POSITION PAPER

Roles and tasks related to the
Internal Control Process
in a service company.

Internal Control Association
www.icib.org

This document is the first release of the Position Paper. Future releases may be edited to respond to new developments or expectations. Suggestions and remarks for further enhancement of the Position Paper can be send to info@icib.org.

This Position Paper is organised around 12 Precepts. A Precept can be defined as a command or principle intended especially as a general rule of action. Symbolically, the number twelve represents a whole, a perfect and harmonious entity.

Version 1, edited 2014

Introduction

Most organisations and companies, both in the private and public sectors, have over the last years been putting in place structures, procedures and resources to maintain and continuously improve the running of their business. Meanwhile, the concept of company governance has gained in maturity and functions such as general inspection, internal audits, management control and risk management have progressively taken root, enhancing the way companies and organisation carry out and control their activities.

The latest evolution in the field of company governance is commonly referred to as internal control, which, unlike internal audit or general inspection, is not a function but rather a process involving all personnel in the organisation.

The importance and relevance of internal control has, in extreme situations, been underlined by a series of cases in the past decades where a number of companies went bankrupt mainly because of major weaknesses in, or even complete absence of an internal control system. This led to a number of regulatory requirements or best practices provisions, some of them relating to the implementation of internal control in organisations.

But what exactly is internal control about?

In a top-down approach, organizations and companies need to define and continuously review their strategy, according to their internal and external environment, their vision or the perspective that the executive management or the board wishes to convey. Further on, the strategy is translated into strategic objectives that are commonly expressed and communicated to the different stakeholders (internal and external ones) through strategic plans.
Based on these strategic objectives, each entity, department or service within the organization defines operational objectives that are presented and communicated within the organization. These operational objectives are cascaded down and translated at all levels of the organization.

Complementary to this top-down approach, each and every activity in the organization should be aligned with the strategy and should contribute to the achievement of those objectives.

Indeed, all stakeholders (internal and external ones) of an organization wish and expect clear objectives to be defined and achieved in order to ensure that the organisation remains sustainable and creates value over the years.

However, organizations sometimes become aware of the non-achievement of their objectives too late, often at the end of the year and with severe consequences for their operational or financial results. To avoid this, organizations can conceive and implement a specific transversal process that makes it possible, on a permanent basis, to obtain reasonable assurance on the achievement of the defined objectives and on the ongoing adjustment of these objectives to the ever changing environment.

As can be appreciated, such a process is not a 'one-person affair' but involves all the actors of the organization, from the operational staff who execute the regular and repetitive tasks to the top management.

This transversal process or system is commonly called Internal Control.

But the need to control the activities is not really anything new. Most companies started long ago to implement different types of measures and procedures, commonly called "controls". However, a clear distinction should be made between the "Internal Control process" and these "controls". The former constitutes the main topic of this Position Paper. The latter, the controls, are to be considered as outputs of this internal control process, in the sense that they derive from a series of initiatives that are undertaken in the process to analyse the risks and decide on how they could be mastered in the most effective way.

In terms of positioning the internal control process, it is commonly accepted that no one can reasonably take on a responsibility without considering how to gain control over the underlying activity. All staff involved in the organisation becomes as such, on his level and within his responsibility, an active contributor to and actor in the internal control process.

In order to further clarify the roles and interactions in the internal control process, most organisations define three lines of defence. The first line of defence relates to everything that allows operations to be effective and to provide products and services in line with expected objectives. It is therefore up to the teams present on the field to implement the internal control process

on a day-to-day basis in their activities. The second line of defence consists of internal departments, mainly non-operational ones that define rules and guidelines to be respected and implemented in the operational activities. The second line can also advice, provide guidance or assistance, and support the process methodologically. In doing so, the second line can give a first independent opinion on the way in which processes are carried out and controlled by the first line of defence.

The internal control process and its roll-out over the first and second line of defence is clearly the responsibility of the management of the organisations. The third line of defence is made up of the independent internal audit functions, in charge of evaluating the internal control process in view of its continuous enhancement and in response to the stakeholders' expectations to gain assurance on the achievement of the companies' objectives.

It should also be noted that it is not the aim of this document to define the various functions within an organisation, but to show the link that exists between internal control and governance functions. In addition, internal control interacts with risk management and indeed complements it, since internal control includes those risks which the operational teams are confronted with when reaching their own objectives.

Bearing in mind these various notions and the relative complexity of the internal control process, ICIB describes it in 12 precepts which aim to complement the reference material which already exists, such as the COSO framework, ISO 31000 standard and the CBOK guidelines, in order to bring together best practices on the topic.

The Position Paper was initially addressed solely to the insurance industry undertakings. Since the context and requirements in other service industries proved to be very similar, we extended the scope of this document to the whole service industry and even to other organisations of the private and public sector.

Pierre LECLERCQ
Vice-President

Yves DUPONT
President

Acknowledgement

Recognition should be given to those who actively participated in the insurance workshop and contributed to this Position Paper in accordance with their experience on the functioning of the internal control framework.

- Stephane Debauve: BNPParibas Fortis
- Jos De Neve: ESGI
- Yves Dupont : ICIB
- Manuel Eusebi: BGL BNP Paribas
- Bernard Guillaume: ICIB
- Frank Helsloot: AXA-Bank
- Alexandrine Henriet: Generali Belgium
- Germain Lanneau: BNPParibas Investments Partners
- Pierre Leclercq: ICIB
- Nicolas Leonard: Sogecore
- Pierre Vijfeyken: Europe Assitance

We would like to thank H.C. Pete Warner, President of ICI and Mike Pregmon, COO and Executive Director of ICI (Internal Control Institute) for their proof reading and remarks.

About the ICIB Association

The ICIB (Internal Control – Contrôle Interne – Interne Beheersing) is an independent professional non-profit organization dedicated to the development and the promotion of sound internal control practices. The Association was created in 2008 as an independent organization and has an exclusive partnership with ICI, the Internal Control Institute in the Unites States, for the granting of personal certifications (CICS / CICP). ICIB organizes training sessions and series of events such as the yearly IC-AWARD, as well as various thematic conferences.

Available regulations and guidelines

For the purpose of elaborating the position paper, the following regulations and standards were considered:

- Solvency II Directive;
- CEIOPS' "Advice for Level 2 Implementing Measures on Solvency II";
- CEIOPS ' Issues Paper "Own Risk and Solvency Assessment (ORSA)";
- EIOPA Final Report on Public Consultation No. 13/008
- COSO Internal Control – Integrated Framework;
- ICI's "Internal Control Common Body of Knowledge"

Preliminary note

This document focuses on specific topics that may help organizations in the daily functioning of their internal control process and in projects to develop such a process. However, it is not the purpose of this document to constitute a comprehensive guideline for the implementation of an internal control process.

This document intends to promote internal control as a performance enabler and value creator for the organization, moving away from the more restricted definition of internal control as being limited to a compliance or inspection role.

Internal Control

Summary of the Principles

Precept 1: Internal control is an active process.

Precept 2: As any other process, the internal control process is submitted to continuous improvement cycles.

Precept 3: The internal control process involves all staff of an organization, from the top management to employees at all transaction levels.

Precept 4: The ultimate goal of internal control is to provide assurance about the capacity of the organization to achieve its objectives.

Precept 5: Internal control is a process with various sub-processes; the set of rules and procedures with which staff has to comply in order to control its activity can be considered as a regular output of this process.

Precept 6: Distinct approaches are developed to organize the different control activities.

Precept 7: Risks are analysed with their interdependencies.

Precept 8: The internal control process is integrated in the business processes.

Precept 9: Second line of defence functions assist management in controlling their end-to-end process and bring in the necessary judgment and expertise whenever necessary.

Precept 10: Specific risk management functions will contribute to and interact with the internal control process on operational risks.

Precept 11: An internal control coordinator acts as an advisor and coach of the internal control process.

Precept 12: The organization will define the responsibility of all participants in the internal control system, in line with the components of the internal control process.

Precept 1

Internal control is an active process.

Art. 46 of the Solvency II Framework Directive requires from the insurance undertakings that they should have in place an effective internal control system. In line with the COSO framework, internal control is defined by CEIOPS (point 3.227 of CEIOPS' "Advice for Level 2 Implementing Measures on Solvency II: System of Governance") in general terms as a *process affected by an organization's structure, work and authority flows, people and management information systems, designed to help the organization accomplish specific goals or objectives.*

Defining internal control as an integrated process emphasizes the importance of a qualitative process management approach. The organization will have a thorough knowledge of its functioning (operational, management and support processes), in order to integrate internal control and risk management activities into its functioning. This is the most effective way to ensure that the internal control process is carried out and supported by all employees in the company.

Precept 2

As any other process, the internal control process is submitted to continuous improvement cycles.

Internal control leading practices encourage organizations to set up their internal control system as a process that is complementary to and integrated into the operational processes. It helps organizations (and its processes) by providing reasonable assurance regarding the achievement of objectives. The internal control process will in itself be subject to the same quality

enhancement cycles (e.g. through a plan/do/check/act cycle) as the ones that inform the quality initiatives on the operational processes.

The role of both internal audit and internal control coordinator (as described in Precept 11) is very important in the functioning of this continuous process improvement cycle.
Beyond what is meant by the "internal control process", the concepts "system of internal control" or "framework of internal control" will be commonly used to designate the process along with its guiding principle, structural elements (roles and responsibilities) and specific tools and methods used to support the process.

Precept 3

The internal control process involves all staff of an organization, from the top management to employees at all transaction levels.

Unlike the internal audit, which is defined as an independent evaluation function or activity, internal control activities are performed by all employees within the scope of their responsibility. Therefore, there is a focus on the role and responsibility of everyone with regard to the internal control process, rather than on the internal control as a specific function within the organization.

All actions undertaken by operational management in the execution of their tasks in the internal control process will be commonly designated as the 1st line of defence in an organization with regard to its risks (see Precept 9).

Guideline 5 (Key Functions) of the final report of EIOPA confirms, in accordance with art. 44, 46, 47 and 48 of the Directive, the undertakings' obligation to implement the following functions: risk management function, compliance function, internal audit function and actuarial function.

However, the Guideline and Directive do not state any obligation to create an internal control function, leaving open the possibility for greater involvement

of management and staff in the execution of an integrated internal control process.

In our opinion it makes sense to designate an internal control coordinator, as stated in Precept 11. The term “coordinator” underlines the principle that the responsibility for carrying out the internal control process relies on the operational management, from the top management to all transaction levels.

Support from the board and top management is of utmost importance to ensure the functioning of the internal control process and the success of continuous process improvement. This support may be reflected in an internal control charter or in separate messages that are issued in support of the project.

Precept 4

The ultimate goal of internal control is to provide assurance about the capacity of the organization to achieve its objectives.

Most internal control best practices and guidelines regarding internal control recognize at least three categories of objectives that drive every organization: operational objectives, reporting objectives and compliance objectives. The ERM (Enterprise Risk Management) approach completes this with the categories related to the strategy of the organization. The internal control process aims at:

- providing assurance concerning the achievement of all of these categories of objectives, focusing on the way management deals with the risk factors related to their own activity and process;
- enhancing the decision making process by creating greater awareness of the risks and enhancing the capacity of the organization to cope with these risks.

Given the interrelation between various objectives, we advise to set up an internal control process that covers all types of risk according to one single internal control framework, with a shared vocabulary and methodology applied by all employees to lead the various stages of the internal control process, regardless of the types of risk or objectives that are treated.

Precept 5

Internal control is a process with various sub-processes; the set of rules and procedures with which staff has to comply in order to control its activity can be considered as a regular output of this process.

Defining internal control as an integrated process implies that it constitutes a continuous activity with sub-processes or components. Most internal control best practice frameworks recognize at least 5 sub-processes:

1. Control environment: this component comprises among others the control culture, integrity, codes of conduct, organizational and HR requirements. Objective setting may also be considered as part of this component.
2. Risk assessment: this component forms the basis of all mitigation action. It can be further divided into three sub-components: risk identification, risk analysis and risk evaluation.
3. Risk mitigation action is a more comprehensive term than “control activities” or “internal control”. This component typically includes risk response initiatives, mitigation procedures and control actions.
4. Information and communication.
5. Monitoring, including (self-)evaluation, advisory and communication.

These components or sub-processes have to be considered as an indivisible whole.

Some organizations tend to restrict their internal control process to the execution and testing of controls or mitigation actions (components 3 and 5), leaving the risk assessment responsibility to specialized risk management experts. We believe that those who design and execute the mitigation actions

have valuable knowledge about the risks related to their process and bear part of the risk assessment responsibility. Their active implication in this component will contribute to the effectiveness of the internal control system and to its continuous improvement. The risk assessment component will of course be led in collaboration with all other relevant risk management initiatives. Given the transversal nature of most risks, their assessment and treatment is above all a matter of consensus between various parties, each in charge of bringing in his point of view on the risks to be identified and assessed.

Components 4 (Information and communication) and 5 (Monitoring) are essential to assure the continuous process enhancement cycle. Self-evaluation is an ideal approach to involve operational management in its control responsibility. It is also the basis of the internal control process "plan-do-check-act" continuous improvement cycle.

These five components are to be considered as sub-processes that each have their own input and output. Considering for example component 3 "Risk mitigation actions", an effective internal control process (system) will generate, on a regular basis, rules, procedures and treatment actions that are appropriate for mitigating the risks. Those "mitigation actions" are sometimes called "internal control**s**", not to be confused with the "internal control" process itself. The internal control process constitutes an ongoing process in the organization and should not be restricted to the mitigation actions it produces. The word "framework of internal control" or "system of internal control" may however, in our view, include both the internal control process and its outputs, provided the difference between them is made clear and the importance of the internal control process for the continuous enhancement of the internal controls is underlined.
For example, art. 46 focuses on the existence of *administrative and accounting procedures (That system shall at least include administrative and accounting procedures, an internal control framework, appropriate reporting arrangements at all levels of the undertaking and a compliance function).* In our view these procedures could be considered as an output of the sub-process 3 as defined above. This sub-process will assure quality and continuous improvement of these procedures.

Precept 6

Distinct approaches are developed to organize the different control activities.

The word control has very different meanings, ranging from the external inspection of an accomplished task to the design by the operational management of (preventive, detective, corrective) mitigation actions in an operational process. Putting a process under control does not necessarily mean that it is subject to external inspection. It rather indicates that sufficient actions have been taken by the management to provide a reasonable assurance that the risks are reduced to below the tolerance level. One could say than that the manager is “in control of his activities”.

There is frequent confusion between internal control (management responsibility) and the more restricted control or inspection initiatives. This confusion is sometimes increased by the existence of an internal control function in charge of verifying the right execution of rules and procedures, reducing the internal control process to the sole component of monitoring the mitigation actions.

Moreover, in some languages (such as in French and in Dutch), the word “control” has a very restricted meaning that comes close to the pure external inspection activity. In English the word “control” tends to encompass the action of mastering an activity or process.
To avoid misunderstandings, we suggest the use of a different terminology to designate the following actions:

- mitigation actions taken by management to reduce risks related to their activity. These actions may take the form of procedures to prevent or detect errors in the process execution or stemming from external factors and are integrated into the business processes. These actions are sometimes designated as “internal controls”, not to be confused with the “internal control” – the designation given to the overall process;

- inspection or verification of the output of an operational process (e.g. verifying outgoing payments) or the execution of a mitigation action;

- evaluation and monitoring of the quality of a mitigation action, of the internal control process or of one of its components (sub-processes).

Precept 7

Risks are analysed with their interdependencies

Categorization of risks is essential for reasons of communication and reporting, as stated in CEIOPS' advice 3.72.b. (*Adequate written policies that include a definition and categorization of the material risks faced by the undertaking, by type, and the levels of acceptable risk limits for each risk type)*. However, risks belonging to one category will often find their causes in elements from another category or in a conjunction of various types of risk elements. The understanding of these interdependencies and the outline of comprehensive risk scenarios will allow management to understand and treat risks in an appropriate way, avoiding the creation of management silos. A large majority of risk events results from a lack of insight into the interaction between different risk elements. As an illustration, some studies state that a large portion of underwriting risks or counterparty risks can be reduced to operational risks, since they find their origin in a weakness of the operational processes or a lack of communication or involvement between the organizational silos.

The need to analyse the interdependency between risk elements and risk scenarios is underlined in points 5.57 and 5.61 of the EIOPA Final Report No 13/008, as well as in art. 44(2) of the Directive: *The risk management policy should not only consider each relevant category and area of risk but also potential accumulation and interaction of risk. To this end, it should set out the frequency and content of overall scenario analysis to be performed.*

As an illustration we mention the foundation of one of the principles issued by the BIS in December 2013 (Progress in adopting the principles for effective risk data aggregation and risk reporting), stating that: *The financial crisis that began in 2007 revealed that many banks, including global systemically important banks (G-SIBs), were unable to aggregate risk exposures and identify concentrations fully, quickly and accurately.*

Precept 8

The internal control process is integrated in the business processes.

Given the interrelations between the various types of objectives and risks, responsibilities in the internal control process should preferably be aligned with the business processes definition. An "end-to-end" process definition will help to avoid a silo-type segregation between services and departments.

An integrated internal control approach would mean that the process owner takes responsibility for the major internal control tasks (including risk assessment, designing mitigation actions and reporting tasks, as described in Precept 5) related to the operational aspects of the process and its sub-processes, whereas the sub-process owner (or equivalent) would take care of the execution and the self-assessment of these mitigation actions. This scheme can be transposed at all levels of the process and sub-processes and will meet regulators' expectations as expressed by the CEIOPS advice 3.231: *An effective internal control system should comprise robust and efficient control activities at all levels of the undertaking. These should be implemented by the management in line with the strategies, business plans and goals set for the undertaking. As an integrated part of daily business, the control activities should be reviewed and documented on an on-going basis.*
This is also, in our opinion, how the statement of art. 44(1), *…That risk-management system shall be effective and well integrated into the organizational structure…* should be interpreted.

In highly centralised organizations working with standardized processes, the responsibility of process owner (and risk owner) may be restricted to only a few persons on head-office level, whereas the vast majority of staff is involved in daily transaction level activities related to first line client services. In our opinion there is however a need for a better involvement of process execution managers in the risk identification and mitigation process.

Some organizations may not have developed an "end-to-end" process approach or appointed process managers to monitor such processes. In these situations, the same role definition for operational management may apply within each silo. The internal control coordinator will set up compensating systems (such as transversal risk maps) to assure that transversal risks are assessed by all management involved and that actions to mitigate those risks are agreed on between the various silo managers.

Precept 9

Second line of defense functions assist management in controlling their end-to-end process and bring in the necessary judgment and expertise whenever necessary.

Most organisations structure their internal control approach on the basis of a triple line of defence model. These can be defined as follows:

The 1st line of defence is the operational management, in charge of major internal control tasks pertaining to risks that are related to their operations, as described in Precept 8. The first line of defence can be considered as the place where the risks hit the organisation first. It encompasses the controls activities that are part of the duty of the organisational units & management;

The 2nd line of defence is composed of risk management, control coordination functions, actuarial functions, financial control functions and compliance

functions. This line is in charge of the evaluation of the first line of defence. Its main activity is to perform monitoring tasks of the internal control process. These lines include the risk management and the compliance functions.

The 3rd line of defence represents the independent evaluation and audit functions. The independent assessment carried out by the internal audit function on the quality and effectiveness of the internal control and monitoring process put in place by the other lines of defence. The internal audit function is in fact responsible for ensuring that an independent assessment is carried out over the extent at which the internal control system is effective and efficient.

In our view, the 2nd line of defence will take on three major responsibilities:

1. Assisting management in the deployment of the internal control framework and practical techniques that are necessary to control the risks related to their activities. The internal control process indeed requires specific methodological skills (such as risk assessment, design and documentation of control activities, reporting on operational risks and their mitigation actions, self-assessment techniques, modelling techniques, incident managers) that are not covered by more traditional management techniques. 2nd line of defence specialists will facilitate those actions and bring in their methodological expertise;

2. Bringing in the necessary expertise on some risk domains, such as compliance risks. These experts are often in charge of business "supporting" processes (HR, ICT, counterparty management, …) and "management" processes (management control, financial functions) and will have a first line responsibility when it comes to the execution of their own process, in combination with a 2nd line of defence role to the extent that they have some authority over the decisions taken by the 1st line of defence, and a "risk observer" or consulting responsibility limited to advising the 1st line managers on specific questions related to their

expertise.

3. Providing an evaluation of the risks and mitigation actions led by the process owners. This evaluation can take the form of a validation of the self-assessment initiatives developed by the operational management and prepares the more independent and less frequent evaluations of internal audit (3rd line of defence). Being involved in the development of the internal control actions, the 2nd line of defence functions will however never reach the level of independence the internal auditor will have.

An organization may prefer to appoint "risk observer" 1st line of defence functions taking on the expert role described in point 2 above. In that case, the risk expert will be consultative and segregated from any direct evaluation responsibility as described in point 3 above.
Other organisations may prefer to reduce their 2nd line of defence functions to the third activity described above, leaving the full responsibility of the other two points to the operational 1st line of defence management. To some extent or another, 1st line of defence management will however need assistance on the design and implementation of the components of the internal control process, requiring techniques and methodology that are often not covered by more traditional management approaches.

A person or service may combine specific 1st and 2nd line responsibilities. For example, actuaries have their process for determining the right premiums and take on a risk management responsibility (2nd line) towards other functions in the organization. They have however their own calculation process and act as a 1st line of defence actor towards risks that may threaten the execution of this process. The same principle applies for example to incident database management functions. Another example is the risk management function where the control activity of the reporting of risks can be considered as a 1st line activity.

Precept 10

Specific risk management functions will contribute to and interact with the internal control process over operational risks.

Specific risk functions are created as part of the 2nd line of defence whenever a specific knowledge, expertise, authority or independence is required to mitigate and report on specific risks (e.g. compliance, fraud, …). As many of those specific risks occur in conjunction with operational events or operational control weaknesses, these risk management functions will assist 1st line management in assessing and mitigating risk elements (causes and consequences) that are related to their risk domain.

On the other hand, operational management may help those specific risk management functions in understanding how these risks and the operational process are interrelated.
As such, a strong segregation between operational risk management (primarily covered by 1st line and internal control coordination) and the specific risk functions may lead to misunderstandings over the real causes and consequences of key risks that are supposed to be managed by these risk management functions.

"Compliance" is one of the three (or four) objectives categories that an internal control system should give assurance over. Solvency II imposes the creation of a compliance function that is defined as follows (art. 46.2): *The compliance function shall include advising the administrative, management or supervisory body on compliance with the laws, regulations and administrative provisions adopted pursuant to this Directive. It shall also include an assessment of the possible impact of any changes in the legal environment on the operations of the undertaking concerned and the identification and assessment of compliance risk.*

Given the importance and complexity of the compliance matters it is indeed

necessary to organize a specific and independent function to organize and overview the undertakings' compliance. In many cases, however, the operational managers remain the ones who are best informed about the occurrence of events that may have an impact on the compliance objectives of the undertaking.

Precept 11

An internal control coordinator acts as an advisor and coach of the internal control process.

In order to facilitate the development of the internal control process, organizations may appoint an internal control coordinator, as part of the 2nd line of defence. This internal control coordinator will act as an advisor and coach in the internal control process and contribute to the creation of:

- a single consistent internal control framework throughout the organization;
- a common internal control policy;
- coordination of all methodological assistance to the 1st line of defence;
- an internal control training programme;
- an internal control reporting to the top management;
- a single point of contact with the regulators concerning the functioning and reporting of the internal control framework.

There is indeed a need to coordinate the internal control initiatives undertaken by the operational management and to coach management in the execution of the internal control processes as described above, contributing to the creation of a single internal control framework throughout the organization.

As a 2nd line of defence actor, the internal control coordinator may contribute to the independent permanent evaluation of the internal control actions lead by the 1st line of defence management. He should however refrain from directly carrying out the tasks that belong to the management with regard to the identification, the assessment and the treatment of risks.

Obviously, the internal control coordinator will assume an even more important responsibility in companies organized by “silo structures” with no transversal end-to-end process approach and poor risk and control communication between various parties involved. Also, his role is essential when an organization starts implementing an internal control process but will decrease over time while the 1st line of defence achieves a higher degree of maturity throughout the process.

The internal control coordinator function may be combined with a permanent control function. Its main task will consist in the evaluation of the (design and operational) effectiveness or deficiencies of the control activities and on the resulting quality of the operational process (in terms of incidents and near misses). The permanent control function coaches management in the self-evaluation process and is as such complementary to the inspection and audit functions. The extent of the actions of a permanent control service will highly depend on managements’ capacity to lead its internal control process and self-assessment initiatives.

Organizations will obtain an advantage by making a clear distinction in the denomination of those functions in charge of:

- On the one hand, coordinating and/or monitoring the internal control initiatives led by the management. Denominations such as “Internal control monitoring” or “Internal control coordination” could cover these activities;
- On the other hand, verifying the right application of existing procedures, by means of testing and inspection initiatives. A service called “Permanent control” could take on this responsibility although we believe that there might be a conflict between this inspection task and the coordination task of such a permanent control department.

Precept 12

The organization will define the responsibility of all participants in the internal control system, in line with the components of the internal control process.

Solvency II art. 44(1) of Level 1 requires that: *Insurance and reinsurance undertakings shall have in place an effective risk-management system comprising strategies, processes and reporting procedures necessary to identify, measure, monitor, manage and report, on a continuous basis the risks, at an individual and at an aggregated level, to which they are or could be exposed, and their interdependencies.*

According to most internal control guidance (such as the COSO Framework), these tasks are also part of an internal control system. However, it is not because they are defined as being part of both the risk management process and the internal control process that they should be executed separately or that a segregation between the functions in charge of these components should be established. In our view risk assessment and mitigation tasks should be executed jointly between all parties that have knowledge of expertise over the risk aspects:

- on the one hand, the 1st line operational employees, who will remain the risk owners of the risks related to the execution of their process. They bring in their knowledge on the functioning of the process and on how the risks factors may interact and risk events occur;
- on the other hand, the 2nd line of defence risk management and 1st line of defence risk observer functions, who bring in their expertise on specific risk domains.

In our view, the best definition of the difference between internal control and risk management is the one stating that they both pursue the same objective

and cover the same actions and components, the first from a process perspective and the latter from a risk expertise side. The definition of the responsibilities for these tasks can best be related to the processes and sub-processes of the organization (see Precept 8). This approach supports the principle of an effective integration of the risk management and internal control process.

According to CEOPS advice 3.64, this risk management system is also to be considered as a continuous and integrated process. CEOPS advice 3.71 establishes the link with the internal control process: *The risk management system shall be integrated into the organizational structure of the undertaking and into its decision-making processes. Good integration includes, in particular, that the risk management system should be supported by a suitable internal control system. The design and operational effectiveness of the risk management system to identify, measure, monitor, manage and report risks the undertaking is exposed to shall be regularly evaluated and reported by the risk management function. The internal audit function will review the assessment process.*

In our view, organizing an internal control system that "supports" the risk management system does not mean that the internal control process should be reduced to the "risk mitigation actions" components of the internal control process, leaving the risk assessment to risk management system (cf. Precept 5). Instead, we consider that the allocation of risk assessment responsibilities should be organized according to the knowledge that each party has on the behaviour of the risks and their conjunction with other risk elements or events. Various actors in the risk management process could, for example, be in charge of identifying and evaluating external risk factors (e.g. new laws are analysed by the compliance manager or the risk related to the applicability of mortality tables by the actuaries), whereas the interrelation of those risk factors with the operational processes will be analysed by 1st line operational management in the frame of their internal control process. A suitable cooperation between all parties involved in each risk area will allow organizations to understand and treat the transversal risks and their interactions throughout the silos of the organization.

As stated in Precept 8, operational management is in charge of the internal control of the business processes they are responsible for. They are the ones who best know the operational risks and control weaknesses related to the functioning of their process. Consequently, they will have a key role to play in the assessment of operational risks and risk factors for other types of risks.

When it comes to the evaluation and monitoring component of the risk management or the internal control process, the need for a high degree of independence of 2nd line of defence functions like the risk management function is however essential, as highlighted in CEIOPS' advice 3.209 : …*The embedding of the risk management function in the organizational structure of the undertaking and the associated reporting lines shall ensure that the function is objective and free from influence from other functions and from the administrative, management or supervisory body*.

The 3rd line of defence with the audit function will provide the independence the 2nd line of defence may lack given their interaction with the operational management in their monitoring task.

CEIOPS stresses the need to establish a risk management function, responsible for the *coordination across the undertaking of risk management activities*. (advice 3.211), whereas internal control is not defined (by Basel II and Solvency II) as a function.

In general terms, we support the idea that segregation of functions is necessary within the execution of the internal control and risk management processes whenever independent evaluation or reporting is to be conducted or risk of errors and omissions is to be avoided. On the other hand, given de transverse and interrelated aspect of most risk elements, knowledge and skills have to be gathered to provide organizations with the necessary level of control over their activities and obtain the vital confidence level from their stakeholders.

ICIB vzw/asbl
www.icib.org
02 305 35 25