Pillar 2
Operational issues of risk management

2011 was a crucial milestone for insurance companies on the path to Solvency II compliance.

April 2012

pwc

Contents

This PwC White Paper focuses exclusively on the challenges of implementing the new Solvency II requirements. It provides the insurance industry with a single concrete methodology and framework, complete with milestones, for adapting the principles of Pillar 2 to their organisations.

Foreword

This White Paper is being issued at a crucial point in the Solvency II regulatory calendar. The challenge of ensuring compliance with Pillar 2 – the cornerstone of solvency risk prevention – is becoming clearer. The initial work on Level 2 measures concerning the system of risk governance is in its final stages. The measures for Level 3 began in 2011 and accelerated towards the end of the year, despite the fact that from January 2011 the Omnibus 2 Directive allowed for transitory measures as well as a grace period under certain conditions and for certain points.

In this uncertain, but already well advanced, regulatory context, the priorities of the insurance industry are concentrated around Pillar 2, which involves the operational application of a risk strategy which is compliant with the Directive's principles and obligations. These new obligations go to the heart of business and organisational management. They also represent an opportunity for companies to optimise their operational performance. In this respect, the documented procedures of Own Risk and Solvency Assessment (ORSA) offer a path to groundbreaking management of solvency over a strategic horizon of three to five years.

PwC assists insurance companies in their projects and has worked side by side with them on risk management issues, including drafting the COSO 2-ERM standard. This White Paper is aimed at extending our contribution to compliance with Solvency II.

Paul Clarke
Global Solvency II leader

Jimmy Zou
Solvency II leader (France)

Overview

On the long journey towards compliance with the new Solvency II regulations, insurers (insurance and reinsurance companies, mutual insurers and insurance cooperatives) are at a crossroads: having thus far focused on the quantitative aspects of the Directive, referred to as Pillar 1, they are now turning towards the more complex qualitative obligations of Pillar 2.

"Through its cross-disciplinary approach, this White Paper clearly presents the key points of risk management and provides illustrations of potential situations. This document reassures us on our approach and gives fresh insight into certain operational strategies for Pillar 2 projects."

Christophe Raballan, Head of Risk Management and Internal Control, MAIF

In 2010, insurance companies concentrated on assessing their ability to build accurate risk models, based on the new framework, and to measure the impact of these requirements on the amount of capital required for the 1 January 2013 implementation. Companies have also recently finalised the QIS 5 exercises, which provided the opportunity to conduct a first dry run to test calculation methods and processes. During this phase, the final adjustments necessary to implement a process for drawing up economic assessments and calculating solvency capital requirements (SCR) were made.

In early 2011, the work concentrated on Pillar 2 of Solvency II, which required companies to challenge their own risk culture, define – or redefine as needed – risk governance and strategy and consider the operational implementation of the risk management function. As the keystone of the Directive is based on risk control, Pillar 2 compliance therefore raises many questions for insurance companies. These tough questions often strike at the heart of business management processes.

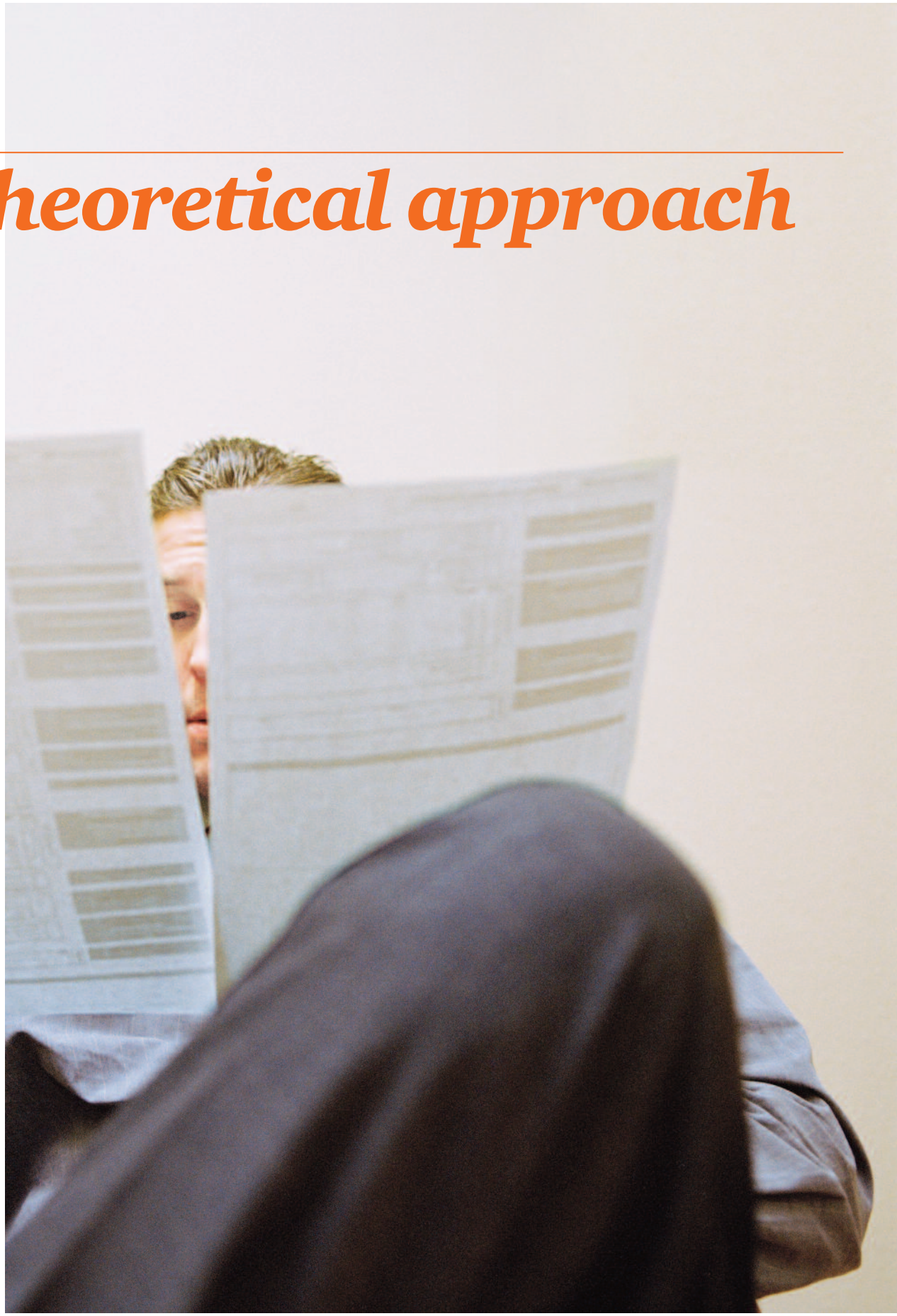
Questions you might ask yourself include: What exactly do Solvency II regulations require? How should, or how can, these provisions be applied to my company? What constraints and determining factors are used to configure an operational risk management system as accurately as possible? What are the specific sub-projects that fall under Pillar 2 requirements in my overall compliance project?

The main difficulty shared by all of our clients, which we address in this White Paper, is how to interpret and apply the regulations properly to individual companies in order to create a risk management process that meets the requirements in an appropriate and efficient manner.

This paper is designed as a toolbox for those involved in the organisational aspects of Solvency II compliance. Following a brief overview of the regulatory requirements and the ERM framework, we break down the operational issues involved in Solvency II compliance projects (risk management function, organisation and governance of the overall risk management processes, scoping of 'cross-business' projects such as data quality and ORSA). We also highlight the fundamental questions and, based on concrete examples, sketch out the main operational approaches to answering them.

As such, this paper is mainly directed at operational Solvency II compliance project coordinators, project managers and heads of risk. It should also provide useful information for the managers and directors of insurance companies. Currently many insurers face difficult choices in finding the right balance between compliance requirements (which can seem excessive) and adapting them to their company's internal environment (a strict compliance or 'best-in-class' approach to risk management?). We hope that you will find the guidelines developed below useful in your compliance work.

1. Theoretical approach



Introduction

Under Solvency II, all companies must demonstrate that they have implemented an adequate and efficient risk management system. The two main vehicles used are:

- The regulatory framework of Pillar 2 is the principal vehicle. Its provisions, outlined in a small number of articles in the Directive, cover regulatory requirements relating to the operational structure of risk management. These articles are further developed in implementing measures, some of which are currently under discussion.

- The technical framework, COSO 2[1] 'Enterprise Risk Management' or ERM, which is most often used to understand what effective risk management criteria are. Rating agencies have now included ERM performance as an evaluation criterion in and of itself.

In this report, we have provided a summary of the main provisions and concepts listed in these frameworks.

1 COSO stands for Committee of Sponsoring Organizations of the Treadway Commission, a non-profit commission which in 1992 established a standard definition for internal control and created a framework to evaluate its efficiency.

1.1 General provisions of Pillar 2

Pillar 2 covers all of the required risk management principles and practices relating to the risk and capital estimates covered by Pillar 1. The main provisions fall into the following four major categories:

Figure 1: The principal provisions of Pillar 2

Risk governance (Art. 41 to 49)

- General governance requirements (segregating responsibilities, managing conflicts of interest, etc.)
- Principle of proportionality of the risk system in relation to the complexity of the risk profile
- Definition of key functions in risk management and the scope of the risk system
- Fit and proper requirements for the main risk management roles
- Good conduct principles in terms of remuneration

New supervision process (Art. 27 to 39)

- A new supervisory review process based on permanent dialogue with the regulator and in which the company bears the 'burden of proof'
- The option of the regulator to sanction any quantitative or qualitative divergence from expected standards through 'capital add-ons'

Internal model (Art. 120 to 126)

- Requirement to show that the internal model is used effectively in monitoring (operational risk management, capital allocation)
- A concrete assessment based on nine principles (adoption by management, accurate reflection of risk profile, etc.)
- Internal validation process for the model...
- … and model sensitivity and stability tests.

Own risk and solvency assessment (ORSA) (Art. 45)

- A set of processes and procedures used to identify, assess, monitor, control and report internal and external long-term and short-term risks that an insurer faces or could face. These risks are used to determine the company's capital requirement to ensure its solvency at all times.
- The ORSA covers the regulatory requirements of Pillars 1, 2 and 3

Source: PwC

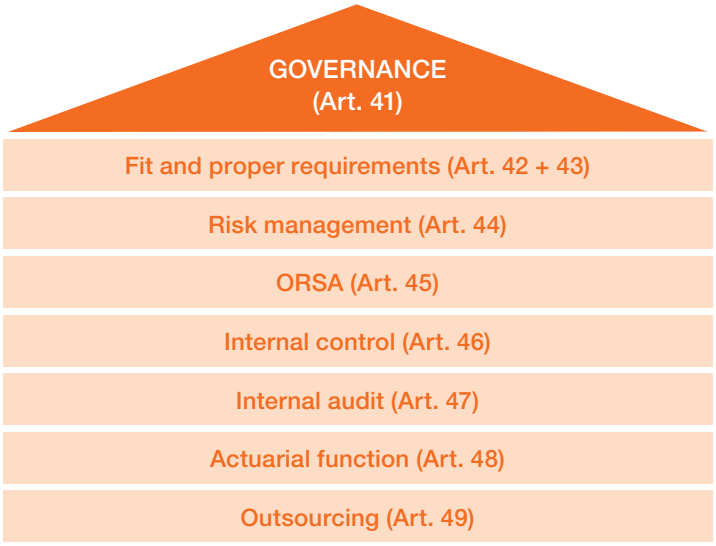
The main difficulty in getting to grips with Pillar 2 is that the articles and implementing measures define the underlying principles but offer no standards as to its practical application. These principles must be interpreted and adapted to apply to the internal environment of your organisation.

In light of this, we focus on the organisational aspect of Pillar 2, namely the governance issues for the risks covered in articles 41 to 49, and the Level 2 and 3 measures currently being defined and discussed between European Insurance and Occupational Pensions Authority (EIOPA) and the European Commission.

1.2 What does the Directive say?

The European Solvency II Directive establishes the ground rules for good governance as a complete system composed of functions and rules used by regulators and models for appropriate decision-making procedures. The system for risk governance (defined in Article 41) features seven main components, each with set expectation levels. These components are detailed in an article focused on the Directive, as illustrated below.

Figure 2: Risk governance



Source: PwC

Art. 41 – General governance requirements

Article 41 introduces the main themes developed in Articles 42 to 49, but above all emphasises that, "insurance and reinsurance undertakings [shall] have in place an effective system of governance which provides for sound and prudent management of the business."

Art. 42+43 – Fit and proper requirements

Article 42 stipulates that "all persons who effectively run the undertaking or have other key functions [shall] at all times fulfil the following requirements: their professional qualifications, knowledge and experience are adequate to enable sound and prudent managment (fit); and they are of good repute and integrity (proper)."

This information must be reported to the supervisory authorities in the event of any changes and must be documented.

Art. 44 – Risk management system

Article 44 states 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.

That risk-management system shall be effective and well integrated into the organisational structure and in the decision-making processes of the insurance or reinsurance undertaking with proper consideration of the persons who effectively run the undertaking or have other key functions."

Article 44 describes limits in the scope covered by risk management (underwriting, asset-liability management, investment, operational risk management, liquidity and concentration risk management, reinsurance and, in part, the internal model). It stipulates that these risk management policies must be documented.

To recap, the Directive:

- presents the risk management function (hereinafter referred to as the 'risk Function') as an efficient, mandatory function integrated into the organisation
- limits the scope of risks covered – notably risks used to calculate SCR, but not necessarily limited to just these risks
- describes the specific responsibilities of this function, acting as the overall 'conductor' for the system and 'pilot' for the internal model, if applicable.

Art. 45 – Own risk and solvency assessment (ORSA)

Article 45 states that as part of its risk management system, every insurance and reinsurance undertaking shall regularly "conduct its own [proportionate and documented] risk and solvency assessment" to determine the Solvency Capital Requirement risk measure and calibration.

ORSA essentially covers three major points:

- as applied, ORSA shows whether or not the risk management processes developed by the organisation are appropriate
- it is integrated into business strategy and is taken into account in the organisation's strategic decisions. Its analyses and reports are taken into account by decision makers
- the assessment can be performed following any significant change in the risk profile of the organisation.

Art. 46 – Internal control

Article 46 states that "Insurance and reinsurance undertakings shall have in place an effective internal control system [including at least] administrative and accounting procedures, an internal control framework, appropriate reporting arrangements at all levels of the undertaking and a compliance function."

Art. 47 – Internal audit

Article 47 stipulates that "the internal audit function shall include an evaluation of the adequacy and effectiveness of the internal control system and other elements of the system of governance… [and] shall be objective and independent from the operational functions."

Art. 48 – Actuarial function

Article 48 describes the actuarial function as an assessment function that aims to "coordinate the calculation of technical provisions; ensure the appropriateness of the methodologies and underlying models used as well as the assumptions made in the calculation of technical provisions; assess the sufficiency and quality of the data used in the calculation of technical provisions; compare best estimates against experience; inform the administrative, management or supervisory body of the reliability and adequacy of the calculation of technical provisions; oversee the calculation of technical provisions..., express an opinion on the overall underwriting policy; express an opinion on the adequacy of reinsurance arrangements; and contribute to the effective implementation of the risk management system..."

Art. 49 – Outsourcing

Finally, Article 49 informs us that "insurance and reinsurance undertakings remain fully responsible for discharging all of their obligations... [when outsourcing] functions or any insurance or reinsurance activities". The outsourcing of activities must not impact the governance system, business, operational risk or the ability of the supervisory authorities to monitor compliance.

Moreover, undertakings shall notify the supervisory authorities prior to the outsourcing of "critical or important" functions or activities.

1.3 What do the implementing measures say?

The Solvency II provisions concerning the organisation and risk governance system are based solely on the guiding principles. The regulators want each organisation to be responsible for determining its own organisational structure, and have therefore defined only key functions and very general requirements. To help interpret Articles 41 to 49, the regulators have, nonetheless, given some specifics.

These specifications on the risk management system are provided in the Level 2 measures in the document "Advice for Level 2 Implementing Measures on Solvency II: System of Governance" (from Consultation Paper 33), published in October 2009. Level 3 measures, currently in preliminary discussions, are based on the same architecture and are expected to clarify certain points, depending on the level of the regulators' requirements.

Essentially, under these requirements all companies which are subject to Solvency II must demonstrate that, in line with these principles, they have an operational system for managing and overseeing its risks which guarantees:

- a true understanding of the risks to which the company is exposed (risk profile) and a reasonable assessment of its exposure at any given time
- a real operational risk management mechanism, i.e., key components are in place, and each component can do what it is supposed to do
- reporting of required information and the ability of the regulatory authorities to make the necessary decisions.

Figure 3: A summary of the provisions

System of governance (SG 1, SG 2, SG 11, SG 13)

- A clear, robust and well-documented system to encourage efficient organisation
- Definition of conflicts of interest, 'four-eyes principle', documented fulfilment of fit and proper requirements for all key functions

Risk management (SG 3, SG 4, SG 7) (see focus)

- Clearly documented processes, procedures and policies
- A minimal scope of the 'risk areas' to be covered: underwriting, reserving, ALM, investments, liquidity and concentration, operational risk, reinsurance and other risk-mitigation techniques
- Responsibilities: (i) ERM architect and coordinator, (ii) producing aggregated risk profile, (iii) reporting on risk exposures and (iv) identifying and assessing emerging risks

Compliance function – internal control (SG 5 and SG 8)

- Reference to COSO framework (control environment, control activities, communication, etc.)
- Responsibilities: (i) compliance of operations, (ii) management of operational activities and (iii) reliability of financial and non-financial information

Internal audit (SG 9)

- An independent, impartial and stand-alone unit with expertise in all businesses and processes fully within its scope
- Requirement to issue an annual report based on an audit plan with a risk-based approach

Actuarial function (SG 10)

- Responsibilities: coordinating the calculation of technical provisions, assessing the appropriateness of data methods and quality, back-testing best estimates and providing management with formal opinions on the reliability of models (formal report)

Outsourcing (SG 12)

- Obligation to ensure that outsourcing does not negatively impact service quality or global operational risk exposure
- Formalised, comprehensive processes and policies covering all areas of an outsourcing project (selection, contract, monitoring, etc.)

Source: PwC

These provisions clearly form a minimal regulatory base. The principles are very broad: each organisation must specifically adapt them to its size, its expertise and the complexity of its risk profile. This is what is referred in the legislation as the 'proportionality principle'. However, the scope of this principle and the level of the 'leeway' allowed for different organisations currently remain unclear.

Focus on Level 2 measures

In the Level 2 text, Article SG3 gives EIOPA's opinion on risk management efficiency and provides the following advice:

a) **Risk management strategy** must be clearly defined and well documented. This strategy must set risk management objectives and key risk management principles, define the organisation's risk appetite and finally describe the roles and responsibilities of the risk management function across the company and in accordance with its business strategy.

b) **Risk management policies must be put in writing and adapted**. They include naming and defining the risks to which the organisation is exposed, classifying them by type and limits of acceptability. The risk management system must apply strategy, facilitate the implementation of control mechanisms and take into account the nature, scope and time horizon of the business and the associated risks.

c) **Risk management processes must be appropriate and procedures adapted** in order to identify, assess, manage, monitor and report risks.

d) **Risk reporting procedures must be appropriate** as must the feedback loops that ensure reporting. These procedures are coordinated and challenged by the risk management function and are actively controlled and managed by all relevant staff.

e) Reporting documents submitted to the above-mentioned bodies by the risk management function refer to the risks (potential or actual) associated with the business of the company and the operational efficiency of the risk management system.

f) Lastly, ORSA **must be adapted** to the company's activities.

Special case of ORSA

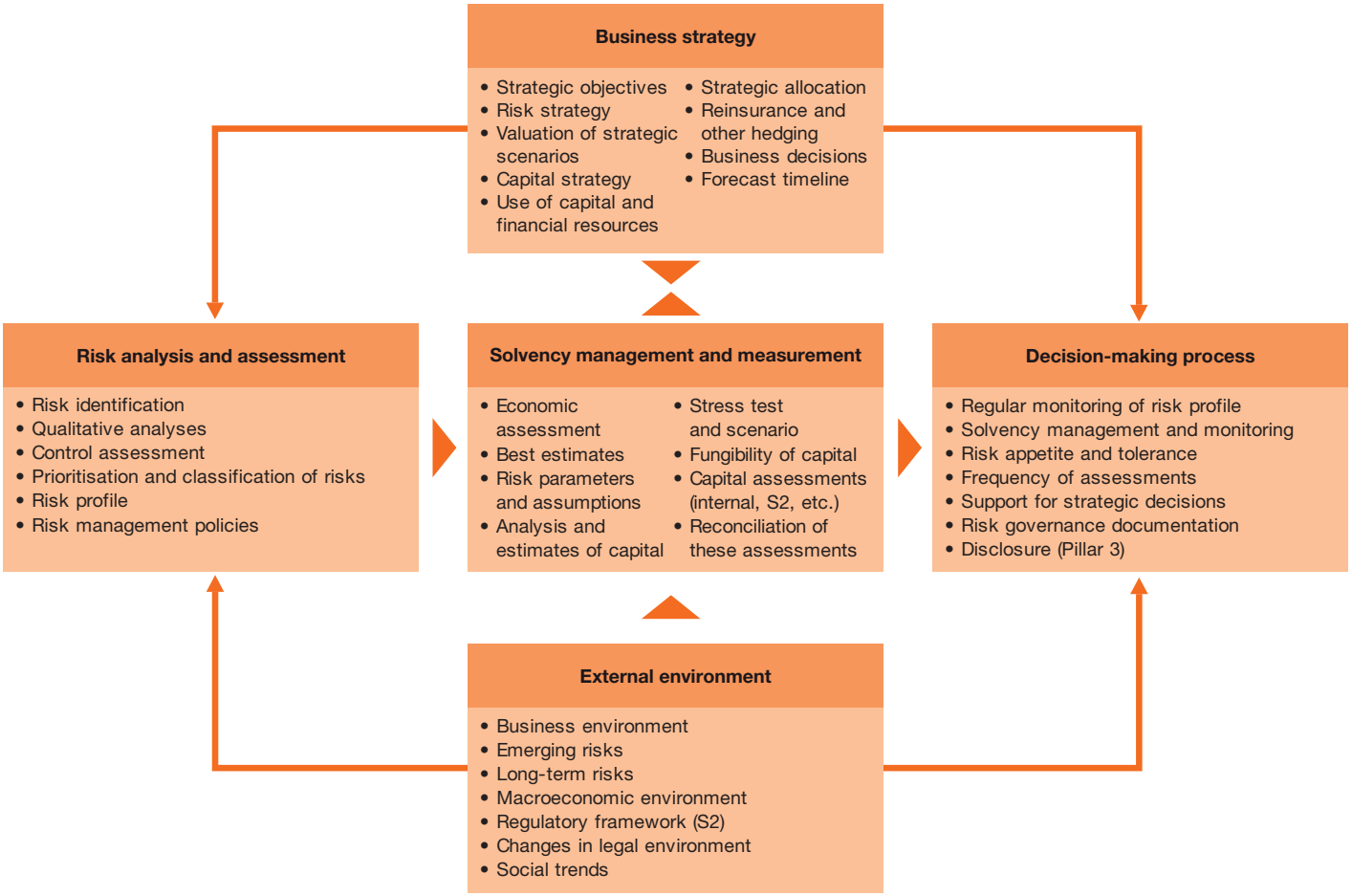
ORSA is a hot topic that was covered in the Level 3 measures that were addressed by EIOPA in the second half of 2011 as well as during a conference on Pillar 2, governance and ORSA held by the Autorité de Contrôle Prudentiel (Prudential Control Authority or ACP) during the second quarter of 2011.

Despite the importance of this process, Article 45 was not described in any text relating to Level 2 measures. CEIOPS published an Issues Paper entitled "Own Risk and Solvency Assessment (ORSA)" dated 27 May 2008.

As presented to date, ORSA is a process designed to ensure that the company is able to calculate and manage its risks and that its capital needs are met. However, certain characteristics should be highlighted. (see chart below):

- ORSA is the responsibility of senior management, in charge of overseeing the process and its results with respect to the regulator.
- It is a documented risk management process that must be submitted to the supervisory authority at regular intervals (at least once a year) and following any significant change in the insurer's risk profile.
- It is an integral part of the day-to-day management of the company (commercial policy, investment strategy, capital management, acquisition strategy …).

Figure 4: Risk management system



Source: PwC

- It offers a holistic and forward-looking approach to managing risk (risks used to calculate SCR and other risks – reputational risk, strategic risk, macroeconomic risk, political risk, etc. – to which the company is exposed over its strategic planning period, traditionally three to five years) across the full scope of the Group (all European entities and those outside the EC under the Group's supervision).

- It allows all organisations to show that they can raise the capital necessary to cover solvency requirements for the strategic planning period (as opposed to the one-year horizon used to calculate SCR).

- The risk assessment in the ORSA process represents the company's 'own' view of its risks, taking the risk modules identified in the SCR calculation, namely the difference in the number of risks identified, how they are measured, i.e., the confidence interval to which the formula is calibrated. Furthermore, the company may use either a standard formula approach or an internal model to assess its risk exposure. The methodology must be proportionate to the complexity of the company's activities and the types of risks involved.

"The main issue is knowing how to implement the key functions and a governance system that are compliant with the Solvency Directive and compatible with joint-management structures. The Directive draws mainly on concepts applicable to corporations and joint management entities as opposed to mutuals, which are based more on the principles of solidarity, compensation and retrocession."

Albert Cohen, Risk and Solvency officer, Réunica

1.4 COSO II – ERM

Background

The COSO framework on internal control was set out as early as 1991 and today is an international benchmark used by companies that want their internal control system to be up to standard. Since 2002 it is the framework used by international companies to assess their compliance with the Sarbanes-Oxley Act, which requires management to assess and report on internal control every year (Section 404/SEC Proposals – October 2002 – and ASB – March 2003), affirming "the responsibility of management for establishing and maintaining an adequate internal control structure and procedures for financial reporting".

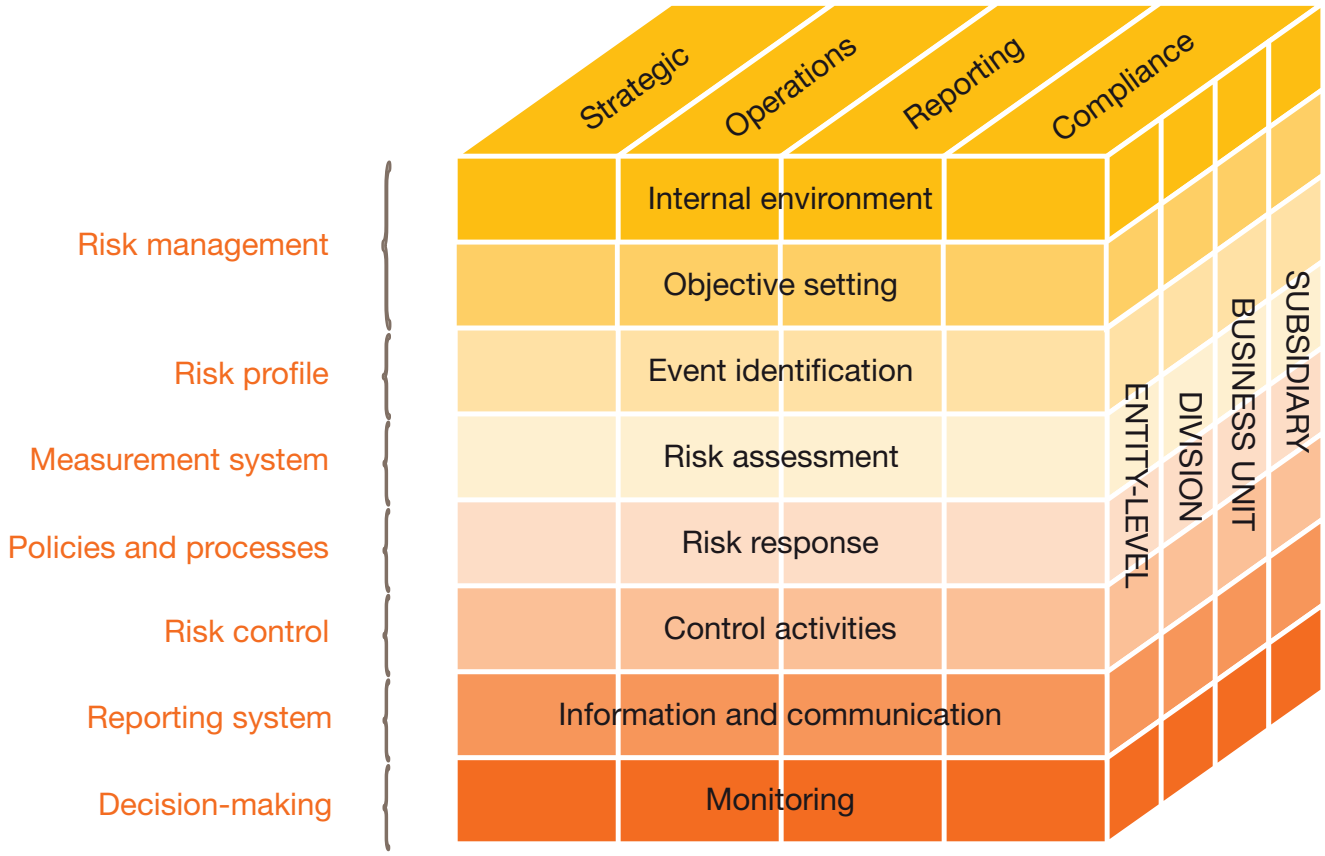
This framework is closely linked to the uncertainty and concerns raised by the corporate scandals in the early 2000s (Enron, Parmalat, Worldcom, etc.). It was originally designed to provide a standard for structuring internal control systems. However, it has evolved as companies have realised that the strict perspective of internal control was too limited and didn't allow for all possible risks to be understood and controlled. 'COSO II– ERM'[2] was introduced in 2004, broadening an approach that aimed to manage and secure operations through control measures including:

- an overview of all types of risk potentially faced by an organisation,
- establishment of different 'blocks' at work in global risk management, and
- the integration of risk management results into business management.

There is a direct relation between a company's objectives and the risk management components required to achieve them. The famous 'COSO cube' is a three-dimensional matrix that illustrates the relationship between these components.

2 COSO, "Enterprise Risk Management – Integrated Framework".

Figure 5: COSO II framework



Source: PwC

Presentation

A company's objectives (represented by columns) fall into four main categories: strategic, operations, reporting and compliance. The eight risk management components are the lines, and the entity units are the third dimension. This matrix shows how to approach risk management globally, by objectives category, component or unit or any combination thereof.

As illustrated above, the COSO framework is the underlying structure that supports the main concepts used by all those involved in risk management: risk strategy, risk appetite, risk profile, risk measurement, reporting on exposure, and so on.

The main purpose of the framework is to provide a way of integrating risk information into the enterprise's decision-making and strategic processes. By following this advice, any enterprise can manage its performance (according to the criteria it defines independently and specifically for its business) with respect to the amount of risk necessary to achieve it.

ERM can now be viewed as an operational process based on COSO II, providing decision makers (managers, directors) with reasonable assurance as to the management of risks actually taken in application of strategic objectives and within the limits of a globally defined risk appetite. It facilitates the management of uncertainty, risks and opportunities, the identification of events that could give rise to risks and the definition of suitable internal control solutions.

Since risk is the essence of insurance, one can immediately see the benefit of a framework that addresses the underlying principles and covers:

- The definition of strategic objectives by the decision-making bodies.
- The identification of risks resulting from the efforts made by the company to achieve these objectives – risk may refer either to threat in attaining objectives or opportunity to be pursued in order to achieve them.
- The implementation of an effective system for managing the exposure to these risks.
- The notification and reporting of risk exposure and failures to the relevant managers.

To integrate risk into management processes, risk management must 'permeate' throughout all the levels and processes of the enterprise.
The system is aligned with the enterprise's organisational model, which breaks down into the following components:

- The **strategic** dimension:
  How do decision-making bodies integrate risk into their processes? How do they define the limits of risk acceptability (i.e., what is authorised to achieve objectives, what is avoided or proscribed)?
- The **organisational** dimension:
  What functions are involved in risk management? What processes are used? How are these analyses related to solvency levels for insurance companies?
- The **operational** dimension:
  How does the undertaking implement risk measurement tools and resources so as to benefit from them fully? What are the reporting channels?

Conclusion

COSO II – ERM, designed as a standard and operational framework, provides the main elements and overall approach for a risk management process. Solvency II adds two specific organisational and business requirements. Insurers must specify the functions involved in their risk management and integrate risk and solvency assessment into their five-year business planning models using ORSA.

The great challenge of Pillar 2 lies in assessing how to interpret, adapt and implement these frameworks within an organisation. In order to be successful, they must be fine-tuned, correctly calibrated and adapted to the specific characteristics of your business, the complexity of your organisational structure and your 'risk culture'.

2. Operational implementation

Introduction

Not all companies place the same importance on risk management. Their choices naturally differ given the heavy investment required to set up an overall risk management process, compliant with the principles and obligations of Solvency II. These choices are difficult to make and objectify, involve top management and must be made in the context of the business' overall strategy.

Our goal here is not to provide a 'magic formula' that solves the challenges you face in implementing your Solvency II projects. Instead, we list the key factors that will determine your choice of structure aligned with the three key dimensions of the compliance programme.

They are:

- Calibrating/fine-tuning the overall structure of the risk management process.
- Implementing the risk management process.
- Overseeing the key cross-business projects.

2.1 Defining the risk management system

The integration of a risk management framework into a company that has a long history of processes, expertise, habits, styles and decision-making bodies is a complex task. Given the extent of the changes and the length of time some established practices have been in place, implementing a risk management process requires complete involvement from all players concerned (first and foremost senior management) throughout the process.

If the main 'new' concept consists of development or implementation of a risk management function, Solvency II projects now go as far as defining organisational structures for the entire risk management process, encompassing all of the functions, processes and bodies involved in risk management.

Our experience has shown us that to do so, five main questions must be answered:

Figure 6: Risk management process

1	**What are the organisational building blocks in the system?**	• What organisational building blocks fall within the scope of the risk management function: Risk management? Actuarial function? Compliance? IT system security?
2	**What should be the scope of the risk management system?**	• What functions have a key role in risk management? • What are their responsibilities (control, monitoring, reporting, etc.)?
3	**How are the different functions coordinated?**	• How are prerogatives coordinated between central and local risk functions, particularly at foreign sites? • What delegation rules should be put in place?
4	**How centralised should the risk management system be?**	• Exactly how should responsibilities be broken down between the risk management function and business functions in respect of key risks (ALM, investment, technical issues, etc.)?
5	**How should the added value of ERM be measured?**	• What fundamental indicators govern the risk/return trade-off (ROE, SCR, MCEV, etc.)? What criteria concretely reflect risk appetite?

Source: PwC

The answers to these questions are determined by complex constraints, which may be regulatory (Solvency II), external (ratings, etc.) or internal (goals, organisation, etc.).

2.1.1. The 'organisational building blocks' of the system

It is essential to recognise and define the scope of functions involved in risk management. In fact, it is not simply a specialist area; its management involves every level of the company. At each level the system must integrate the different elements: operational risk-taking, coordination of risk-taking and supervision of risk-taking.

The 'three lines of defence' model provides a useful framework within which these various functions and elements can work together.

- Front Office business staff have primary responsibility for the risks they take, and risk management practices and processes in place at this level constitute the 'first line of defence'.

- The 'second line of defence' is held by specialised risk management functions. Their role is to design, coordinate and manage a consistent framework for taking risks, but without being directly exposed to business risk. This covers the key functions of risk management as defined by Pillar 2 (risk management, internal control and compliance).

- The regular, independent, risk-based audits performed by the internal audit function provide reasonable assurance as to the pertinence and correct operation of the system. This is the 'third line of defence'.

Building on this framework, companies generally define the main principles for coordinating the different strata involved in taking risks, as illustrated overleaf. The organisational diagram most often defines responsibilities at each step in the risk management process. These principles then serve as a basis for assigning specific risk management roles and responsibilities in accordance with the risk profile.

Figure 7: Three lines of defence

	First line of defence		Second line of defence	Third line of defence
	'Operational' functions	'Specialist' functions	'Risk' functions	'Assurance' function
Scope	**All functions** (IT, HR, Finance, Production, etc.)	- **Actuarial/Technical Dep.** - **ALM/Investment Dep.** - Other (underwriting, etc.)	- **Risk management** - Internal control, compliance, etc.	**Internal audit**
Principles and standards	N/A	Proposes	Reviews and approves/ proposes	Carries out independent, empirical reviews on: - appropriateness of systems - their correct application
Implementation	Applies	Proposes/applies	Coordinates/applies	
Controls	Applies/proposes	Applies/proposes	Supervises, consolidates, analyses	
Reporting	Produces	Produces/analyses	Consolidates, analyses, manages	
Action plans	Applies	Proposes/applies	Approves and manages/ applies	

Coordinator role/operational role

Source: PwC

Two challenges often arise when implementing these principles:

- The risk management function may have different responsibilities depending on the type of risk. Acting as a coordinator, it may take on direct responsibility in certain areas such as operational risk. These details are outlined in the analysis of the risk function's position (see below).
- Internal audit has a special role in the system that is often difficult to position. The provisions of the Solvency II Directive place great emphasis on the independent nature of this function. Its resources must be free of any other operational responsibility. According to the Institute of Internal Auditors, the purpose of internal control is to independently provide management with reasonable assurance as to the pertinence, quality and appropriate application of the risk management system. It is easy to understand why this function must be independent in order to establish its own approach (based on its perception of risk) and express opinions free of any outside influence.

2.1.2. Scope of the risk management system

Solvency II places the risk function at the core of the risk management system. Regulations define responsibilities and a scope of minimum risks on which the function is based. If a company uses an internal model, the function is in charge of designing, testing, implementing and monitoring the performance of the model, either in part or in totality. Most companies naturally launch Pillar 2 projects by putting in place or reviewing the positioning of the risk function. It is in charge of overseeing all risk management processes (see above), even if it does not directly carry out the operations, analyses and calculations required in this process.

The reference for defining the risk profile

When a risk function is set up, its first task is to identify the risks to which the company is exposed. Although each company faces its own specific set of risks, defining a risk profile follows a few best practices.

The first involves the scope of risks, which must be identified in the risk profile:

- It must cover at least the basic risk modules used to calculate capital requirements, whether determined based on a standard formula or an internal model, namely underwriting, market, interest rate, operational, etc.
- It is not, however, limited to just these risks, as they are too limited to give a true picture of the actual risk profile. The risk function must identify other risks that are specific to the company, taking account of all its subsidiaries and businesses (not necessarily insurance alone) as well as specific risks related to the company's structure.

The risk function must also bear in mind that this risk profile is not merely an inventory of all the potential or actual risks:

- Based on its analyses and the points of view covered, it prioritises the risks that must be monitored. Its added value lies in its ability to provide a 'shortlist' of risks that justify investing in measurement, monitoring and permanent supervision, based on the company's business objectives.
- As such, this management tool is developed by combining the 'risk philosophy/vision' of operational staff (a bottom-up approach to risk management based on the comprehensive identification of risks) with that of management (a top-down approach whereby investment in risk management is justified and prioritised).

Finally, the risk function ensures that an operational risk management system is in place and that it covers all the risk profile components. Each risk must be assigned to a risk 'owner' who is the 'subject matter specialist' available in the company: i.e. actuarial department for underwriting, certain counterparty and reinsurance risks, asset management for market and credit risks, and so on. Assigning a risk owner is the first step in implementing an operational risk management system. The components in the risk management process are set out below in section 2.2.

The evolving risk function under Solvency II

Above and beyond the purely technical aspects, companies have enhanced the risk function's 'right of inspection' in operational decisions. This notion fully covers the risk department's prerogatives in terms of processes, policies and risk-taking for which it is not the leading expert. In reality, the risk function's involvement is in line with the strategic priority associated with the risk:

- A company may take a conservative approach to risk, its priority being not to compromise the protection offered to policyholders and to ensure performance. In this case, the risk function would take on an advisory role, assisting operational managers in their processes and associated risks. It has little (or no) latitude to block decision-making processes.

- A company may decide to base its value creation on managing the risks it takes and the impact of these risks on its strategic variables: market consistent embedded value (MCEV), market capitalisation, economic capital, etc. In this case, the risk function takes on an essential role in operational decisions. It is a full stakeholder in these processes, is consulted for all important decisions and issues a formal opinion. It may have the power to block decisions (which in turn requires an arbitration process). These companies almost systematically use an internal model that is integrated into their strategic and operational decision-making processes.

Companies gradually advance along the ERM maturity curve between these two ends of the spectrum. As the ERM process develops, the positioning of the risk function evolves:

- The position of the risk function tends to rise within the company's hierarchy. Nowadays it is increasingly attached to upper management, indicating an understanding by them of the importance of the ERM in insurance companies.

- The role of the CRO is evolving. Often seen initially as a conservative and technical profession, it will gradually develop into that of a business adviser who works with decision makers. With a unique understanding of the risks taken by the company and how they interact, a CRO can offer advice on how to create value.

- The resources required to take on these functions have grown sharply. Risk departments were initially set up to meet successive regulatory requirements (anti-money laundering, anti-fraud and so on) but have since developed into more refined structures, most often broken down by types of risk (operational, technical, economic capital, etc.). These resources are more numerous, more highly qualified and more specialised.

"Implementing Solvency II, and particularly Pillar 2, will require greater coordination between all participants in risk management. The process will draw on existing management rules, which themselves will need to be strengthened. The resulting discipline will create growth opportunities and strengthen relations with customers, while guaranteeing all stakeholders (employees, shareholders, customers, etc.) improved control of risk and its impacts on business structure."

Ronan DAVIT, Head of Risk, Euler Hermes Group

2.1.3. Coordinating different functions involved in risk management

Once the basic components of the system have been identified and calibrated, the challenge for the risk function is to promote the implementation of an efficient risk system underpinned by clear, shared decision-making processes. To do so, the risk function has two main levers.

The definition of the roles and responsibilities for the principal risks

To do so, the risk function moves on from establishing the risk profile to coordinating the roles and responsibilities for each of the risks included in the profile. The main challenge lies in the diversity and heterogeneous make-up of the risk functions and risk owners. Risk departments must first harmonise the various risk management solutions proposed.

While the three lines of defence model outlined above provides a general framework in this regard, this harmonisation process must be specifically adapted to each risk in the profile. It is therefore necessary to:

- Map the appropriate functions to handle this risk: businesses, support, management or governance, etc.
- Pinpoint the best subject matter expert within the company to manage this risk (generally the risk owner identified in the system implementation phases upstream).
- Clearly define the roles and responsibilities of each player involved in the process. Close attention should be paid to the support functions' power to block processes (typically the risk function) as opposed to the relevant operational functions. The notion of 'right of inspection' for operational decisions should be specifically defined. This right in turn requires the establishment of a clear arbitration process in case of a conflict between the risk department and the business line concerned.

The matrix below is an example of the types of roles and responsibilities involved, offering a simple method for establishing a clear distribution of roles.

Figure 8: Investment management roles and responsibilities matrix

	Investment management
Responsible (ultimate responsibility)	**Board of Directors** (through the risk committee): takes responsibility for global supervision **General Management:** approves and monitors investment policy
Implementer (oversees operational implementation)	**Investment Department:** submits strategic allocation plan for validation, defines tactical allocation specifics, monitors implementation
Consulted (opinion requested systematically, published and taken into account in the decision)	**Risk Department:** issues an opinion on the Group's and the entity's total exposure to market risks and overall solvency level. If it issues an unfavourable opinion, the case is submitted to the executive committee for arbitration
Informed (regularly informed of new management decisions)	**Cash Department** (Financial Department): informed of all changes in investment policy, receives a copy of all investment flows

Source: PwC

The implementation of a decision-making architecture

Even the best-designed risk management system will only be efficient and effective if an operational decision-making architecture has been codified. It must ensure first that all useful information is reported to the appropriate committees and other decision makers in a timely manner. Second, it must ensure that these bodies review the issues at hand and make the necessary decisions. The company is then in a position to continuously manage its risk exposure and react promptly to any unexpected deviation in its risk profile.

The structure of the decision-making process is specific to the culture of each company and is in line with its position on the ERM maturity curve. However, the review or implementation of the decision-making architecture follows several key steps:

- Define the key organisational levels in risk decisions, which often correspond to the company's main decision-making levels (executive committee, key functions in risk-taking, operational staff, etc.). They are defined in line with the roles and responsibilities identified for each type of risk in the risk profile.
- Prioritise the types of risk that require formal supervision on a regular basis. The company must formally define the responsibilities required at each organisational level in line with these priorities (global supervision, definition of practices, monitoring and reporting, etc.).
- Design ad hoc decision-making bodies at each level: type of committee, members, voting rights, assignment of roles, meeting frequency.

As such, the structure of the company's system of committees can be consistent throughout, as illustrated in the example below:

Figure 9: Committee matrix

Source: PwC

The close relationship between risk management and risk control

One of the main lessons learnt from the financial crisis (notably the Kerviel case) is that efficient risk management requires coherent and consistent operational coordination between:

- the definition of major risk policies and processes (primarily by the risk department), and
- the appropriate application of these policies and processes by the relevant entities (operational functions, internal control, etc.).

Historically, most insurance companies have developed internal control approaches that are often granular and always complex. These approaches aimed to identify and to manage the risks specific to certain processes or operational areas, namely: reliability of financial reporting processes (SOX projects), security of information systems, anti-fraud or anti-money laundering processes, etc.

This work has led companies to focus specifically on operational risk management. The primary role of internal control (or permanent control) is to ensure the appropriate management of the company's processes and operations and the reliability of financial and non-financial information produced by the company. At the time of writing, work has begun in this area but has seen little or no application among insurance companies: operational risk is difficult to understand, differs completely for each company and is not specifically defined in Solvency II. Furthermore, SCR calibrations for operational risk produce negligible capital requirements, further inciting companies not to invest in a complex system to manage this risk.

Some market players are currently implementing specific procedures for operational risk analysis and risk – control coordination. The main ones include:

- **Gradual merging of risk and control functions** under the responsibility of a single function (most commonly the CRO). This ensures greater consistency between initiatives that were sometimes fragmented in the past. The primary focus is often on compliance, raising the question of whether operational risk is best managed by legal professionals (regulatory watch) or internal control (integration of legal provisions into operational processes). The trend clearly seems to be to: (i) appoint a compliance officer to take charge of defining the company's main compliance issues and coordinate the application of the relevant legal provisions while (ii) maintaining the legal department's responsibility for legal monitoring, setting up a body that meets regularly between the two departments. Broadly speaking, companies tend to put their risk management function in charge of supervising both the effectiveness of their ERM framework and the appropriate application of its provisions.

- **Definition of the operational risk system.** First of all, operational risk must be defined. This analysis generally reveals that operational risk covers any factor that could compromise the achievement of the objectives of operational processes (see the list of risks defined by Basel II) or the appropriate application of risk policies as defined by the company. Some companies have taken this a step further: given the sheer volume of operational risks, they have prioritised the critical areas of exposure and focused their efforts to deploy management systems in these areas.

- **Modelling of operational risk.** Some companies have implemented data collection systems for operational losses. These systems are used to assess the company's real exposure to operational losses, set up a more coherent management system or even to save on capital requirements. To be effective, however, the system's parameters must be determined (e.g., by clearly defining an operational loss and the minimum loss amount for data collection) and cover an adequate historical period. Results are deemed significant after three to five years of collection.

2.1.4. The extent of centralisation of the Risk function

Insurance groups are faced with a major operational difficulty: the operational scope of the risk function. How do they integrate such diverse entities and businesses that are not necessarily related to insurance (asset management for complementary pension or social security plans, healthcare and assistance services, strategic investments, and so on.) into their analyses and processes?

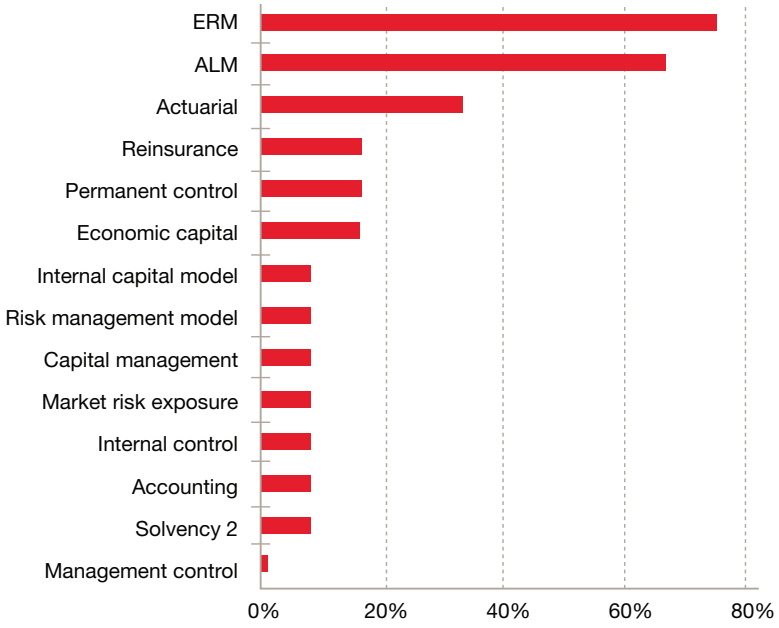
Although most companies are still trying to establish an efficient way of coordinating the risk system across their different entities, the following best practices have emerged:

- Aligning risk management process with the organisational and decision-making structure within the group that is already in place. In a highly decentralised group, the different entities or subsidiaries often have a local risk function that reports to their general management but falls under the responsibility of the group's risk department. In a more centralised group, the group risk department oversees legal entities. It may apply the principle of subsidiarity that determines the entities' leeway, and in this case a 'risk representative' is appointed. In either configuration, the risk function is a network-based structure.
- Groups, when dealing with all of their insurance entities, tend to require consistent reporting principles and structures that are defined and supervised locally. This applies especially to international groups with foreign subsidiaries or entities in countries not subject to Solvency II. Most often they opt for double reporting, with one set of reports prepared based on local prudential standards while another is submitted to the group in 'Solvency II format'.

There are often overlapping principles on the structure of the risk management process, as illustrated in the diagram below.

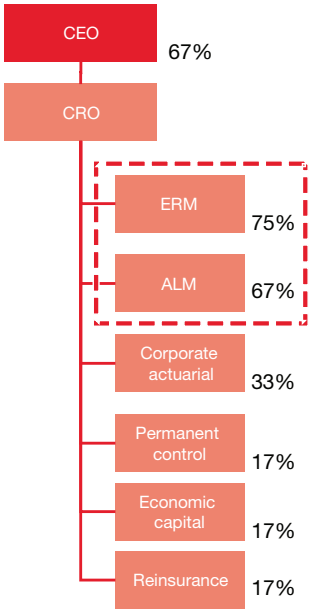
Figure 10: PwC Risk function benchmark

Principal responsibilities of the CRO



Based on the benchmark study conducted with 30 of the most important companies in the insurance industry (insurance companies, mutual insurers and pension funds)

Possible organisation chart of risk function



Source: PwC

That being said, there is no standard structure that is widely shared, especially with regard to the extension of the risk function to non-insurance subsidiaries.

In some cases, the problem has more to do with difficulty in adhering to the principles of independence in relation to the operational function. Many companies have also tried to 'force' their risk function beyond the strict minimum regulatory requirements. In fact, this function is supposed to become more centralised but not all of the issues at stake are necessarily evident in the beginning. Therefore these companies have added the more 'traditional' functions to the risk function, giving it more substance and importance.

The solutions seen are most often based on the principle of subsidiarity: the subsidiary has considerable autonomy in managing its risks, and the group only covers the few types of maximum losses that can be generated by the subsidiary (notion of 'subsidiary risk').

2.1.5. Measuring key indicators of the risk management system

In working with general management, one of the most fundamental roles of the Risk function is to define the key metrics of risk management. The choice of these indicators shows the importance the company gives to efficient risk management in its overall strategy.

This process is part of the establishment of risk strategy, as described in the next section. However, before beginning, the benchmark metrics must first be defined. They must feature certain characteristics:

- They reflect the main aspects of the risk/return trade-off offered to stakeholders (ROE, service quality, security of protection, etc.). They can measure the entity's resilience in some extreme cases (i.e., distribution tails) but remain realistic and always incorporate the notion of performance (profitability, etc.).
- They are easily measurable, i.e., the cost of implementing the calculation and management infrastructure is not prohibitive (especially if it is based on processes that are already in place) given the added value of monitoring.
- They are clear and understandable for those in charge of monitoring them. It is therefore essential at this point to define or validate them with management bodies, ensuring that they understand them and do in fact want to have these management indicators in place.

In most cases, however, companies may use a very limited number of 'fundamental' indicators to support their ERM approach. Their approaches generally combine:

- an **income indicator** such as pre-tax net income
- a **value measure** such as MCEV
- a **solvency indicator** such as the SCR coverage ratio or economic capital.

2.2 Implementing the risk management process

The risk management process can be simplified and broken down into the steps presented in the diagram opposite. Each of these steps features a certain number of components. The purpose of this section is to examine these components, identify the main issues involved and their operational application and provide concrete examples of their application.

Figure 11: Steps for implementation of risk management processes

Source: PwC

2.2.1. Defining the risk framework

Articles 44 and 45 require the company to demonstrate that it has implemented an adequate and efficient risk management system that includes a clearly defined and documented strategy for managing and monitoring its risks. The Directive also requires the establishment of a clearly defined relation between risk and return objectives in this risk strategy.

Components of a risk strategy

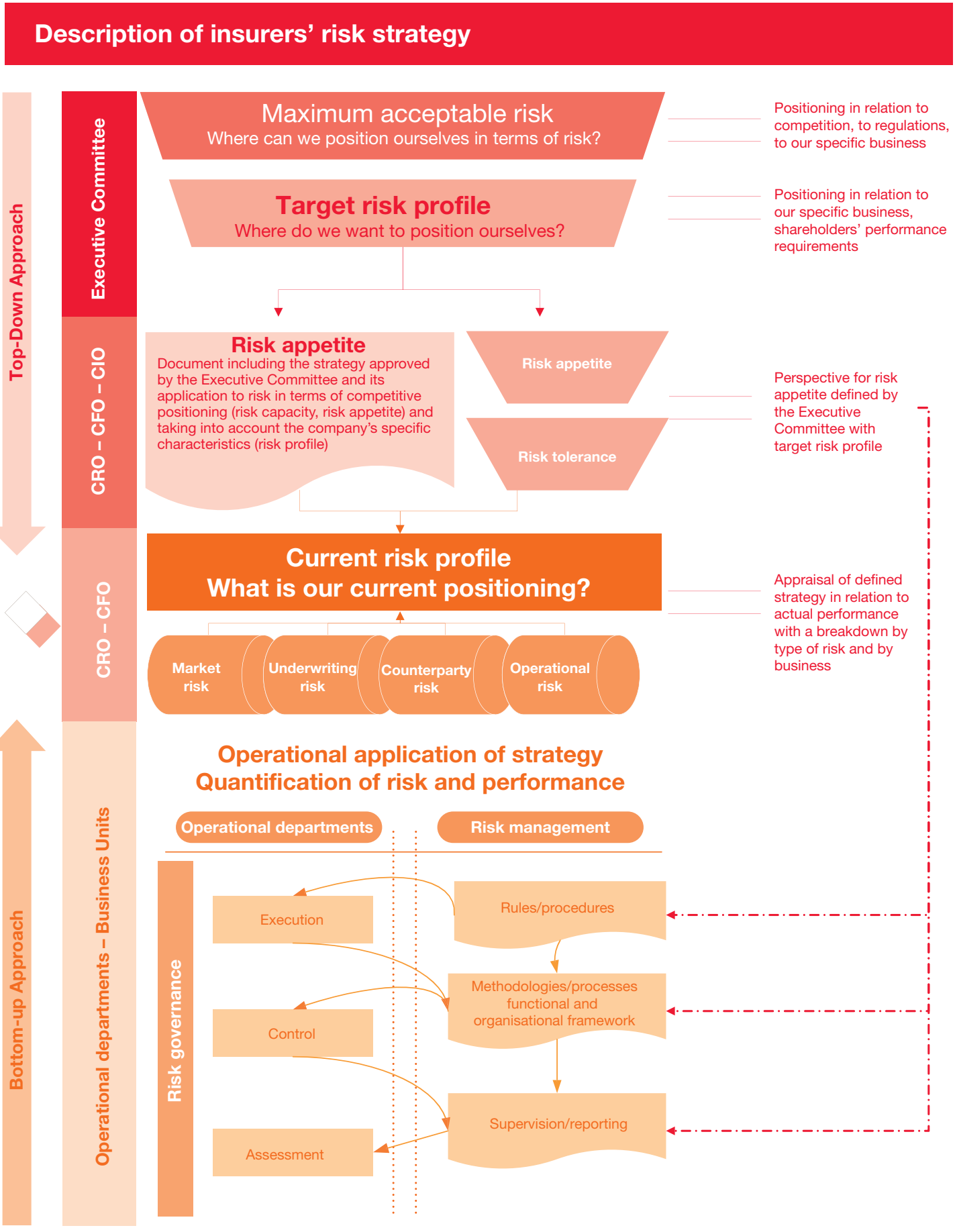
The risk strategy provides the means to define the accepted framework for risk management. The benchmark metrics applied to risk management are pre-defined, as indicated above. A risk strategy approach is based on five key concepts:

- **Risk appetite** represents the aggregate level of risk (i.e. at Group level) that a company is prepared to take in pursuit of its business and its development. It is a maximum threshold that is declared by management and is expressed in the form of the accepted deviation of the company's key aggregates from the desired outcome.
- **Risk tolerance** represents the level of risk that a company is prepared to take in pursuit of its business and its development pertaining to a limited scope. It is a distribution of risk appetite at a more specific level. It can be adapted to both broad risk categories and entities or geographical scopes.
- **Risk limits** are defined as the operational limits in line with the risk budget and/or risk appetite. These limits are specific to the processes with which they are associated.
- **Risk profile** is the measure of risk exposure expressed in the form of a reaction of key financial aggregates to a shock in an underlying variable. It is measured for a given scope on a given date. It can cover a very limited scope, such as the mortality risk for a specific product at a given subsidiary, or it can apply to all possible aggregation levels for the company's entire scope.
- The **risk budget** measures the anticipated level of risk exposure for a specific timeframe within a given scope. It measures the risk profile for a company's forecast, with identical levels of granularity.

Risk strategy not only determines the framework within which risks may be taken, but also the terms under which these general principles apply within the entity. It defines the budgets and targets adapted to the company's willingness to take risks in line with the defined risk strategy.

In coordinating the different components of risk strategy, a totally integrated asset-liability management model is also defined. This strategy is primarily defined through a top-down approach (i.e., defined by management), along with the contribution of reporting from operational staff (bottom-up approach):

Figure 12: Description of risk strategies in the insurance industry



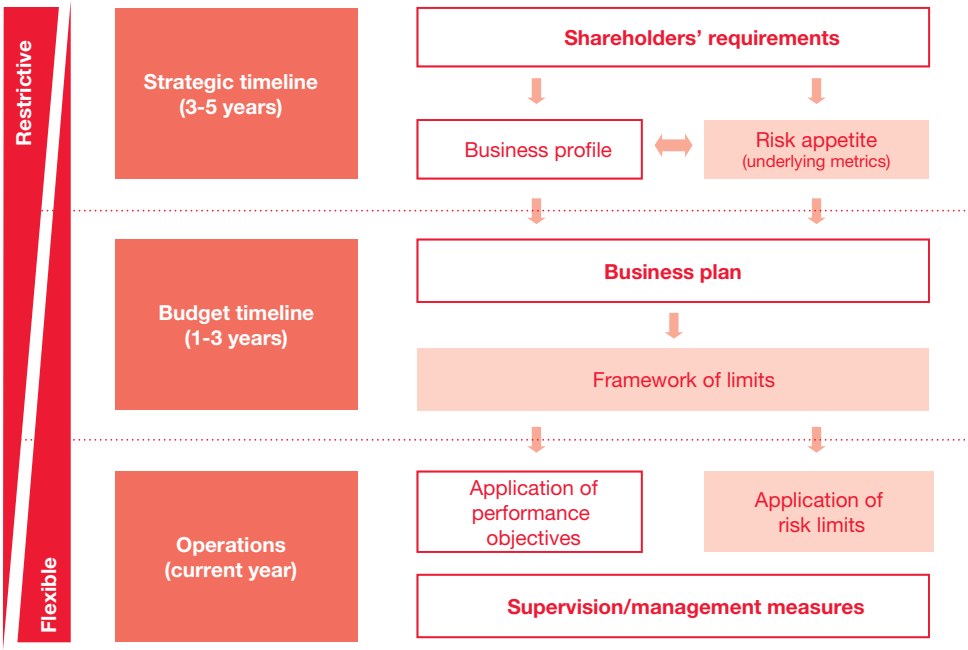
Source: PwC

Application of risk strategy

A general strategy based on results or solvency metrics is not sufficiently specific to provide useful operational guidelines for risk takers. Applying this strategy to operational risk limits is therefore crucial to the implementation of this strategy.

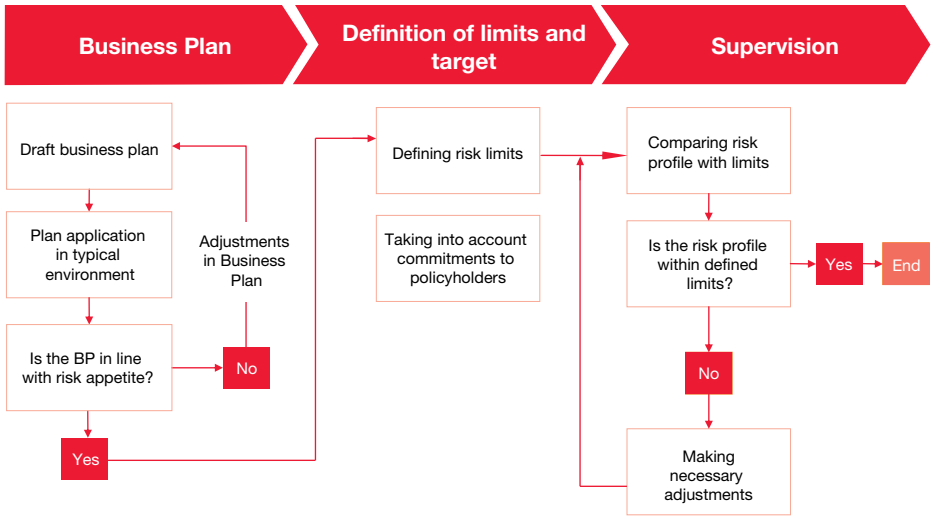
Management involvement is of prime importance. The different stakeholders (shareholders, market, clients, rating agencies, etc.) and their respective requirements must be mapped out. Understanding these requirements is the first step in defining the company's risk strategy and applying it to a system of operational limits.

Figure 13: Breakdown of risk strategy



Source: PwC

Figure 14: The budget process



Source: PwC

For smoother integration of risk strategy content into decisions, the budget process must also be updated to include assessment criteria that take into account the amounts of risks incurred.

2.2.2. Identifying and measuring risks

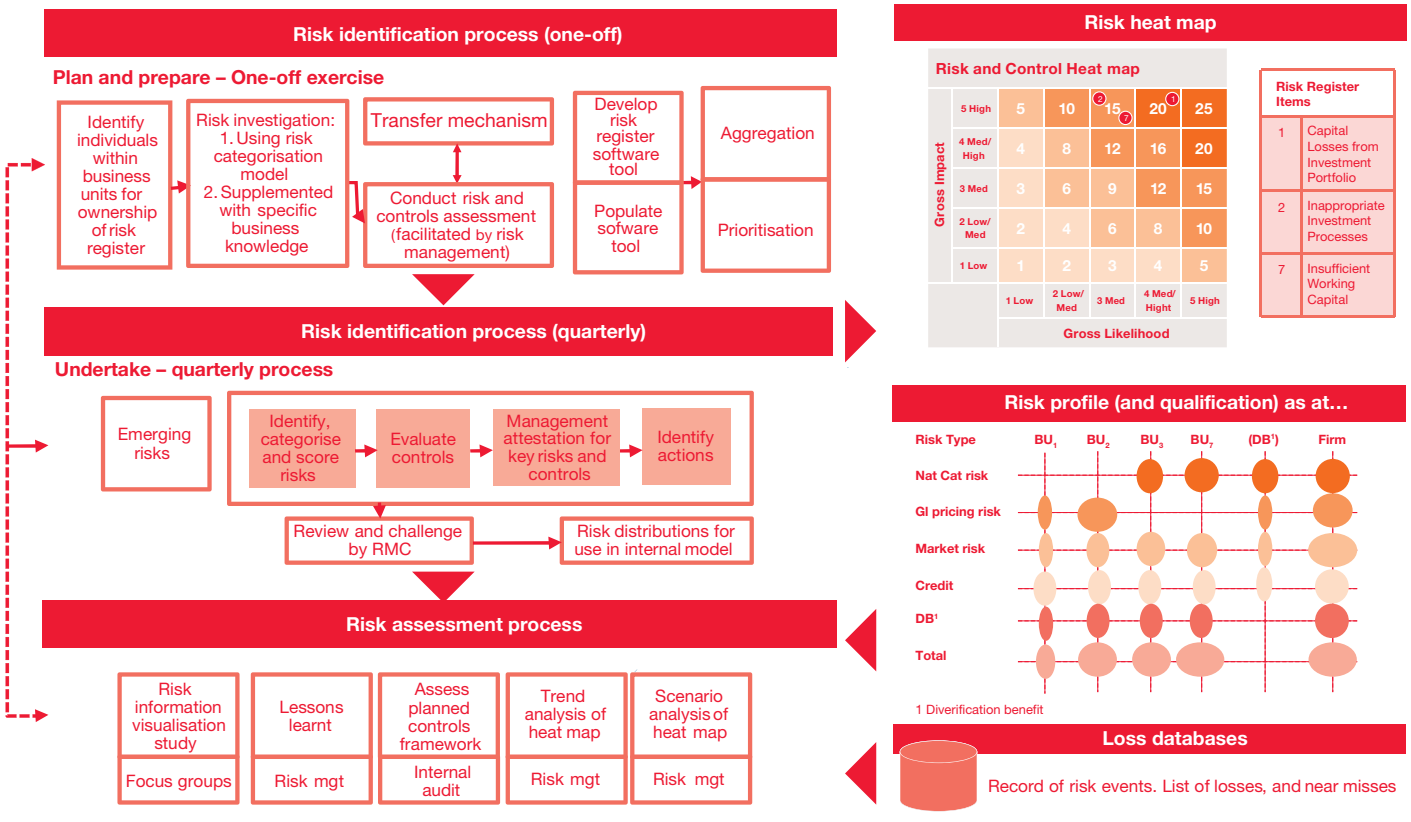
Identifying risks applicable to the business

A robust risk identification system must be able to predict all risks and align them with the company's major risks in order to understand the causes and interdependencies. It must be regularly updated following any significant change in the risk profile.

The risk identification system (see diagram below) includes two main components:

- A risk map (or 'heat map') that is used to classify risks according to their potential financial impact and their probability of occurrence. Financial impact and the probability of occurrence must be assessed in the same way throughout all operational entities (same risk taxonomy and calibration of impact) and for all types of risk. Equally important is the efficiency of the collection and update procedures for risk data (loss databases).
- A list of major risks that must include the few large-scale critical risks to which the company is exposed. Large-scale risks are those that could lead to bankruptcy and require in-depth analysis in order to identify their key components (causes, scenarios, impacts, etc.).

Figure 15: System for identifying risk



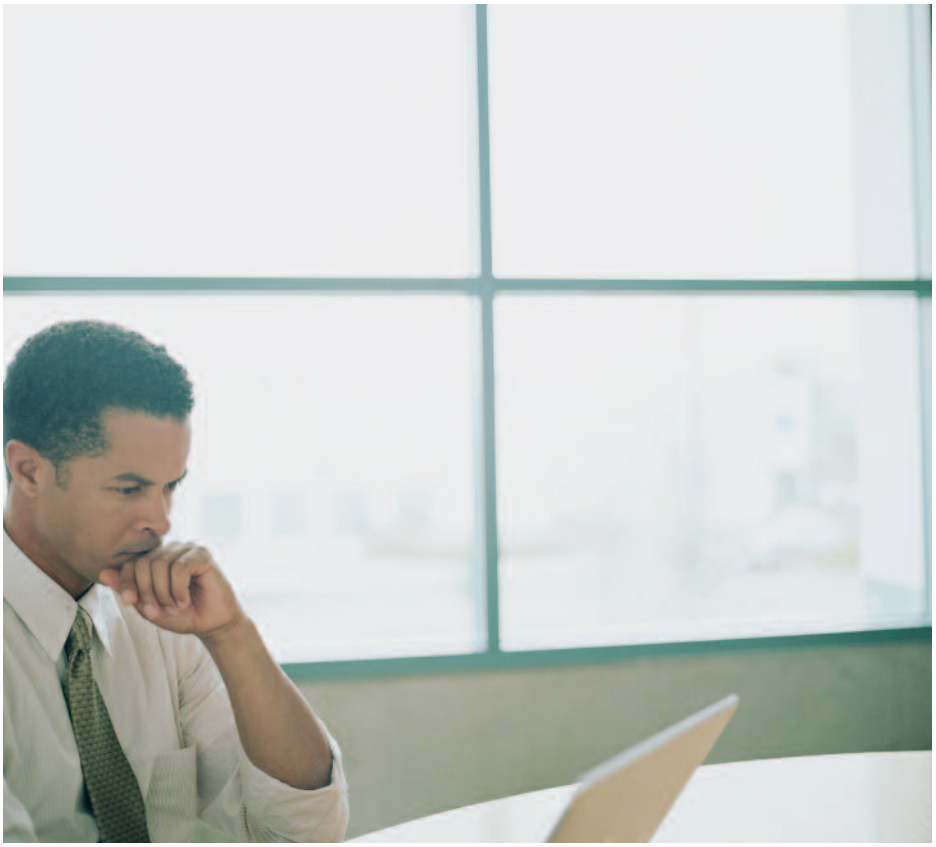
Source: PwC

Risk measurement systems

Risk measurement methodologies are covered by Pillar 1 of Solvency II in the standard formula that defines the modelling principles for technical provisions using best estimates and requirements for calculating SCR (risk module, shocks to be applied, correlation matrix).

Companies may also use an internal model that best reflects their specific risk profile. An internal model can apply the same base to a number of uses, ranging from solvency requirements to embedded value, asset-liability management, profit-testing when creating products, risk appetite or even ORSA.

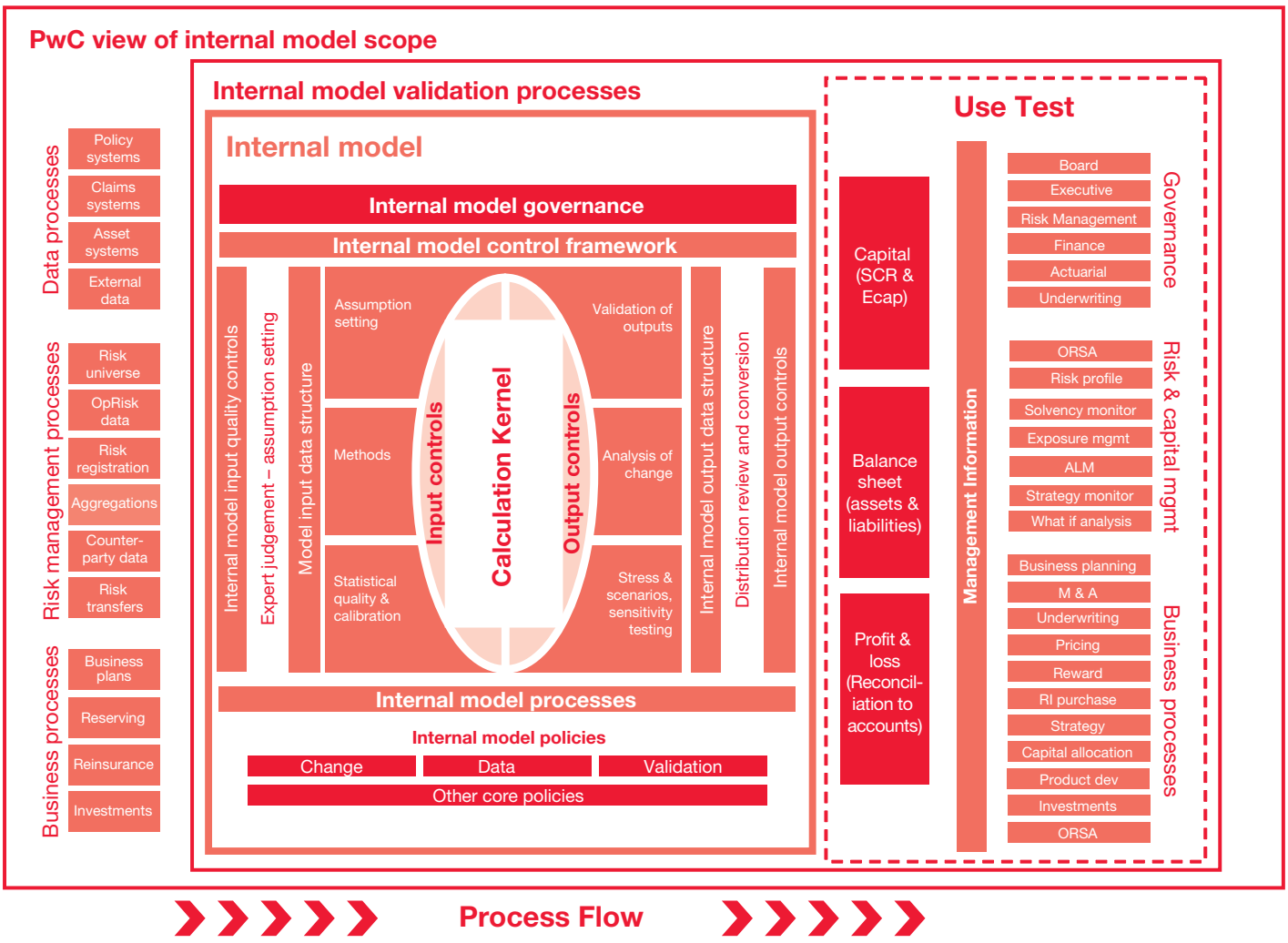
The internal model is more than just a calculation tool. It is used to measure, control, manage and report on risks. It is at the core of risk strategy and risk management. As illustrated in the following diagram, it is made up of methodologies, assumptions (endogenous and exogenous) and configurations designed by experts which reflect defined policies and apply to internal processes that are specific to the business. Within an environment limited and secured by internal control, the internal model can also be used to produce a variety of reports designed to meet management's requirements. In this example, it is used to produce the information used to determine MCEV, economic assessments that measure economic performance or the company's new solvency measures. In the future, these models will also serve for evaluating accounting in IFRS under IFRS 4 phase 2.



The internal model plays a pivotal role in the company's decision-making processes at every step, both in underwriting contracts upstream and in managing underlying risks. The internal model, a key component in governance, is implemented in line with the internal control, internal audit, actuarial and risk management functions. However, its implementation may be costly, especially as Solvency II provisions already require considerable resources for insurance and reinsurance companies. In such cases, it may seem more appropriate to apply a standard formula. The use of an internal model is not mandatory.

Finally, internal models must be approved by the regulators prior to use. This point is developed in section 2.3.

Figure 16: Internal model scope



Source: PwC

2.2.3. Managing risks

Once the risk strategy is defined, it can be translated into a risk policy applicable to all entities or adapted to account for country regulations or specific local markets.

Risk policy is based on the implementation of governance systems that cover at least the following risks:

- Underwriting
- Market
- Credit
- Operational
- Outsourced services
- Internal audit

A governance system is a set of principles and rules established to monitor and manage risks based on a clear, shared decision-making process and adapted tools. It generally features the following components:

- A **set of rules**: best practices (industry standards or company-specific practices), tolerated practices, prohibited practices.
- **Delegation of authority procedures**: any decision that could significantly engage the company must be approved by at least two people at management levels that correspond to the level of commitment.
- **Pricing** and **provisioning**: profitability target, technical bases used, pricing and provisioning methodology.
- **Risk monitoring**: risk indicators, specific risks requiring specific monitoring, stress tests.
- **Tools**: documentation, standard and non-standard tools.

An example of policy: Actuarial function

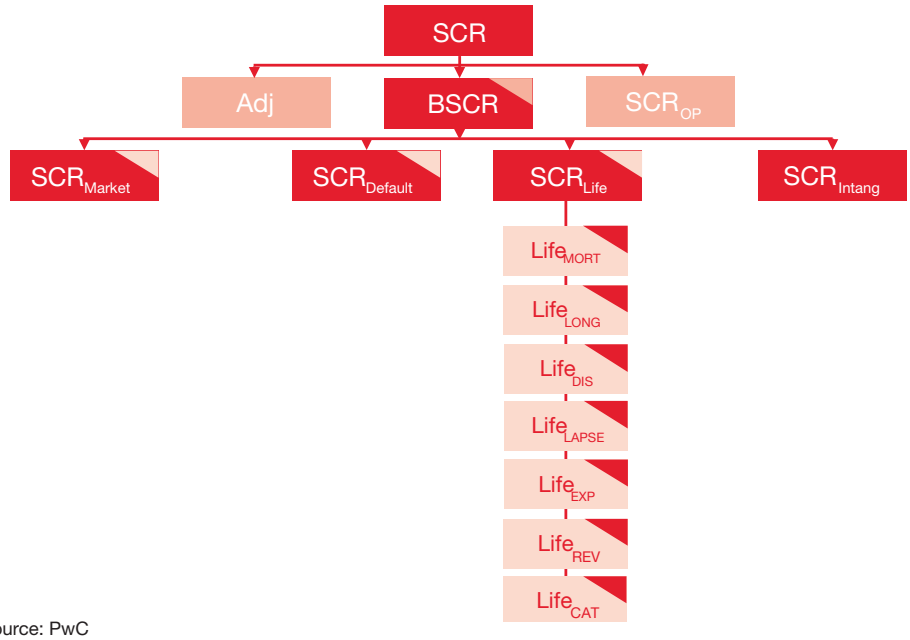
The first section in this paper discussed the principles for governance set by the Directive. We understand that these risk policies are broken down by risk according to the modular risk-based approach of Solvency II.

How does it work in practice? Let us take the actuarial function as an example. This function 'owns' the underwriting risk and is therefore in charge of measuring, managing, controlling and communicating the components of this risk. The underwriting risk policy must reflect all of these aspects.

Governance is based on compliance with principles or guidelines established in accordance with best practices recognised by the industry as well as the company's internal practices. These guidelines are applied as soon as a contract is underwritten, as they set pricing policies in terms of risk selection (when possible) and measurement of the cost of risk.

For example, in dealing with longevity risk in annuities, the actuarial function may prefer an experience table certified by an independent actuary rather than the local country regulatory mortality tables. With more detailed knowledge of the portfolio, a company may apply mortality assumptions that are lower than the standard if the type of population covered enjoys a better standard of living and healthcare.

Figure 17: Risk models for life insurance



Source: PwC

2.2.4. Monitoring and reporting on risks

Using risk measurement tools and processes, the risk management system must produce all the information necessary to the relevant managers to ensure appropriate and hands-on oversight. Internal and external reporting structures must be put in place.

Internal reporting

The purpose of a risk report is to facilitate risk monitoring by providing necessary information and analysis of the existing and potential risks to which the company is exposed.

The content of the risk report must be adapted to its readership:

- Senior Management: the report presents, in about ten pages, an overview of the risks affecting the company (the risk map, the three to five major risks, the market environment, and comparisons with competitors).
- The business line or operational entity: the report covers, in about 15 pages, the risks to which the business line or operational entity is exposed.
- Detailed risk report: this document, often about 100 pages or more, provides all the evaluations and detailed action plans for each risk.

External reporting

These reports are covered in Pillar 3 of the Directive. The reporting scope is described in CP58, which includes quantitative and qualitative sections on various aspects (accounting, prudential, governance, etc.). Further details are provided in the following documents:

- Annual Reporting To Supervisors (RTS): notably includes an annual Quantitative Reporting Template (QRT) that provides details on the information contained in the RTS.
- Annual Solvency and Financial Condition Report (SFCR): for the market, adopts the structure of the RTS without the information for supervisors.
- Quarterly RTS: mainly includes a quarterly QRT, a concise version of the annual QRT.

The necessary convergence of Risk and Finance

We have seen that companies increasingly tend to plan a specific operational project on this subject for a number of reasons:

- Technical issues: Companies are confronted with an increasing number of reporting requirements (SFCR and RTS within Solvency II at deployment, MCEV, IFRS 4 Phase 2, reports to rating agencies, etc.), for which the frameworks are not always the same. Each company must ensure that it can cope with the risks of error in the different reporting processes (internal control principle), and be able to reconcile and justify the differences between the different reports (differences in method, measurement basis, etc.).
- Operational performance issues: In light of the requirements mentioned above, many companies will have to increase the number of their closing and reporting processes. This gives rise to legitimate concerns about efficiency and cost-cutting in these low value-added processes. Several companies plan to set up a shared data warehouse that will be updated by source systems (management, assets, inventory, etc.) and from which data will be extracted in the same way by different users for different data processing activities. Downstream, these companies tend to organise all market disclosures for more consistent communication and to assure greater control over publication schedules.
- Strategic issues: As a result of regulatory pressure, market practices are converging towards the assessment and management of risk-weighted performance. In addition to 'traditional' financial and operational performance, management systems must produce a review of the risk incurred by the company to reach these figures, or more specifically the 'performance' of the company's risk-taking. This new approach will undoubtedly result in the set-up of projects to consolidate these systems and overhaul the management tools used by general management and shareholder communication. These areas are a priority for general management and policymakers and will gradually be implemented as the ORSA processes mature.

2.2.5. Establishing strategic capital planning

The forward-looking analysis of capital could be considered the last deliverable in the risk management process. Under Solvency II, measuring and managing risks must enable the company to maintain its solvency at all times and to strike a balance between business objectives and the amount of risk incurred to reach them. The forward-looking analysis of capital requirements or strategic capital planning is the prime focus of the ORSA process and must be carried out in close collaboration with management.

This process is designed to show that the insurer can raise the capital necessary to cover solvency margin requirements for the strategic planning period. For each business strategy, the insurer simulates a large number of scenarios in which risk parameters are adjusted to compare solvency margin requirements and available capital. This analysis is carried out prior to every major strategic decision (merger, acquisition, launch of a new business, etc.).

If the analysis reveals insufficient capital, the insurer must prove that it has a realistic back-up plan, e.g.:

- A recapitalisation plan
- Transfer of risk (reinsurance, derivatives hedging, securitisation, etc.)
- Limiting of gross exposure (underwriting limits, investment limits, etc.), e.g. by adjusting the strategic configuration (joint venture rather than a new company, and so on)
- Loss absorption mechanisms (participation reserves, call for supplementary contributions, etc.).

The company must also be able to measure the sensitivity of these analyses to any deterioration in its competitive or macroeconomic environment. Along with these capital planning analyses, stress tests are performed to understand the underlying assumptions, the determinants of capital planning and its sensitivity to risk. Stress testing can notably be used to identify potential threats and devise back-up plans to reduce their impact on the company's financial position. Stress scenarios are clearly explained, for example those used by EIOPA in 2009 to determine the solvency of the European insurance industry:

- **Adverse scenario**: 15% to 50% decline in relative value of interest rates depending on maturity, widening of credit spreads, 10% to 20% drop in equities, 15% drop in property simultaneously with a massive wave of redemptions.
- **Deep recession scenario**: 40% to 60% decline in relative value of interest rates depending on maturity, widening of credit spreads, 40% to 55% drop in equities, 25% drop in property simultaneously with a massive wave of redemptions.
- **Inflation scenario**: 40% to 500% rise in relative value of interest rates depending on maturity simultaneously with a massive wave of redemptions.

2.3 Managing cross-business projects

Within your Solvency II compliance programmes, Pillar 2 provisions will require the implementation of certain cross-business 'sub-projects'. Although not directly required by the regulatory provisions, these sub-projects are in fact essential from an operational standpoint. We shall develop this subject further here, focusing on a limited number of projects that are closely linked to Pillar 2 provisions:

- **Data quality** – Measuring and managing risks, then applying them to strategic capital planning requires significant confidence in the reliability of the data and calculation processes used.
- **Validation of the internal model** – Companies that have opted to use an internal model as of 1 January 2013 must take into account the myriad of constraints of the pre-validation process and then the final validation by the regulator.
- **Change management** – Regulatory requirements most often call for a major organisational transformation and significant changes in practices that you will need to understand, calibrate and guide.
- **Implementation of ORSA** – This process must show the company's ability to integrate its risk effectively into its management and its strategy. Only rarely do companies have all of the necessary pieces of the puzzle in place to meet regulatory principles.

2.3.1. Ensuring data quality

Data management requirements
Data quality is a key issue in the Solvency II Directive. Following the example of Basel II, it concerns the completeness, appropriateness and accuracy of the data used to produce regulatory solvency indicators.

The choice between an internal model and the standard approach does not affect the management of data quality. As only internal models require validation by the regulator, this option requires the greatest compliance effort. The level of quality must be certifiable and verifiable. In other words, the standards are more or less comparable with those for an accountant. The burden of proof lies with the insurer.

In order to comply with the regulatory requirements, a distinction must be made between two aspects of data quality:

- Static aspect: in which the quality of the data that feeds the model must be assured, irrespective of source, and
- Dynamic aspect: control of data extraction, transmission and transformation processes where the data comes from management applications that are used in actuarial calculation, cash flow projection engines and in reporting components for the 'publication' of regulatory solvency indicators.

These two aspects are to be understood in light of the fundamental purpose of Solvency II as opposed to the current solvency regime, which is based on a fixed percentage. The new regime introduces sensitivity to insurers' risk portfolios. Each business line is handled separately, based on the notion that for the same premium, exposure and therefore capital consumption vary depending on the type of risk.
The calculation of solvency capital requirements (SCR) is specific to each business line, as are the tools, controls and data, e.g., Life, Non-Life, etc.

'Static' issues: managing data
The Directive and several consultation papers mention the three criteria of data quality analysis from a static point of view:

- **Completeness**: The data available cover all the risks in the portfolio with the same granularity and historical depth, whether in direct management, delegated management, coinsurance or reinsurance.
- **Accuracy**: The data contain no bias caused by human, IT or technical error that would make it unfit for use in calculating a regulatory indicator.
- **Appropriateness**: The data is suitable for the intended purpose. In the event of any deficiency or lack of data, the proxy used is explicitly documented and justified in order to be clearly understood by the regulator.

These principles cover all the data used within the framework of regulatory calculations, from management applications (description of contracts, claims, premiums), asset-liability management, accounting (fees, commissions, etc.) or external sources (assumption data, marketing data, shocks, ratings, economic scenarios, macroeconomic data, etc.).

Three main deliverables are prepared in order to comply:

- The data dictionary, which lists all of the data used in the internal model or standard formula. This specific scope of data is where the company must show that it can successfully meet the three data quality criteria listed above.
The regulatory authorities require all insurers to internalise these three concepts and adapt them into measurable criteria for data quality. This crucial work is to be carried out as the dictionary of data used by the risk management processes is being built. Determining these measurement criteria for data quality while building the dictionary by business line and source process/system is the cornerstone of two major deliverables, namely the insurer's data quality charter or policy and the data governance model.

- The quality policy for risk data is a fundamental document which sets out precisely:
  - The objectives, scope issues, resources, etc.
  - The measurement criteria of data quality, aligned with the three criteria of the Directive (completeness, accuracy and appropriateness) for each business line.
  - The principles for data quality review (frequency, depth, scope, retrieval, responsibility).
  - The dashboard for monitoring data quality by business line, notably based on:
    - Data and network security
    - Data integrity
    - Data availability
    - Compilation of records
- The risk data governance model defines:
  - The objectives, scope issues, resources, etc.
  - The measurement criteria of data quality, aligned with the three criteria of the Directive (completeness, accuracy and appropriateness) for each business line.
  - The principles for data quality review (frequency, depth, scope, retrieval, responsibility).
  - The dashboard for monitoring data quality by business line, notably based on:
    - Data and network security
    - Data integrity
    - Data availability
    - Compilation of records

'Dynamic' issues: securing transmission channels

Work on dynamic issues includes the control of the infrastructure and processes in risk data management. Most firms have set up data warehouses into which business data are fed to be used to calculate indicators (economic capital, MCEV, etc.), technical provisions and operational and financial management indicators. They are also generally used to update data in management dashboards and accounting/management reconciliations.

Insurers should concentrate their efforts on data transmission channels. The source of a Solvency II data channel is in a management application. The channel integrates components from infrastructure and transformation operations, aggregation and data calculation, through to the integration of assumptions, shocks, cash flow projection, calculation of different SCRs and production of internal and regulatory reporting. It is an end-to-end process that must include a thorough, documented audit trail. There are virtually as many data channels as there are source systems. The role of data centres or warehouses is to concentrate data. The data dictionary is used to align the flows from source systems and reconstitute the data from a given system if necessary so as to ensure perfect consistency between portfolios, regardless of their source systems.

The other positive consequence is to prevent spreading the business approach of applying source management throughout the data warehouse (relational principles, terminology, etc.). The data extracted and transformed are available for a larger number of 'clients' and more easily meet use test requirements, as stipulated in the Directive.

2.3.2. Obtaining validation of the internal model

As mentioned above, the internal model is more than a mere calculation tool; it is a key element in the company's decision-making processes. Whether total or partial, this model must be approved by the regulator. A considerable amount of documentation must be drawn up to prove that the model meets the Directive's requirements.

Validation procedures

The Directive defines eight tests that a candidate company must pass to validate the internal model:

1. **Use test:** Management must understand the internal model's risk and capital assessments as a fundamental driver in implementing its business plan and strategic decision-making processes.

2. **Statistical quality standards:** Assessments must be based on relevant, reliable, consistent and understandable risk factors and realistic, credible and verifiable assumptions.

3. **Calibration standards:** Results must be calibrated to a 99.5% VaR over one year.

4. **Profit and loss attribution:** Companies must regularly check whether the risk classification and the profit and loss attribution in their models accurately reflect the causes of profits/losses of operational units.

5. **Validation standards:** The appropriateness of assessments and underlying assumptions must be tested regularly against data drawn from experience. Companies must also gauge how sensitive results are to changes in key assumptions.

6. **Documentation standards:** Regularly updated written records must be kept on the model's design, operational details, mathematical bases and underlying assumptions.

7. **Internal model governance:** The internal model is only approved if the insurer meets satisfactory governance and internal control standards.

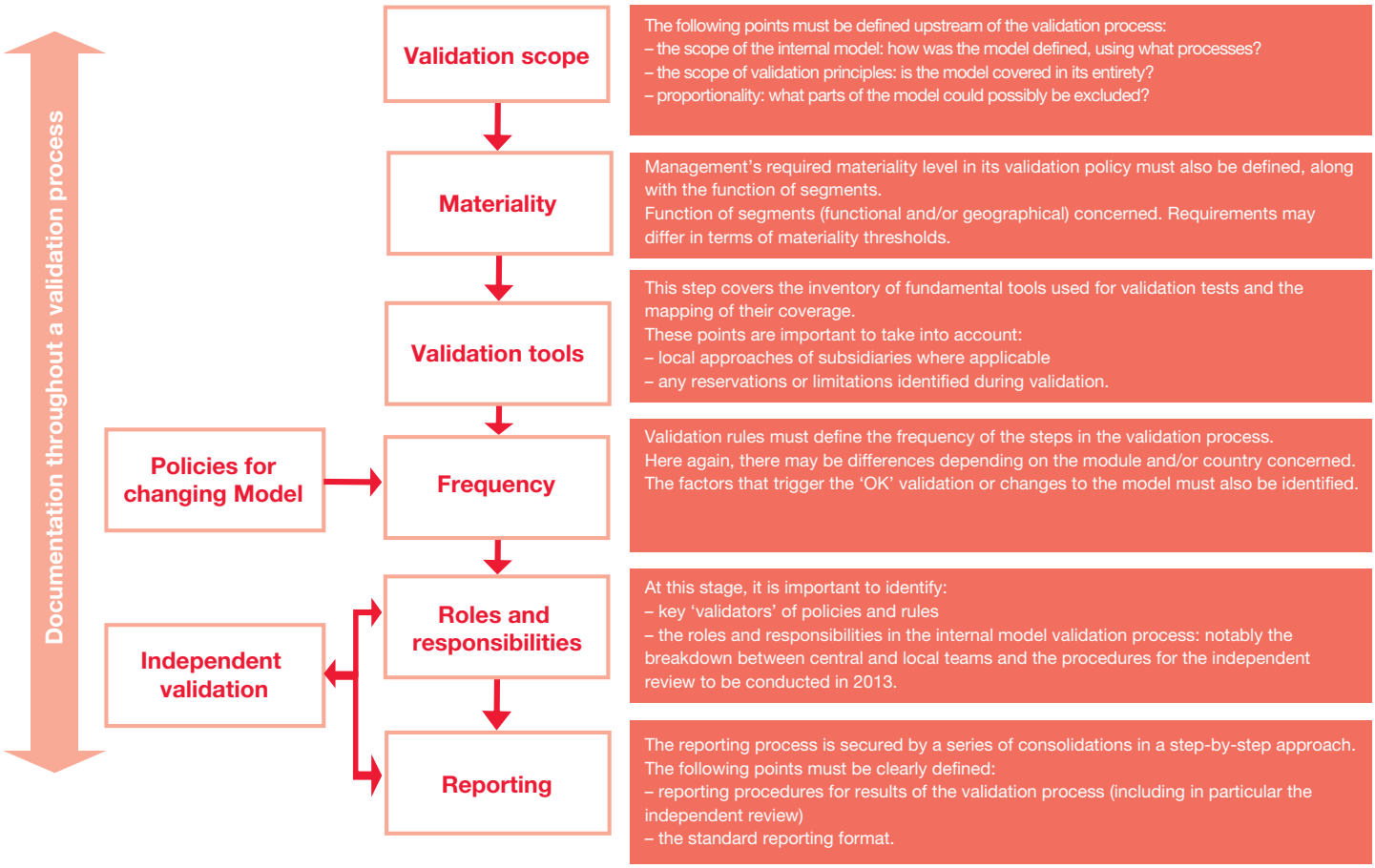
8. **External models and data:** These tests also apply to third-party (outsourced) data or models.

Organising the validation process

It is important that the company can demonstrate that the model has been adapted to its business by the decision makers, that it is understood and applied correctly. Basically, it must show that the model plays its intended role in the governance system. The calculation methods used by the model must be adequate and based on credible assumptions. The company must be able to justify any differences between the underlying assumptions used in the model and those in the standard formula. The model must cover all the risks to which the company is exposed and its calibration must have no adverse effect on policyholders' benefits.

The model must allow for the annual analysis of the business' profits and losses broken down by risk category included in the model. This should determine the company's real risk profile. The model must also be monitored and approved on a regular basis to ensure that it remains in line with the risk profile. This validation process, illustrated in the diagram below, must show the regulator that the capital requirements calculated by the model are in line with the company's actual risk profile.

Figure 18: Internal model scope validation



Source: PwC

The company's application for validation analysed by the regulator must include all of the above-mentioned items. The application should show that the internal model is the result of a structured approach and is perfectly integrated and documented. This step in preparing the validation application can actually be rather complex and should therefore be carefully planned. At its conference on 22 November 2010, the ACP offered some useful pointers concerning the documents it expects in the validation application:

- In addition to the application that will form the basis of its assessment, the ACP expects all of the supporting documents to be completely available and compiled into a detailed summary.
- For international groups, the working language is English, but at least a partial translation of the application into French is required.
- The mathematical methodologies used (assumptions, operational application, configuration, frequency of revaluations) must be clearly described.
- A precise description should be provided of the model's governance processes, notably regarding coordination between subsidiaries and the Group.
- The internal validation policies for the model, data management and enhancements to the internal model should be included in the application.

The regulator performs the internal model validation process in line with the timing constraints set by the Directive. This process includes a preparation and a pre-validation phase. At the same conference, the ACP indicated the main milestones in its validation timetable:

- Preliminary discussions with applicants about their model should have been completed by 31 March 2011.
- The regulator expects the company to submit its internal model validation application (i.e., documented application that has been approved internally) by 31 March 2012.

"Governance under Solvency II requires a clear commitment from all heads of operating units. Change management will be central to ensuring acceptance of methods that are far more binding than many risk officers have previously experienced."

Philippe Léglise, Risk officer, Allianz France

2.3.3. Managing change

Generally speaking, the Solvency II compliance project is a fundamental, company-wide programme with an impact at almost every structural level: strategic and decision-making processes, organisation, governance, information systems and, especially, corporate culture. These new operational procedures require full involvement from all staff as Solvency II changes both behaviour (notably regarding risk) and the way of working. It is vital that resources are planned, scheduled and implemented in order to help spread 'Solvency II culture' from the outset of the project.

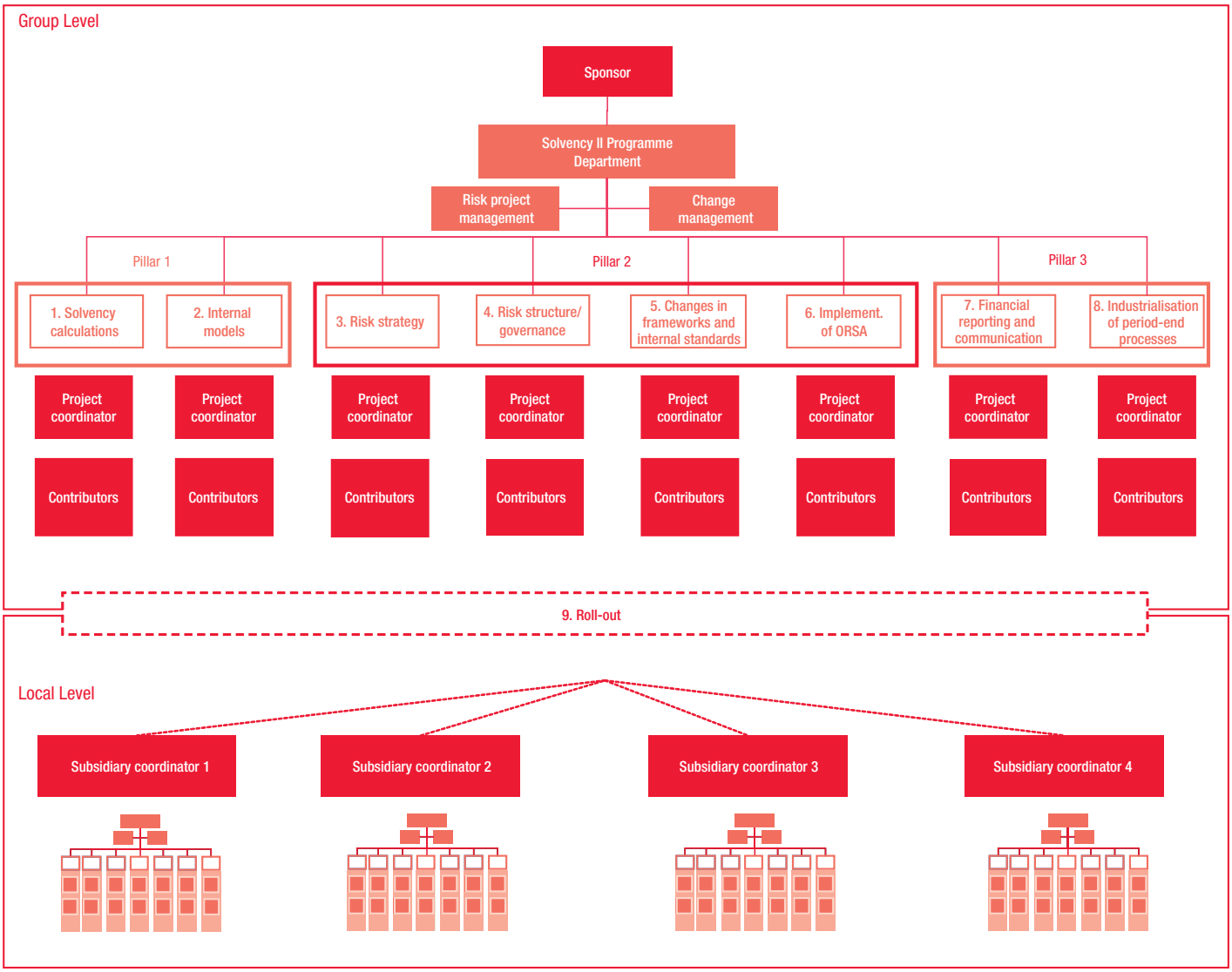
Necessary discipline in managing the programme

A project is referred to as a programme if it includes several complex sub-projects that must be coordinated. Given the breadth and complexity of all of the Solvency II sub-projects and the number of contributors involved in implementing an efficient cross-business programme, management structure is a key factor in the programme's success. It is a pre-requisite for the launch of the operational projects and covers all related responsibilities:

- Coordinating the various projects relating to the three pillars and other related projects (e.g, upgrade of the information systems already underway, enhancement of the internal control system, etc.).
- Coordinating programme communication and training.
- Fostering a 'Solvency II culture' within the company.

There is no ideal structure; each company defines its own programme management procedures in line with its specific constraints, objectives and timetable. We have provided a generic example of this type of structure in the diagram below. We would also like to point out two major factors for its calibration:

Figure 19: Example of project structure for Pillar 2 Implementation



Source: PwC

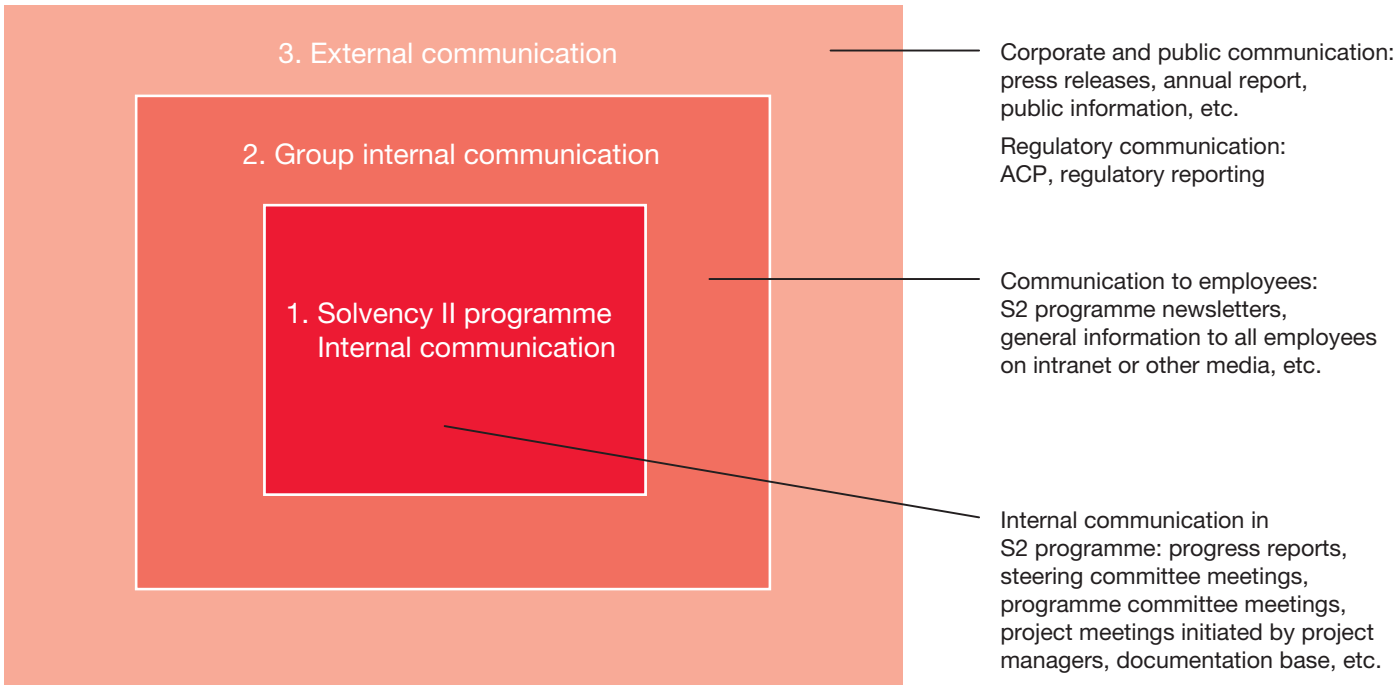
- It must be able to manage various projects in the programme and their interaction simultaneously (pooling of resources, cross-impact analysis of key choices made for a specific project, etc.).
- It must closely reflect the existing organisational structure in place in order to roll out the culture-related projects and enhancements needed throughout all Group entities.

The ideal scenario is to create a dedicated change management unit to lead and coordinate change. It should be responsible for managing internal communication on the programme and the implementation of the risk culture. It can also oversee, in conjunction with HR, the requirements for training and additional resources in order to complete the various projects. The change management scope extends beyond just the Solvency II programme scope; instead, it covers all company staff.

Defining a communication strategy

Communication is fundamental to managing change and bringing about a new corporate culture. The communication strategy must take into account the different levels of communication, corresponding to different audiences and requirements:

Figure 20: Communication strategy



Source: PwC

A global communications strategy is a useful tool in managing the Solvency II programme. Its main objective is to promote the involvement of key players in the Solvency II programme through initiatives designed to help them understand the requirements of the three pillars and how they are applied to each operational level. The communications strategy is often broken down into communication plans. The table below is an example outlining the main points:

Figure 21: Example of communication plan

Communication level	Recipients/Target audience	Communication channel or medium	Role of the Solvency II Programme management/ Change Management Unit	Role of the Communication Department
1. Solvency II programme internal communication	• Everyone involved in Solvency II programme • Steering Committee members • Project Committee members • Bodies specific to each project	• Team meetings, working groups, committees, etc. • Internal documentation (presentations, training materials, minutes to meetings, etc.)	• Is responsible for and independently manages internal communication programme	• Advises/provides the project with communication tools if applicable
2. Group internal communication	• Directors • Executive Committee members • Management Committee members	• Programme progress reports, general and/ or technical information (e.g.v training material) • Option of dedicated page/ portal on intranet	• Proposes the format • Approves content and messages • Is responsible for distribution	• Checks and approves the consistency of messages and format • Manages communication tools
	• Is responsible for announcement/publication • All Group employees in the broad sense	• Slovency II programme newsletters, general information to all employees on intranet, etc. • Programme presentation material	• Proposes content and contributes to formulation of messages	• Checks and approves the consistency of messages and format • Is responsible for announcement/ publication
3. External communication	• General public • Group clients	• Press releases, annual report, public information on Group website, press conferences	• Proposes content and contributes to formulation of messages	• Approves content, messages, format with GM • Is responsible for
	• ACP • European supervisors (CEIOPS, etc.)	• Reporting on progress, ACP requirements, participation in industry-wide discussions and working groups, etc.	• Approves content, messages with other departments concerned (Technical Department, Finance Department, etc.) • Is responsible for announcement/ publication through ACP representative	• Is systematically informed prior to any announcement/ publication

Source: PwC

Managing changes in human resources

Human Resources is the second critical area of change management. The Human Resources department is critical to the programme's success, given the important role played by many of the functions within its remit:

- *Training*: Develop employees' business expertise and provide them with the technical knowledge required to perform their duties in a Solvency II environment.
- *Recruitment*: Attract external expertise that the company does not currently have and foster loyalty among these experts, taking into account the high-pressure environment for some profiles (actuaries, risk management specialists, etc.).
- *Knowledge management*: Identify the technical and managerial expertise which needs to be developed in the Solvency II environment and coordinate the transition.
- *Management of individual performance*: Foster and guide changes at the most basic level of the organisation.

Training contributes considerably to developing employee expertise, not only during the project phase but also following the implementation of the Directive. This includes training on the content of the regulation itself (e.g. the three pillars of the Directive, the CPs, QIS 5) and risk management. It is expected that training on the new risks to be taken into account by insurers will be requested most often:

- Market risks
- Credit risks
- Operational risks, and so on.

Similarly, a sharp rise in requests for training on financial techniques and products is to be expected from employees involved in technical, risk or finance processes or even other business lines.

In order to promote a risk culture, a key issue in Pillar 2, both technical training for professionals and 'awareness' training aimed at all company staff are essential. The latter type of training must focus on presenting the Directive's main concepts, what they mean for the company and the insurance industry, and the changes to expect in the insurance profession.

One of the ways to accelerate learning about Solvency II in the company is to encourage its rapid adoption among operational managers. They must be at the heart of training and should be among the first informed and trained. They should in turn be able to train their teams, at least in the areas that directly concern them. This is the 'train the trainer' model. Solvency II training has been an extremely important issue in 2011 and will continue to be in 2012. HR managers should already be defining needs and assessing their impact on training budgets.

In terms of knowledge management, companies with a strategic workforce plan should also take into account the expected changes in employees' expertise very early on. Expertise (current vs. target) must be entirely remapped. Any gaps must be closed through both training and hiring, meaning that recruitment needs for 2012-2013 must be identified rapidly, as some profiles, such as actuaries or asset-liability managers, are particularly difficult to find.

Finally, performance management is also important in stepping up change. In order to advance their compliance to Solvency II, companies may plan to set specific targets for managers, e.g., on implementing Pillar 2 (ORSA implementation, formal definition of processes, identification of risks and controls, etc.), either in new assignment letters or annual performance reviews.

A portion of performance-related pay should depend on meeting these targets in order to boost motivation.

2.3.4. Implementing ORSA process

ORSA implementation follows a five-step process that is integrated into the company's risk management:

- Risk identification
- Risk appetite
- Strategic planning
- Stress testing
- Capital allocation

Activating this process affects every level of the company, following either a top-down or bottom-up approach:

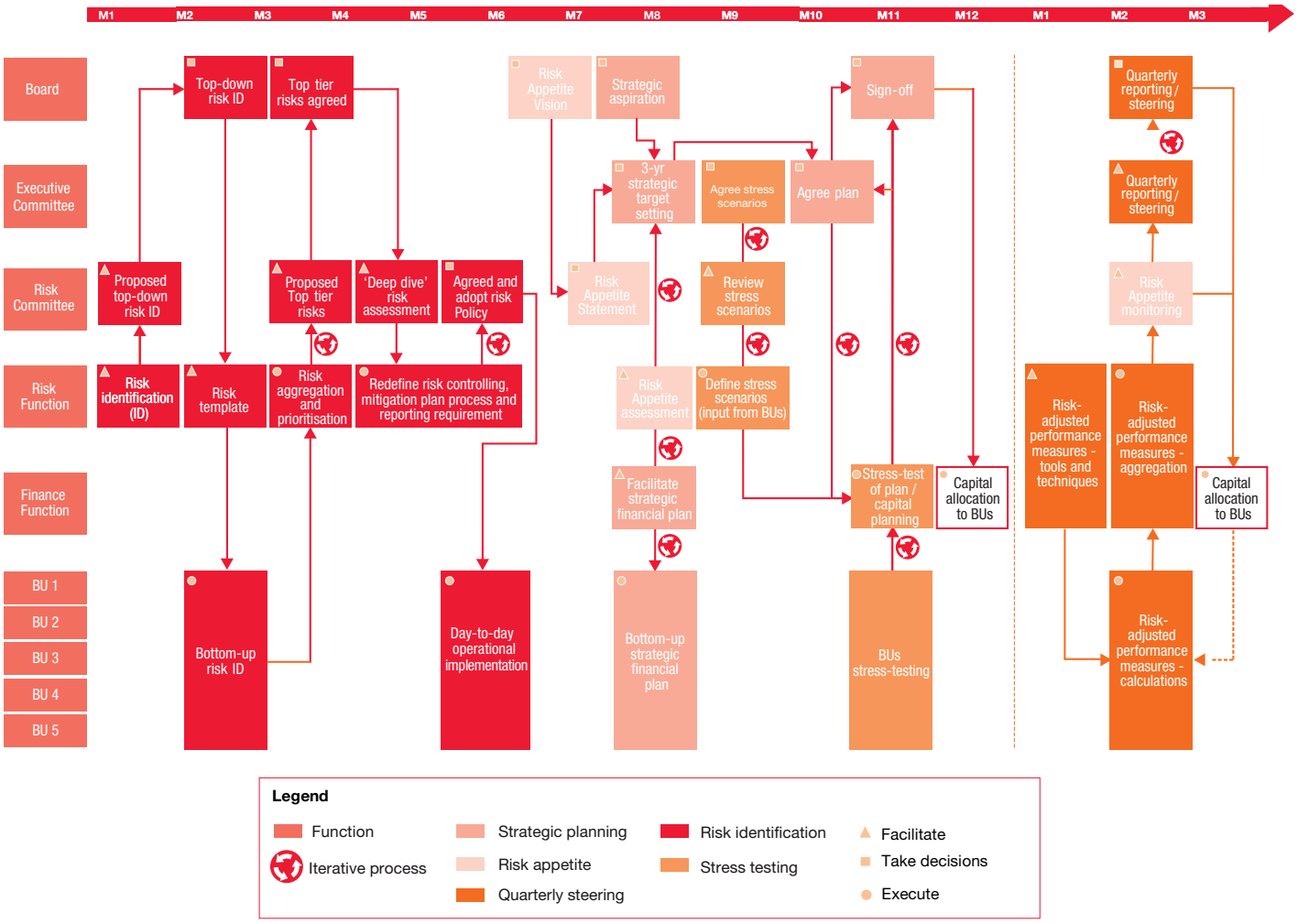
- From senior management to operational units: definition of company strategy, risk appetite, capital allocation to business lines.
- From operational units to senior management: risk identification, measurement of the risk profile, risk reporting.

"ORSA is set to be a strategic management and oversight tool for the insurance business. The benefits it brings will be closely linked to the flexibility of its operational implementation."

Sébastien Simon, Head of the Solvency II Programme, Société Générale Insurance

The following dynamic diagram provides an overview of the ORSA process over the budget period:

Figure 22: ORSA process (throughout the budget process)



Source: PwC

Coordinating and industrialising the ORSA report with Pillar 3 risk reports

Directive Articles 35 and 50 and CP 58 stipulate that the ORSA report submitted to the regulator must contain quantitative and qualitative information that is also included in the reports (RTS and SFCR) required under Pillar 3.

Conclusion

Operational implementation requires deep-seated change in terms of both organisation and business management. Launching projects such as these requires careful attention to a few key concepts underscored by the Directive.

'Risk appetite' must be defined and documented with respect to the business goals. The same applies to the company's 'risk culture', i.e., acceptance by staff of a clearly mapped-out risk profile and strategy. The third key to ensuring operational compliance is the choice of which organisational and governance models to use for the risk management process. Which decision-making model should be implemented? To whom should decision-making and control powers be assigned? How should the risk function be scoped?

These decisions will pave the way for the interpretation and adaptation of the principles of Pillar 2 based on your organisation, its specific set-up and its commercial strategy.

Overall Conclusions

Of the three pillars of the Directive, Pillar 2 is undoubtedly the most important and complex to implement because it requires companies to place risk management at the heart of their operational business models.

As we have explained throughout this paper, it involves the introduction of a new standard framework for risk management that must now form an integral part of all managerial functions. Above all, Pillar 2 implies making difficult decisions related to configuring and adapting the operational application of this framework at all levels of the company – organisation, control, governance, relations with 'suppliers', and so on.

The tools and framework, together with the ERM approach, serve to align company strategy with the risk accepted and taken on by management and operational staff. Under this Pillar 2 approach, the risk function becomes the cornerstone of the risk management system.

Implementing a risk culture, another key issue in Pillar 2, is also critical to meeting compliance objectives and ensuring that they are both operational and effective. Companies will be aided in this endeavour by two main drivers, communication and human resources.

Pillar 2 also represents a radical change for many companies in the insurance sector. Except for large groups, many companies have not changed their structure or operational processes for several years. The Solvency II Directive provides an excellent opportunity, particularly in a climate of economic crisis, to optimise company management and increase operational efficiency in all functions by defining and streamlining processes, upgrading information systems and tools, building staff knowledge, and so on.

In the same way, implementing ORSA also offers a number of opportunities by prompting insurers to optimise their operational performance over a strategic three- to five-year timeframe, ensuring that the company's capital is in line with its risk profile and business ambitions. ORSA is destined to become a key instrument for strategic management.

This expected enhancement of operational performance should, in the long term, largely offset the significant implementation costs of compliance with the Directive, especially Pillar 2.

The results of the PwC 2010 pan-European study[1] on preparations for Solvency II demonstrate that insurers seem to be coming to terms with the challenges involved in implementing regulations that place risk governance at the heart of their business.

1 Source: Getting set for Solvency II: Comparing goals and benchmarking progress on Solvency II implementation across Europe, November 2010

Authors

Eric Dupont
France Insurance Leader
+33 1 56 57 80 39
+33 6 08 90 64 52
eric.dupont@fr.pwc.com

Jimmy Zou
France Solvency II Leader
+33 1 56 57 72 13
+33 6 74 27 34 79
jimmy.zou@fr.pwc.com

Quoc Nguyen Dao
Director
+33 1 56 57 57 14
+33 6 74 32 19 33
quocnguyen.dao@fr.pwc.com

Contributors

Thank you to our contributors:

Sébastien de la Lande, Dominique Daijardin, Antoine de la Bretesche, Pierre-Antoine Duez, Stéphanie Artigaud, Benoît Germain, Rémi Sauciém and Nicolas Simon.

Contacts

Julia Schüller
PwC (Germany)
+49 69 9585 2667
julia.schueller@de.pwc.com

Clint Sookermany
PwC (Norway)
+47 95 26 12 78
clint.sookermany@no.pwc.com

Lena Mörk
PwC (Sweden)
+46 10 212 4879
lena.moerk@se.pwc.com

Garvan O'Neill
PwC (Ireland)
+353 1 792 6218
garvan.o'neill@ie.pwc.com

Elena Demidenko
PwC (Russia)
+7 495 967 6414
elena.demidenko@ru.pwc.com

Jim Bichard
PwC (UK)
+44 207 804 3792
jim.bichard@uk.pwc.com

Alessandro Di Lorenzo
PwC (Italy)
+39 02 6672 0571
alessandro.a.di.lorenzo@it.pwc.com

Jose Luis Lopes Torres
PwC (Spain)
+34 915 685 482
jose_luis.lopez.torres@es.pwc.com

www.pwc.com/solvencyII