the effectiveness and appropriateness of the internal control system (including information on activities, findings, conclusions and recommendations) to enable assessment of the insurance company's progress toward its goals and the sufficiency of its internal control system.

e10) Request that any internal control weaknesses and deficiencies, whether identified by supervisory authorities, management, staff, internal or external auditors, other control personnel, or market conduct activities indicators, are reported in a timely manner so that appropriate action can be taken.

e11) Review the internal control guidelines making the necessary recommendations in order to correct and, if necessary, improve the internal control system.

e12) Ensure that the management promptly follows up on the recommendations.

- Management

a) Management is responsible for carrying out the directives of the board of directors, including the implementation of strategies and policies and the establishment of an effective internal control system.

b) Management is responsible for the effectiveness of the company's organisational and procedural controls.

c) Management is responsible for keeping the board of directors updated as to the effectiveness and appropriateness of the internal control system.

d) To fulfil its responsibility, the management should:

d1) Maintain an organisational structure, in line with the board of directors directives, that clearly assigns responsibilities, prudent and appropriate levels of delegation of authority and reporting relationships.

d2) Ensure that employees have the requisite skills and experience to allow them to carry out their specific function within the company.

d3) Ensure a prudent segregation of functional responsibilities within the company, both between individuals and between functions. An effective internal control system should require that there is appropriate segregation of duties and that personnel are not assigned conflicting responsibilities.

d4) Ensure that any areas of potential conflicts of interest are identified on a preliminary basis, minimised and subjected to careful and independent monitoring. If done efficiently, certain risks such as operational risk (including individual fraud), investment risk, underwriting risk or even reputational risk can be reduced.

d5) Set down clear lines of reporting ensuring an effective communication throughout the organisation.

d6) Develop and maintain comprehensive documentation that clearly sets out the responsibilities, the delegation of authority and reporting relationships within the company's organisation.

d7) Establish and document appropriate internal control policies and procedures in all business units in line with the board's guidelines, and ensure that those activities are a part of the daily activities of all relevant personnel**.**

d8) Ensure the compliance with the outsourcing policies defined by the board and implement the specific controls over the outsourced functions, certifying that they are efficiently carried out.

d9) Implement the procedures and controls defined by the board of directors that will allow detect money laundering activities and ensure that such procedures are efficiently executed.

d10) Ensure an effective level of management control through all levels of the insurance company and its various activities.

d11) Implement a mechanism to regularly verify compliance with the control policies and procedures and monitor the adequacy and effectiveness of the organisational and internal control system. Appropriate early warning systems related to the control activities are an essential tool for the control scheme and objectives and should therefore be implemented.

d12) Request regular detailed reports on the internal control activities in order to allow continuous evaluation of the effectiveness and appropriateness of the internal control system.

d13) Report periodically to the board of directors on the effectiveness and appropriateness of the internal control system, to detect and remedy any weaknesses or deficiencies detected, whether within the company or by an external party, e.g. supervisory authorities, external auditors.

d14) Implement the recommendations made by the board of directors on the improvement of the internal control system.

4.3.2.5 Control activities consist of a variety of procedures and policies. There are control activities common to all entities, as well as insurance specific ones. Specific internal control policies and procedures should be defined and implemented in conjunction with specific functions within the insurance company. These should be adequate for the nature and scale of the entity's business.

Specific control activities should be defined and implemented for the main activities within the insurance company, including the following:

- Underwriting policy - Control activities should ensure that underwriting activities are in line with strategic goals and internal risk tolerance policies, ensuring that the product design is accompanied by a technical analysis of the risk profile, in order to ensure correct premium pricing.
  e.g. A conflict of interest may arise if determination of technical basis is subordinated to commercial purposes. Although both areas have to work side by side, internal control need to maintain an appropriate balance between them, avoiding for example that commercial goals predominate on a sufficiency of premiums strategy, thereby endangering the solvency level of the insurer’s activities.

- Distribution channels – There should be clear rules for all distribution channels, with defined responsibilities for the supervision of both internal and external persons involved in distribution.
  e.g. It should be ensured that premiums are paid in a timely manner, so that the insurance undertaking does not become the creditor of significant amounts of premiums. Management should establish rules and procedures ensuring that agents comply with the firm's policies and respect their contractual obligations. Commission structure should be closely monitored.

- Claims management - The processing and follow up of claims, as well as their amount and frequency should be accurately documented. This should be done both for each claim and for every branch the undertaking is authorised to operate.
  e.g. Every payment exceeding a certain predetermined amount should be authorised by a competent responsible manager. This dual custody should avoid fraud or other manipulations; certain contracts may be reviewed and if deemed necessary not renewed.

- Set up of technical provisions - A clear set of rules should provide guidance on the principles of how to determine case provisions. In every individual case the assumptions underlying the calculations of the provisions should be recorded. Actuarial analysis will complete the process ensuring the provision's sufficiency. In addition, unexpected loss (deviations) should be taken into consideration sufficiently.

- Investment policy, including control of operations with derivatives and safeguarding of assets. Insurance undertakings should define an investment policy in accordance with their commitments. A continuous follow-up of its content, the investment policy, and the degree of compliance with it should be done within the entity.

  Special attention should be paid to financial derivatives through the establishment of detailed internal rules which should be closely observed. Such rules should determine the maximum acceptable risk exposure.

  Access to certain types of assets, such as cash or securities, and transactions (e.g. OTC operations) should be limited to designated individuals, whose responsibilities must be strictly documented. This should be complemented by periodical verifications of the operations made.
  Internal Control systems have to guarantee an appropriate independence between investment trading functions and financial controlling functions, the front and back offices. In this area, financial insurance activities share most of the topics involved in banking financial activities. Therefore clear separation of decision, execution and control statements is a generally accepted principle of sound internal control organisation.

- Fulfilment of the solvency requirement – Analysis of the solvency implications of the business written, to ensure that there are sufficient economic resources to absorb losses that may occur from technical or other risks.

- Accounting policy – Control activities must ensure that accounts give a true and fair view of a company's assets and liabilities, its financial position, and whether it is compliant with the applicable laws and regulations.
  e.g. Internal Control systems should foresee the reconciliation of accounts.

- Protection of the insured/assured - Entities should implement effective systems to deal with policyholders' claims and complaints.
  A customer service department dealing with queries and complaints may be a good method to increase customer satisfaction and enhance the entity's reputation.
  In order to carry out effective policyholder protection, functions of claims handling should be separate from those functions that the insurer may have created to assess customer complaints. As far as claims departments have among their goals the monitoring and management of claim payment levels, it is obvious that a customer complaint due to an unsatisfactory claim payment can not be assessed fairly without the separation stated in this example. Furthermore, this is a clear example of added value created through an appropriate internal control system, having in mind that the main factor to create customers' satisfaction is an effective and fair service in case of claims.

- Control of the Reinsurance Program and other risk transfer instruments: A good Reinsurance program should be seen as an essential mechanism for the undertakings to lessen their exposures. Thus effective protection depends on the sufficiency and adequacy of the reinsurance programme, as well as on the quality and solvency of the reinsurers.
  (Examples of risks faced by insurers when accepting or ceding reinsurance may include amongst others those derived from conflict of interest, contractual misunderstanding, inadequate cover, or jurisdictional risks.)

- Information systems – Control activities must ensure that accurate information is provided on a timely basis. Information systems should allow the recording of all transactions made by the company, including Intra-Group Transactions and Exposures (according to Directive 98/78 and to Directive 2002/87).

- Anti money laundering procedures – Control activities must ensure that adequate measures are taken to investigate suspicious transactions.
  These should include preventive measures such as an identification of the customer upon conclusion of the contract and verifications of contracts in case of suspicious transactions. As commercial goals have a more immediate impact on insurance undertakings, the entity should implement regulations and controls to tackle the risk of commercial goals leading to the assumption of significant legal and reputational risks.

4.4 INFORMATION AND COMMUNICATION

4.4.1 Principle

Insurance Undertakings should have reliable information at all levels within their organisation, in order to define, achieve and review the objectives settled by the board of directors, through effective decision making processes.

Internal Control systems should ensure the effectiveness of communication procedures. Such communication should be internal as well as external, and may include both formal and informal paths.

4.4.2 Recommendations & Comments

4.4.2.1 Insurance undertakings should have both financial and non-financial information relating to the past and current situation of the entity, obtained both on internal and on external bases. The same rule of thumb should apply to operational data, for example data on compliance with external regulations and internal procedures.

4.4.2.2 Information should have at least the following characteristics and information-gathering controls should reflect these:

a) *Accurate*: information should be contrasted and verified upon being obtained and prior to use.

b) *Complete:* information should cover all relevant aspects of the undertaking on quantitative and qualitative terms, as well as indicators which only have a direct and indirect impact on the business plan.
e.g., if the provisions of a specific claim handler are consistently too high or too low compared to the final settlement.

c) *Timely*: information should be available on a timely basis, so as to facilitate effective decision making thereby enabling the undertaking to anticipate and react to future events.

d) *Consistent*: information should be recorded using models which allow for information to be compared both horizontally and vertically.

e) *Transparent*: information should be presented in a manner which is easy to interpret, ensuring that the key elements of the information are clear.

f) Relevant: All information used should relate directly to the purpose for which is required, as well as being reviewed and improved continuously to ensure that it is consistent with the needs of the organisation.

4.4.2.3 Accounts of the entity should be compliant with all the aforementioned characteristics for information as well as with their applicable legislation.

4.4.2.4 Insurance undertakings should establish, maintain and improve effective communication channels both within the company and externally in order to achieve its goals. Such communication should flow both horizontally and vertically, top down and bottom up.

4.4.2.5 Communication lines inside the company should also encourage adverse reporting, particularly when flowing upwards (in order to avoid that employees did not share such negative information), and permit breaking the chain of managerial reporting should the situation call for such action. Quality reports, timely reporting, accuracy, completeness, suggestions should be encouraged.

4.4.2.6 Management should be responsible for ensuring all employees are familiar with their roles, responsibilities and duties in relation to Internal Control, as well as the objectives of the undertaking.

Employees should be aware of the importance of Internal Control in relation to their work as well as the company's goals. They should know and understand the company's strategic objectives and organisational plans. Guidance on technical and accounting information which may affect the performance of the job should be given.

4.5.2.7 The information given to third parties, such as supervisors and customers, should be reliable, timely, relevant, qualitative, quantitative, and communicated clearly and effectively. Appropriate disclosure should have a positive impact on the Insurance market and its transparency.

4.5.2.8 Information coming from third parties on the deficiencies or weaknesses of the undertaking's Internal Control should be seriously considered when improving the entity's Internal Control systems.

4.5 INFORMATION & COMMUNICATION TECHNOLOGIES

4.5.1 Principle

Insurance Undertakings should implement Information and Communication Technology (ICT) systems appropriate to the activities they carry out, their strategies and needs. Security controls for the risks inherent in ICT should be established to effectively enhance management of those risks, allowing the insurance company to recognize both the potential benefits and the associated risks of such systems.

4.5.2 Recommendations and Comments

4.5.2.1 Insurance Undertakings are becoming more and more dependent on information and communication technology (ICT). Such dependence means both implicit and explicit risks for the company that should be identified and tackled in an appropriate manner.

4.5.2.2 Based on their individual strategies, insurance companies should assess the advantages of establishing effective and efficient ICT systems, by defining a strategic ICT plan, coherent with the undertaking's business plan. A continuous assessment of the effectiveness and efficiency of such systems should be implemented through monitoring, benchmarking and using feedbacks to improve them. This should cover all ICT-processes as well as the assessment of the adequacy of the Internal controls. Insurance companies might consider having such assessments carried out both internally and independently by external bodies.

4.5.2.3 Adequate ICT systems should be implemented regarding the following fields:

- Policyholders information, allowing an improved follow-up and more integral analysis.
  e.g. when the customer has more than one policy in the same company or group, allowing a complete vision of his performance and providing him/her a better service.
- Insurance policies, reducing the cost of issuing and handling.
- Claims, allowing a better and more efficient management, as well as making claims provisioning easier and more transparent.
- Risk Management, with a better control of risks through the accumulation of more and more accurate and updated information.
- the integration of management systems (specially in cases of mergers, takeovers…).

4.5.2.4 The uses of ICT have been expanded due to increased usage by policyholders of Internet access to conclude insurance contracts. Such external access to insurance systems heightens levels of vulnerability.
e.g. including opportunities for insurance fraud, money laundering, misselling of products, 'small print' not realised or understood, ambiguities in application of contract law, to whom to address policy complaints, etc. Undertakings internal control on ICT systems should reflect such risks.

4.5.2.5 The outsourcing of ICT functions may lead to increased risk through the transmittal of sensitive and confidential information about both the undertaking and policyholders to third parties, cross borders…

4.5.2.6 Security of ICT systems is an integral element of sound management practice of the entity. Security systems should not only cover the undertakings themselves, their hardware, systems and data, but also access to information, integrity of policyholders etc. Security controls implemented should include:

- Managerial Controls: e.g. assessments of existing risks within the organisation, planning and setting up an ICT platform and organisation to support it, monitoring performance and security.
- Operational Controls: e.g. clarification of duties and management of human resources, developing and testing contingency plans.
- Technical controls: those incorporated in the systems themselves.

4.6 MONITORING

4.6.1 Principle

Insurance undertakings should implement appropriate monitoring systems for their Internal Controls' efficiency and effectiveness. Monitoring should be carried out on an ongoing basis, complemented with separate evaluations.

As an integral part of an internal control system and in keeping with the diversity and complexity of the insurance undertaking's activity, there should be an effective and comprehensive internal audit carried out by operationally independent, appropriately trained and competent staff.

The internal audit function should be conducted through a professional audit program designed to provide reasonable assurance that Internal Control objectives are met. An effective internal audit function should also comprise a follow-up process on audit findings in order to assure that they are being dealt with adequately.

4.6.2 Recommendations and Comments

4.6.2.1 The Internal Control system should be monitored in a continuous way in order to assure that, in the face of internal and external circumstances, compliance there with is maintained. Design of the Internal Control system should include embedded monitoring of operations and performances. Account ability for the monitoring processes should be clearly identified and stated.

4.6.2.2 Ongoing monitoring should occur in the course of normal operations and should allow the insurance undertaking to, in a more regular and promptly way, improve their internal control system.

4.6.2.3 Apart from being part of the daily activities of the insurance undertaking, monitoring should also include periodic evaluations of the overall internal control system. Separate evaluations should help obtain an all-round perspective of the situation of the company, thus providing the board and management with important data for decision making. Such evaluations may be carried out by personnel of the company, the internal audit function, personnel of another entity in the same group or conglomerate, or outsourced.

4.6.2.4 Monitoring should include procedures to detect gaps or problems. Further, these problems should be registered and documented. Recommendations, decisions, or criteria adopted should also be documented to facilitate future benchmarking.

4.6.2.5 The internal audit function should form an integral part of the company's internal control environment, assessing the adequacy of and the compliance with the policies and procedures established by the insurance undertaking. It should be of a nature and scope appropriate to the business of the entity and ensure a comprehensive examination of the effectiveness of the monitoring activities as well as of the internal control system.

4.6.2.6 The internal audit function should have sufficient authority to carry out its responsibility objectively and independently. To ensure appraisals are made without bias or influence, the Internal Audit should be independent of the day to day functioning of the insurance undertaking.

4.7.2.9.

4.6.2.7 Considering the importance of this function, the internal audit should be staffed with competent, qualified, well-trained and independent people who should have a clear understanding of their role and responsibilities.

4.6.2.8 A comprehensive plan governing the audit objectives for the period under review should be developed. The plan should identify the risk activities, operations and internal control systems to be reviewed, specifying the frequency of the audit and identifying the necessary resources to carry out the plan.

4.6.2.9 Criteria for assessing the adequacy of specific policies, procedures and controls should be established to address the risks and / or controls objectives.

4.6.2.10 To be effective in the execution of its function the internal audit staff should always have access to all the insurance undertaking activities, including branches and subsidiaries. Complete access to all activities, documents and persons should be granted.

4.6.2.11 The internal audit function should report directly to management and should direct access to the board of directors. The deficiencies and recommendations identified by the internal audit should be reported, in a timely manner, to the appropriate management level ensuring that the evaluation it is not biased in any way and that issues arising thereof are promptly addressed.

4.6.2.12 The internal audit function should conduct follow-up reviews in order to ensure that the necessary measures to address the deficiencies have been taken.

4.6.2.13 The board of directors and management should, periodically, receive reports summarising all control issues that have been identified. A broadly view of those controls may show, in isolated and immaterial deficiencies, trends that could become significant inadequacies if not address promptly.

4.6.2.14 Insurance undertakings should consider the appropriateness of creating an Audit Committee to assist the board of directors in the assessment of the effectiveness of the IC systems.. Should this be deemed unnecessary, assessment of the convenience of such a facility should be discussed at Board level regularly.

Rather than being viewed merely as a link between the board and the Internal Audit Department, the Audit Committee should also carry out core functions such as the verification of the whole audit process and units, structure, compliance with the Audit Plan, selection of the External auditors, analysis of the implementation of the different recommendations issued by the External auditors…

Under no circumstances may the settlement of an Audit Committee transfer responsibilities from the board of directors.

5. SMALL ENTITIES

5.1 International organisations frequently refer to the valuable social role of small insurance undertakings (especially in certain jurisdictions) and agree on the need to establish and implement general principles and regulations relating to the special features and characteristics of these entities. Consequently, the Working Group has included a special chapter on the application of Principles on Internal Control to small entities.

5.2 Small entities should apply all the IC principles outlined, regardless of the size or features of the insurer. Nevertheless, internal controls effective in large organisations may not be suited to small entities and the implementation of these may be executed differently in small undertakings.

5.3 The definition of small entities may differ depending on the circumstances and jurisdictions of each entity. As a result, the Working Group considered the respective regulators should decide on a definition of 'small entity', according to specific experiences, supervisory practices and regulations.

5.4 Thus, an approach by small entities to Internal Control could be expressed as the balance between:

- the cost and practical reasonability of implementing an internal control system in a specific way.
- the benefit obtained from such implementation, assuring that ultimate goals of Internal Control are achieved.

5.5 Consequently, when considering a 'small entity' approach, it can't be identified as a relaxing allowance or a lack of essential goals of Internal Control.

5.6 In line with the aforementioned, a "small entity approach" can not be applied using purely quantitative criteria (such as total balance or premium income; number of staff;...). Experience shows that quantitatively small entities may require an intensive IC if certain qualitative circumstances are present (such as the number or relationship between stakeholders, situations where the insurance undertakings carry out risky classes of business, etc.).

5.7 On the other hand, a medium-sized entity with a very low risk profile in certain areas of activity, may not require such an intensive IC system on those areas.

5.8 Therefore, more important than defining arbitrary boundaries between small versus medium and large entities, when assessing IC requirements, is the consideration of the final goals of Internal Control and their achievement.

5.9 In practice, it is usual to find small entities outsourcing some of their activities, including core activities. Thus, "outsourcing" is a key topic for small entities.

- 5.10 Firstly, outsourcing ought not mean relaxation on Internal Control. Moreover, "outsourcing" implies additional risks from an Internal Control viewpoint, that have to be addressed. As a common example of those specific risks, "outsourcers" may not completely understand the goals of the small entity, while the small entity may not

understand the actual service that has been acquired or a conflict of interest may arise with other clients or with the goals of the "outsourcer".

5.11 When selecting the most suitable outsourcing alternative, small entities should not only focus on budgetary considerations but also on the contribution of the outsourcer to improve the Internal Control systems of the entity. The validity of an outsourcing contract that weakens the Internal Control systems of the insurance undertaking is questionable. Furthermore, as outsourcers offer specialisation and larger structures and capabilities, improvements to the IC systems of the small entity should be evident.

5.12 Outsourcing does not release the insurance undertaking, nor its board of directors or management, from its liabilities and obligations.

5.13 In small entities, segregation of duties may be restricted due to limited resources, which may lead to staff having to multi-task. In such cases, the goals targeted in the "segregation of duties" principle may be achieved through practices other than segregation (rotation of duties, external reviews on regular basis, unannounced verifications, etc.). As conflicts of interest within such an entity are difficult to identify, external assessment on an independent basis may prove beneficial.

5.14 As previously mentioned, several small insurers, even medium-sized entities, only offer a small number of products with a low risk profile (taking into account the simplicity of the products, the individual policy and cumulative policy exposure.)In this case a "small entity approach" seems reasonable as it contributes to the efficiency of the insurance undertaking without undermining solvency or confidence in Internal Control.

5.15 If the establishment of an internal audit function is not feasible or not appropriate in the lights of the organisational structure of the company, the board should apply additional monitoring procedures or outsource this function in order to give sufficient assurance of the Internal Control systems' adequacy.

6. OUTSOURCING OF BUSINESS ACTIVITIES

6.1 Many insurance undertakings, regardless of size, type of business and products, outsource different functions, including key ones. Reasons vary significantly; it may allow undertakings to focus in their core activities, while having access to services and products necessary for managing the entities and complying with regulations and requirements.

6.2 Practice has shown how outsourcing may raise additional risks for the undertaking, and such risks must be managed in an appropriate manner. Also evident is the risk of relaxation of Internal Controls of the function outsourced. Failure to set rules for outsourcing activities and monitoring of performance may threaten the solvency situation of the undertaking.

6.3 The Working Group, bearing all the aforementioned in mind, has included a special chapter on the Internal Control systems of outsourced functions, given the importance of the subject. In addition to this chapter and having in mind the importance of outsourcing for small undertakings, specific references are also included in Chapter 5 of this document, on Small Entities.

6.4 Outsourcing of a function does not release the insurance undertaking from its liabilities and obligations. The board of directors and the management are responsible for ensuring that adequate internal controls and risk management systems relate to the outsourced functions.

6.5 Outsourcing often implies additional risks from an IC viewpoint. Therefore the insurance undertaking should clearly identify the strategic purposes, benefits and risks that are involved in outsourcing.

6.6 The Board of directors must approve outsourcing plans and/or a written contract for the significant operations. The plan must show how risk management and other internal controls relate to the business .

6.7 Outsourcing ought not prevent the insurance undertaking from accessing information nor impede the management and monitoring of the outsourced functions. Also the supervisory authority must have full access to the information of outsourced activities.

6.8 The contractual liabilities and responsibilities, including those related to IC itself, must be clearly defined in a written contract.

The written contract should include the following points:

- A full and comprehensive description of the services to be provided, timeframe and costs.
- How reliable reporting is ensured.
- Clarification on who with the responsibility for each procedure lies.
- How the monitoring of compliance with external rules and regulations and internal procedures has been arranged.
- How the internal audit works in the case of outsourced operations.

6.9 Insurance undertakings should ensure that selected suppliers of outsourced services are economically viable, have sufficient expertise and commit themselves to comply with binding rules of the insurance entity on outsourced operations. Furthermore, the insurance undertaking should ensure that the supplier is compliant with national laws and regulations.

6.10 The supplier must be committed to act according to good insurance practice and in compliance with the regulations concerning confidential information. Outsourcing of certain functions (e.g. IT services or Management of Claims) allows the provider of the service to have access to important confidential information. The provider should be obliged to keep such data private.

6.11 The contract may not be further outsourced to a third party without the prior consent of the insurance entity. The insurance undertaking shall have the right to cancel the outsourcing contract if the service provider fails to provide the agreed service . Management should implement procedures control the efficiency of the outsourced function.

6.12 The insurance undertaking should ensure that periodic independent internal control and/or external audits are conducted to at least the same extent as if the activity was carried out by the company itself.

7. REFERENCES

7.1 The Working Group has taken into consideration, amongst others, the following documents and reports.

- International Association of Insurance Supervisors (IAIS) Core Principles and Methodology, October 2003.
- IAIS Guidance paper on Stress Testing by Insurers, October 2003.
- IAIS Anti-Money laundering guidance notes for Insurance Supervisors and Entities, January 2002.
- The Joint Forum, Corporate Governance and the use of the Audit and Actuarial Functions for Supervisory Purposes, July 2002.
- COSO, Internal Control, Integrated Framework, 1992.
- COSO, Addendum to Reporting to External Parties, Internal Control Integrated Framework, 1994.
- COSO, Enterprise Risk Management Draft document, 2003.
- Basle Committee on Banking Supervision, Framework for Internal Control Systems in Banking Organisations, September 1998.
- European Monetary Institute, Internal Control Systems of Credit Institutions, July 1997.
- Securities Exchange Commission (SEC), Management's Reports on Internal Control over Financial Reporting and Certification of Disclosure in Exchange Acts Periodic Reports, 2003.
- COBIT (Control Objectives for Information and related Technology) Framework, issued by the Information Systems Audit and Control Foundation, 1996.
- London Working Group Report on Prudential Supervision of Insurance Undertakings, December 2002.
- KPMG Study into the Methodologies to assess the overall financial position of an insurance undertaking from the perspective of prudential supervision, May 2002.

7.2 In the latest stages of the work carried out by the Group, the European Commission issued a document, MARKT /2539/03, on ¨Solvency II- Reflections on the general outline of a framework directive and mandates for further technical work ¨, of vital importance to this Working Group, as it includes certain areas of work concerning different aspects of insurance supervision, including Internal Control. Furthermore, the structure envisaged for the framework Directives foresees a new article on ¨requirements on Internal Control and administrative organisation ¨.