AGERS Guide to the risk management function in insurance companies

María Nuche Otero
Risk Management Director
Consorcio de Compensación de Seguros

The presentation of the AGERS (Asociación Española de Gerencia de Riesgos y Seguros) [*Spanish Risk Manager's Association*] Guide to the risk management function in insurance companies took place on 6 October 2020. The Guide was written by the members of AGERS's Committee of Experts on Insurance Company Risk, including two members representing the Consorcio de Compensación de Seguros, Eva Valenti, Head of the Actuarial Review Department, and María Nuche, Director of Risk Management.

The Committee of Experts is made up of members in charge of the risk management function at insurance companies of different types and sizes who have been closely involved in the work of implementing and monitoring risk management operations.

This publication is intended to furnish a Practical Guide to the risk management function in the service of the profession, setting out insurance company risk management best practices and in addition addressing compliance with Solvency II requirements.

The main purpose of the Guide is to provide a reference intended to enable insurance company risk managers to ascertain whether or not what they are doing is in line with the common tasks and practices considered, with a view to being able to establish an efficient risk management system. The idea is to provide a flexible model that will allow each company to perform proportional self-assessments under the proposed framework, taking into account its own nature, structure, and internal rules and procedures.

The main purpose of the Guide is to provide a reference intended to enable insurance company risk managers to ascertain whether or not what they are doing is in line with the common tasks and practices considered, with a view to being able to establish an efficient risk management system. The idea is to provide a flexible model that will allow each company to perform proportional self-assessments under the proposed framework, taking into account its own nature, structure, and internal rules and procedures.

This publication is aimed at all companies, without regard to size, corporate form, or type of business, on the basis of common patterns that apply to all companies in the person of their risk management officer.

Another of the Guide's aims is to show the supervisory authority the role and position of the risk management function and how common tasks have been implemented by insurance companies in practice for purposes of compliance with regulation general requirements.

Turning now to the actual content of the Guide, the idea has been for each section to provide a description of the tasks and best practices making up a suitable structure for risk management systems and of each of the steps that will ensure proper functioning of each company's risk cycle.

The **first section** looks at the **risk management system and risk management function** as basic components of the governance system under Solvency II. This system comprises strategies, processes, and information procedures needed to identify, measure, monitor, manage, and report the risks to which a company is or could be exposed as well as its interdependencies.

The risk management system should be integrated into the organisation's structure and into the company decision-making processes. To this end, companies should:

- identify their objectives and assess the risks that could prevent them from attaining those objectives,
- design internal controls and strategies to manage or mitigate those risks, and
- monitor the controls and strategies to ensure that they are operating effectively.

Insurance companies will, furthermore, put in place a risk management function that will serve to implement the risk management system. This function, together with the compliance, actuarial and internal audit functions, is one of the key functions under the Solvency II directive. The director of the function should therefore fulfil the fit and proper requirements needed to ensure proper performance of the function.

The key tasks of the risk management function are:

- To define the risk categories and the methods for measuring and managing them.
- To coordinate risk assessment and evaluation processes.
- To set risk tolerance limits for each type of risk in accordance with the company's overall risk profile.
- To formulate the scope and frequency of stress testing.
- To monitor compliance with action plans derived from risk management.
- To promote a risk management culture within the company.
- To assist upper management, the Board of Directors, and the other key functions with a view to effective operation of the risk management system.
- To report detailed information on risk exposure to the Board of Directors on a regular basis.
- To identify and evaluate emerging risks.
- To report all potentially major risks promptly.

The Guide includes a section on the role of the **Board of Directors** and **Delegated Committees** in the operation of the risk management system.

Insurance company Boards of Directors will bear final responsibility for:

- Ensuring the effectiveness of the risk management system.
- Setting the risk appetite and tolerance limits.
- Approving risk management strategies and policies.

Therefore, in the interest of performing the above duties, Boards will:

- Interact with the risk management function by proactively requesting information and questioning that information where appropriate.
- Document the decisions taken and the extent to which the information furnished by the risk management system has been taken into account.
- Ensure that the company has sufficient resources to perform the risk management function.
- Resolve any conflicts of interest that may arise.

The management body, as part of its duty to supervise the risk management system, will ensure that:

- Account is taken of all risks faced by the organisation in the pursuit of its objectives.
- The risks are appropriate to the organisation's objectives.
- Risk management systems are implemented and operate effectively.
- Information concerning those risks and its management is adequately reported.
- Authority, responsibility, and accountability are assigned to the appropriate levels within the organisation.

Company Boards of Directors commonly set up Delegated Committees to assist in the performance of their duties in this context. Organisations thus commonly establish Risk Committees or else assign these tasks to the Audit Committee. These Committees will:

- Ensure that all relevant information relating to risk management reaches the Board of Directors.
- Include risk supervision on the agendas for Committee meetings.
- Ensure that risk is a factor taken into consideration in all of the organisations decision-making.
- Review the risk map at least annually.
- Use internal controls to keep the risks faced by the company within the tolerance levels set by the Board commensurately with the benefit-cost ratio.
- Identify and understand emerging risks and hold meetings with the directors of the organisation's various business units to drive home the idea that they bear responsibility for effective risk management.

Section two of the Guide considers the **risk manager's role at each level of the risk management system**.

The risk management system will include:

- A risk management strategy consistent with the business strategy. Strategy's objectives, risk tolerance limits, and allocation of responsibilities will be documented.
- Decision-making procedures.
- Policies for defining and classifying risks and the risk tolerance limits for each type of risk.
- Procedures and information processes for monitoring and assessing significant risks and making changes when necessary.

Thus, all risk management systems can be seen to comprise the following five components:

- Strategy.
- Risk appetite.
- Risk Management Framework.
- Policies.
- Management and control processes and procedures.

Risk managers will perform the following tasks in connection with **strategy**:

- Identifying potential risks capable of jeopardising attainment of the stated strategy and objectives.
- Advising in respect of management actions should potential risks materialize.
- Monitoring fulfilment of the strategic plan within approved risk limits.
- Ad hoc analysis of corporate transactions.
- Advising on changes to the system of governance with a view to being able to achieve objectives.
- Ensuring that the concepts of capital and risk are considered in decision-making.
- Including the strategic plan in the ORSA process (i).

(i) ORSA (acronym for Own Risk Solvency Assessment) is the set of processes and procedures laid down by the EU Solvency II directive (Directive 2009/138/EC) to enable insurance and reinsurance companies to evaluate short-term and long-term risks they may have to face in the context of their internal capital availability and requirements.

Desired risk appetite is a key element in the risk strategy to be specified by the Board of Directors on the advice of the risk management function. Once it has been established, the risk management function will ensure regular monitoring of the level of appetite to make sure that the specified risk profile stays within the previously established levels of risk at any given time.

The risk appetite is the amount and type of risk the company is prepared to take on to achieve its objectives. It must be linked to the company's strategy and is a point of reference for business planning and decision-making. Setting this threshold makes it possible to optimise the relationship between risk and profitability.

To allow this global parameter to be put to practice use, it has to be broken down into more detailed limits suitable for applying specific, measurable day-to-day business management metrics.

Two further parameters also need to be defined:

- Risk tolerance, that is, the acceptable level of variation in the target risk appetite.
- Capacity, that is, the maximum level of risk the company can accept in achieving its objectives. Risk tolerance will act as a warning to prevent the company from reaching the level of its capacity, which would jeopardise solvency.

It is essential for risk managers to take the lead in regularly monitoring compliance with established risk limits.

The risk profile, i.e., the level of risk carried at the close of each period or at a given point in time, needs to be contrasted with the level of risk appetite approved by the Board of Directors.

Each risk is to be checked to see whether it is within the limit specified in the policies. If any limits are exceeded, the corresponding action plans are to be put forward and implemented so as to be able to stay within approved risk limits and intervals.

The results of regular comparison of the risk profile (the risks taken on at a given point in time) and the specified risk appetite are to be compiled in a report for submission to the Board, either directly or via Delegated Committees if there are any, for approval.

The **internal risk management and control framework** encompasses the risk management procedures and approaches to be implemented and employed within the company, resting on three essential pillars:

1. A suitable structure that clearly defines responsibilities in respect of risk ownership, control, and supervision. This structure will be embodied in functional and hierarchical organisation charts and in the corresponding information, reporting, and decision-making flows throughout the organisation.

2. Corporate policies that set the key operational principles aimed at attaining the stipulated objectives along with the risk limits and tolerance levels.

3. Structured and documented management procedures reported to the organisation that implement the company's management system and indicate how to carry out tasks and set up monitoring activities so as to mitigate risks. As the directive indicates, these monitoring activities should meet the requirement of being proportionate to the risks arising from the activities and processes being monitored.

The risk management framework is to be reviewed on a regular basis. Conducting the review annually is a best practice.

The set of **corporate policies** formulate the principles to be followed by the company in managing certain areas of risk and help ensure the attainment of business objectives and compliance with regulatory requirements in the territories where the company does business.

The policies should specify first and second-line responsibilities with regard to the content, assessment, approval, functioning, supervision, monitoring, and reporting of the policies. Another best practice is the direct involvement of the risk manager in drawing up a specific policy for risk management function, detailing its activities as a key supervisory function and its rights, obligations, relations, communication flows, and reporting throughout the organisation. This policy is to be approved by the Board of Directors and reviewed yearly.

The risk manager assists and advises the operational areas owning of the risks in drawing up the content of their individual risk policies. It is essential for the company to allocate responsibility for risk management and control to the risk owners.

The specific risk management policies should cover at least the risk areas referred to in the directive:

- Underwriting risk management and reserve constitution.
- Asset-liability management.
- Investment risk management.
- Liquidity risk management.
- Concentration risk management.
- Operational risk management.
- Reinsurance risk management and other risk mitigation techniques.

Risk management activities are to be transverse across all the company's processes, involving all the different operational areas of the company.

It is therefore essential to put in place **well-defined risk management and control procedures** that can identify, monitor, and measure the impact of the different risk categories. They should describe the areas responsible for managing and controlling each category, the frequency and scope of the controls and the situations that call for greater care, and a specific plan; they should also ensure that the risks are described and are known to the persons in the areas where they may occur.

The existence of these procedures, suitably documented, ensures that the system will be effective; enabling the company to stay within the risk limits set by the Board of Directors and thereby guarantee its solvency.

The risk management and control procedures established should encompass the following processes:

1. Drawing up a risk catalogue.

   Mapping the company's risks is the basic process for all risk management systems. Risk mapping may extend solely to operational risks or may also include reputation, strategic, compliance, business, financial, and other risks.

   A customary procedure for drawing up the risk catalogue consists of identifying risks by business area or by process (or vice versa, taking the process as the focus, irrespective of the particular business areas where the risks arise). The inherent impact and probability of occurrence of each risk is scored. A series of controls designed to mitigate the impact or frequency of occurrence are assigned for each risk, yielding a residual risk score. This scoring is used to monitor evolution of the risks.

   The catalogue may further include other risk-related details, such as the persons in charge of the various control procedures, associated action plans, key risk indicators or KRIs, key risk markers, and the like.

2. Identifying and updating the risks on an annual basis.

   The procedure for identifying and updating risks should span all the company's operational business areas and activities and consists of reviewing all the risks identified in the risk catalogue, verifying whether they remain current, where appropriate redefining or removing risks and allowing new risks to be added.

   The risk manager should approve any changes proposed by the various operational areas and then include them in the risk catalogue. This process includes updating processes and activities, risks, controls, and associated action plans. Any action plans regarded as appropriate to ensure that the company is in compliance with the specified risk appetite may also be included.

3. Regular risk assessment process.

   The regular assessment procedure will again involve all of the company's areas and its most important activities and consists of updating the scoring of the mapped residual risks and the level of effectiveness of the controls. This results in an updated map of the possible impact of the risks identified on management.

   The frequency of the process may be set on the basis of the priorities of the activities being monitored and whether they are business or support activities.

   The risk manager should provide the various operational areas with a way to report changes in their processes, risks, controls, and action plans and to carry out new self-assessments of existing risks and controls.

   The approach used to implement the three above-mentioned processes should be set down in writing in a risk management procedure manual.

4. Risk notification process.

   Interested parties may be notified of the findings of the above-mentioned processes by reports on the general internal risk management and control framework that include a description of the methods used to score the risks and controls and the annual scoring results.

   The frequency of these reports will be set in the risk management policy and may vary according to the criticality of the risks being assessed. Risk management activities must therefore be transverse, spanning all processes and involving all the company's operational areas.

The **third section** of the publication focuses attention particularly on the risk manager's role in the **ORSA process**, inasmuch as own risk and solvency assessment is an essential tool on which the entire risk management of insurance companies hinges.

The ORSA process plays an essential role in drawing up strategy and in business planning, since it furnishes an overview of the current and future risks to which the company could be exposed and of the unencumbered assets the entity needs to have available to be able to meet possible losses that could occur in the time horizon under consideration.

Risk managers, especially the director of the risk management function, play an essential role in the different stages of the ORSA process. The scope of their duties, together with the procedures and methods used to perform the ORSA analysis, data quality standards, and assessment frequency, should be set out in general fashion in the written policy for the process.

The ORSA results obtained should be compared with the company's risk appetite so that if any stipulated risk limits are going to be exceeded, the management measures planned for each individual case can be taken.

In accordance with Solvency II, the ORSA process should include at least:

(i) ascertaining the company's overall solvency needs having in mind all the risks inherent in its business with a view to proper short and long-term decision-making based on its capital requirements;
(ii) verifying ongoing compliance with capital requirements and technical provisions;
(iii) ascertaining the extent to which the company's risk profile deviates from the assumptions underlying the solvency capital requirement calculated using the standard formula.

The ORSA Report is to be submitted to the company's upper management and Board of Directors for validation and approval. It is to be sent to the supervisory authority (Spain's Direction-General for Insurance and Pension Funds [*Dirección General de Seguros y Fondos de Pensiones*]) within two weeks of completion (i.e., the date on which the report is approved by the management body). The recommendation is to submit the report by 30 June of the first year forecast in the report. The ORSA Report as approved will also be brought to the attention of the company's key personnel.

Section four of the Guide explains the risk manager's role in **various aspects coming under Solvency II**, e.g., its involvement in calculating the solvency capital and the minimum capital requirements, in complying with the disclosure and transparency requirements under Pillar III of Solvency II, as well as his/her role in particularities of the risk management function of insurance groups, and in outsourcing.

Given the current situation all companies are going through as a consequence of the COVID-19 pandemic, the **fifth and last section** of the Guide has considered it essential to address the role of risk management in cases of serious contingencies, that is, unexpected events that may pose a threat to business continuity. It presents a topical discussion of the risk manager's role in this connection, both in the period leading up to a contingency as the person in charge of securing the organisation's approval of the **Business Continuity Plan**, and during management of the actual contingency itself when it has occurred and afterwards, monitoring events until the organisation's business activities get back to running normally.