ECIIA

The role of Internal Audit under Solvency II

ECIIA task force / Solvency II / position paper / Internal audit

TABLE CONTENT

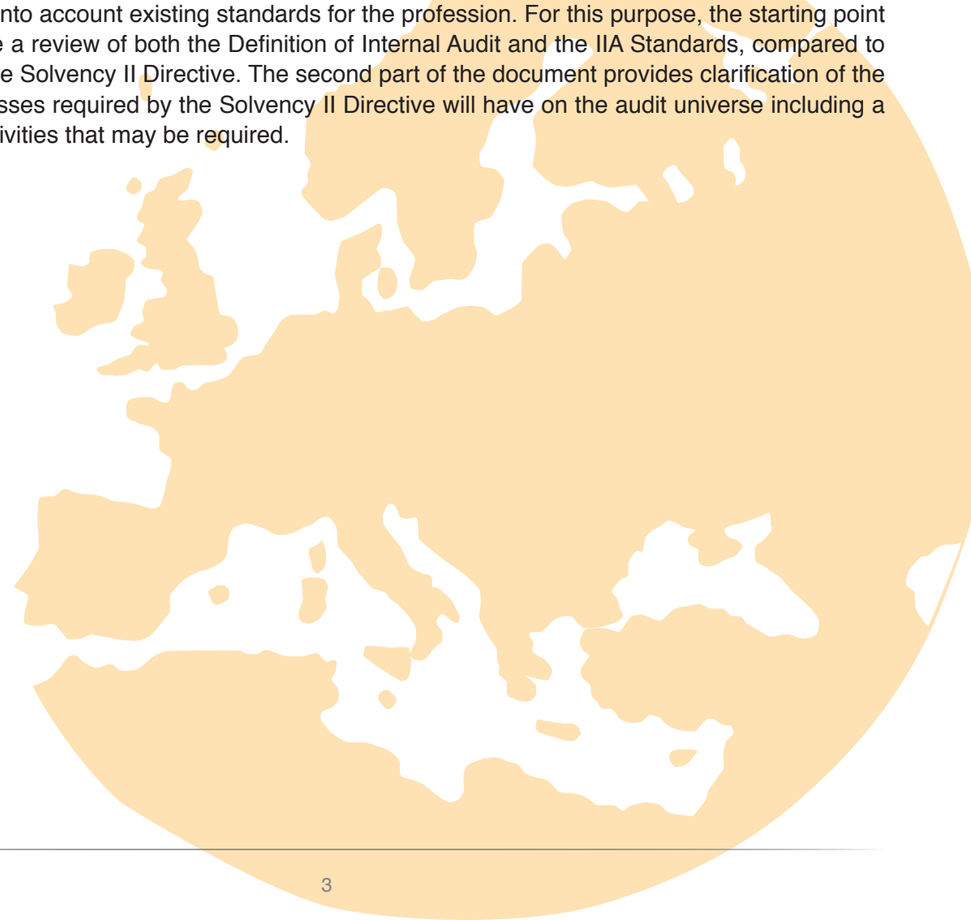
1. INTRODUCTION

The European Confederation of national institutes of internal auditors ('ECIIA') is a confederation of national institutes of internal auditors speaking for the Internal Audit profession in the wider geographic area of Europe and the Mediterranean basin, representing a membership base of over 40,000 internal audit professionals. As such, the ECIIA is an Associated Organisation of the global Institute of Internal Auditing (the IIA), which is the global professional organisation with more than 181,000 individual members in some 190 countries. Throughout the world, the IIA is recognised as the internal audit profession's leader in certification, education and research regarding internal auditing. The IIA also maintains the International Professional Practices Framework (IPPF) which includes the International Standards for the Professional Practice of Internal Auditing, the definition of internal auditing, the code of ethics, practice advisories and other guidance (the IIA Standards). (http://www.theiia.org/guidance/standards-and-guidance/interactive-ippf/.)

Accordingly, the ECIIA is fully committed to guiding the continuous evolution of Internal Auditing by offering its view and advice in all significant public consultations. For this reason it has set up a working group of Chief Auditors of Insurance Companies to arrive at a common understanding and view of the role of Internal Auditing in the new future legal background of Solvency II.

This document represents the common thinking and position achieved by the working group on this topic and aims at promoting a homogenous approach by its practitioners as well as boosting the cooperation with the European Insurance Authorities. This cooperation is considered vital by the ECIIA to ensure an effective and efficient implementation of the third and fourth level of the Lamfalussy process, consistent with the high level of internal control knowledge and expertise already achieved by Internal Audit.

The document discusses to what extent the internal audit function is already in line with the new requirements of Solvency II, taking into account existing standards for the profession. For this purpose, the starting point for the analysis will be a review of both the Definition of Internal Audit and the IIA Standards, compared to the requirements of the Solvency II Directive. The second part of the document provides clarification of the impact the new processes required by the Solvency II Directive will have on the audit universe including a description of new activities that may be required.



2. DOES THE ROLE OF INTERNAL AUDIT CHANGE WITH SOLVENCY II?

The ECIIA welcomes the fact that with the Solvency II framework the important role of Internal Audit in the system of governance has been acknowledged by the EU for the insurance industry. In particular, the high level of independence of Internal Audit, clearly distinguishing it from the other governance functions, has been emphasized by Solvency II. A high level of independence is a key factor if Internal Audit is to perform its primary role as the assurance function for the Board of an insurance undertaking. The definition of the position, role and tasks of Internal Audit in the Solvency II directive is fully in line with the existing IIA Standards and the generally accepted good practice of the profession (see under 4). Thus Solvency II does not in principle lead to any real change in the role of Internal Audit.

However, the ECIIA acknowledges that - depending on the already existing regulatory framework in the different countries of the EU - in some countries there may still be a long way to go before all internal audit functions in insurance undertakings are fully compliant with the already existing IIA standards and principles. This applies both in respect of the position of Internal Audit, as the independent assurance function in an insurance undertaking, as well as to the specific requirements for Internal Audit according to Solvency II. The ECIIA wishes to support EIOPA by promoting the further development of the internal audit function and by finding practical solutions for the implementation of the Solvency II requirements.

3. SOLVENCY II REQUIREMENTS FOR THE INTERNAL AUDIT FUNCTION

Solvency II leads to some major challenges for Internal Audit. One of the most important of these is Internal Audit's position within the organisation of an insurance undertaking, if it is to fulfil its role as the independent assurance function for the Board. In order to be able to act independently Internal Audit must have direct und unrestricted access to the Board, whose members should receive, as a minimum, a summary of and access to all audit reports. The Head of Internal Audit should report functionally to the Board and administratively to the Chief Executive Officer. Furthermore Internal Audit should have the right to audit any activity of an insurance undertaking at its discretion without any limitation and free of any influence in the performance of its audit. A high level of proficiency and integrity of the auditors is another prerequisite for the independence of Internal Audit.

Solvency II has a profound impact on insurance undertakings by defining a new governance system and requiring the creation of an adequate risk management system. Therefore, Internal Audit also has to extend its activities to including auditing this new framework (see annex 1). These new activities will to some extent require Internal Audit to have different competences than those traditionally required. In particular, the ECIIA believes that Solvency II will require insurance internal auditors to further enhance their technical abilities by, for example, a greater emphasis on general governance, risk assessment and on actuarial skills, in order to be able to ensure confidence in the new legislation and to ensure the right capabilities are in place to assess the controls which should be implemented in the new processes. This may require greater investment in the training and human capital of Internal Audit departments and/or more structured insourcing of skills.

Another challenge lies in the cooperation with the other governance functions, which in many countries have not been mandatory before and for some insurance undertakings will be completely new (see point 5. below). The challenge here will be how to clearly segregate the duties of the different governance functions to avoid, on the one hand, overlapping and duplication of work whilst, on the other hand, ensuring a comprehensive coverage of all risks by these functions. The ECIIA is convinced that using the 3 Lines of Defence model helps companies to structure its governance system in a consistent way by clearly demonstrating the tasks of Internal Audit as the 3rd Line of Defence compared with the other governance functions in the 2nd Line of Defence (see annex 2).

4. THE STANDARDS OF THE PROFESSION

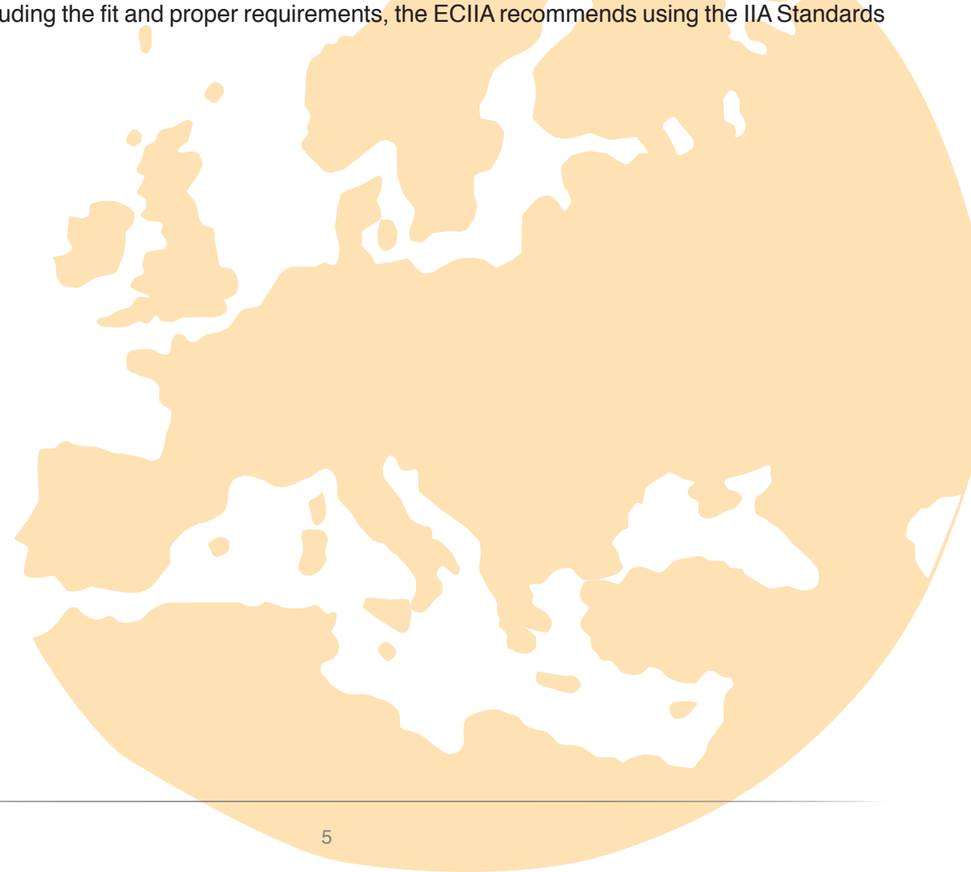
Today, Internal Auditing is generally considered not just a company activity but also a profession, due to the specialised nature of its outputs and its provision of objective, fact based and analytical evaluations. The performance of the Internal Audit function is inspired by principles rather than rules, unlike more standardised activities.

The IIA has helped practitioners to fulfil their objectives by providing the IIA Standards which have the following purpose:

1. To delineate the basic principles for the practice of internal auditing;
2. To provide a framework for performing and promoting a broad range of value added internal auditing;
3. To establish the basis for the evaluation of internal audit performance;
4. To foster improved organizational processes and operations.

In this respect, the IIA Standards are a "permanent lighthouse" in guiding the performance of internal audit activities, so that these may be flexible, adaptable and responsive both to the type of business and the organisation's size and complexity. Internal Audit should adopt these principles and apply them to the operational context. This requires Internal Audit to possess both technical and personal competency. The IIA Standards along with the prerequisite skills allow the Internal Auditor to adapt their audit to respond promptly to changes in the audit universe, which may be the result of changes in business or regulatory requirements. Furthermore, IIA Standards set out the prerequisites to assess compliance with the fit and proper requirements.

Looking at the requirements placed on Internal Audit as set out in the Solvency II guidelines, one can see that these requirements are perfectly in line with the expectations defined by the profession itself. Though the IIA Standards consist of a much more detailed set of guidelines and requirements, the underlying principles are the same. To assess the adequacy of an Internal Audit function in an insurance undertaking under Solvency II, including the fit and proper requirements, the ECIIA recommends using the IIA Standards as benchmark.



5. INTERNAL AUDIT'S ROLE IN THE GOVERNANCE SYSTEM DEFINED BY SOLVENCY II

With the new governance system defined by Solvency II, new functions become mandatory such as the compliance and actuarial functions, in addition to Risk Management and Internal Audit. This can cause unnecessary confusion and duplication of responsibilities, with negative impact on the efficiency and effectiveness of the internal control system. A good coordination between the governance functions is therefore vital for a sound governance system.

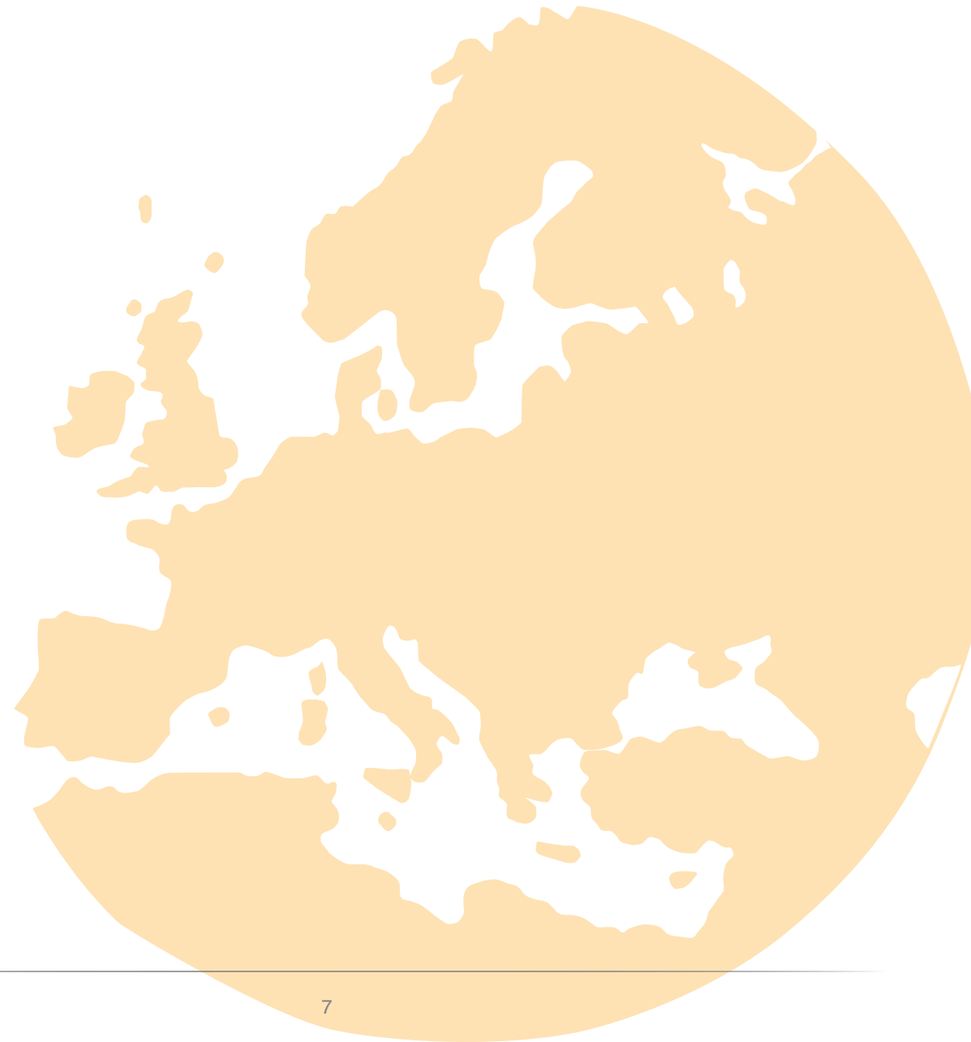
The ECIIA supports the "Three Lines of Defence" (3LoD) - model as a benchmark for future regulatory guidance. This model has been increasingly applied to corporate governance, and particularly risk management, over recent years. The ECIIA finds that it is a useful tool to explain and demonstrate the different roles in governance and risk management, the interplay between them as well as how they fit together to provide stronger corporate governance (see annex 2). The 3LoD-model's basic concept is that Internal Audit is uniquely able to put in place an independent assessment of internal controls, whereas the other company functions, including the 2nd line of defence ones, will be required to influence internal controls directly.

In a Solvency II scenario, the ECIIA expects Internal Audit to:

- regularly review the adequacy and effectiveness of the main governance process installed by other governance functions;
- ensure a fair exchange of information with other governance functions;
- discuss with other governance functions risk categorisation, opinion parameters, reporting tools, materiality metrics etc. and thus enable all governance functions to speak to the Board (including the Audit Committee) using the same language;
- use the output from other governance functions to build independent risk oriented audit plans. Internal Audit should proactively work to enhance effective collaboration, clear responsibilities and peer acceptance with other governance functions in addition to seeking Board approval of the above-mentioned topics.

6. CONCLUSIONS

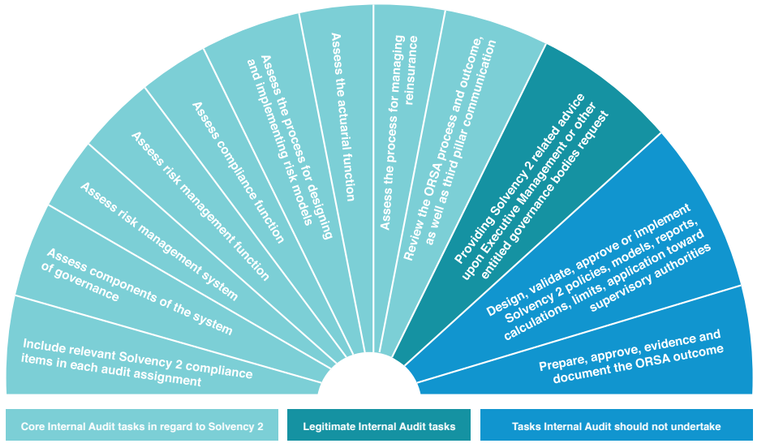
In conclusion, we are of the opinion that the requirements set out in Solvency II as to the work, structure and organisation of an Internal Audit department are not new as they follow the guidelines already defined by the IIA for the profession. However, Solvency II presents a challenge for the profession as there may still be a long way to go for many insurance undertakings to fully comply with the new regulation and the existing IIA Standards. This applies in particular in the area of the independence of Internal Audit. This is crucial, if Internal Audit wants to act as the objective assurance function for the Board. Another challenge is the extension of the audit universe by Solvency II, which requires an internal audit function to possess additional skills. Internal Audit will need to ensure an adequate professional knowledge through and investment in human capital as well as insourcing expertise as appropriate. Last but not least the creation of a new governance system by Solvency II means a challenge not only for Internal Audit but for an insurance undertaking taken as a whole, if the governance system is to work effectively.



Related Internal Audit tasks in the Solvency II framework

As a further explanation of the matters discussed in principle in this paper, the ECIIA believes a dashboard illustration can be useful. The "assurance" tasks to be performed by Internal Audit are listed on the left hand, and the tasks excluded from the internal audit activities are listed to the far right of the dashboard: all these tasks are briefly explained below. It should be borne in mind that not all of these activities are expected to be a part of the audit scope in a given year.

Figure 1 – Internal Auditing's role in Solvency II



1. In respect of "including relevant Solvency II compliance items in each audit assignment", Internal Audit should consider in the audit approach specific steps to evaluate the application of risk related policies, set limits, the review of use tests as well as the reliability of data that will feed risk reporting and the Own Risk and Solvency Assessment ('ORSA') process.

2. Internal Audit should "assess the components of the system of governance" (see art. 41 & art. 47) and make appropriate recommendations for improving it. In particular, Internal Audit should pay specific attention to:
   - the content, approval, application and reporting in respect of the remuneration policy (Advice on System of Governance);
   - the process in place for ensuring compliance with regulatory provisions regarding outsourcing (art. 47-49).

3. The assessment of the "Risk Management function" and of the "Risk Management system" should consider the Solvency II requirements as defined by art. 44. Following the completion of a preliminary risk analysis, Internal Audit should carry out the audit plan by performing periodic evaluations and tests of the overall risk management process, as well as the appropriateness of internal controls. In general, Internal Audit evaluates the independence and the global effectiveness of the insurance company's risk management function (art. 47).

4. The assessment of the Compliance function should consider the European supervisory authorities' requirements, as noted in the Advice on Systems of Governance paragraph (3.232 to 3.250, 3.256-3.258) relating to the Solvency II Directive (specifically in respect of the Compliance function): the requirement for compliance with all legislation and particularly in the areas of Anti Money Laundering and Privacy.

5. In the assessment of the "Process for designing and implementing risk models" special attention should be paid to the control activities implemented for ensuring:

   - the adequacy of the model documentation and of the internal validation procedure;
   - compliance with the procedure to apply in the event of model change;
   - compliance with the reporting requirements;
   - the degree of inclusion of the different risks in the model;
   - the embedding of the model in the risk management;
   - the integrity of the management processing and information systems;
   - the quality of the data sources (consistency, reliability, continuity, timeliness, synchronism);
   - the quality and the accuracy of the model and of the "ex post" control;
   - the quality of the stress testing;
   - the accuracy of MCR & SCR calculation;
   - the use test

   in line with what is set out in Recital 68 and art. 112, but also within the Pre-application process for internal models (formerly CP80).

6. The assessment of the actuarial function should consider the European supervisory authorities' requirements as stated in art. 48.

7. The assessment of the reinsurance management process should include evaluating the achievement of this process's objectives in terms of the company's solvency and profitability as well as the safeguarding of assets through optimisation of the reinsurance coverage in line with the company's risk appetite/ profile. In addition the evaluation should cover the processes for monitoring reinsurers' solvency, ceded reinsurance premiums and claims interventions.

8. Internal Audit, in its assurance role, will review the Own Risk and Solvency Assessment (ORSA) document process and outcome as it will be one of the key strategic decision-making processes of the undertaking as well as an important element in the risk management of the company. This review should facilitate the Board of Directors and Executive Committee in discharging their responsibility to "approve the ORSA policy and to ensure that the ORSA process is appropriately designed and implemented". In order to maintain its independence Internal Audit should not be responsible for the preparation of this document.

The ECIIA believes that the application of all standards implicit in the "Core internal audit tasks" should be included in the audit plan based on a risk based approach.

Possible consulting roles in the Solvency II context

The centre of Figure 1 above shows a global consulting role that Internal Audit may undertake in relation to Solvency II. In general, the further to the right hand side of the dashboard Internal Audit ventures, the greater the safeguards that are required to ensure that its independence and objectivity are maintained. The consulting roles that Internal Audit may undertake relate to "Providing Solvency II related advice upon Executive Management or other entitled governance bodies request".

As far as internal audit principles are concerned, the achievement of Internal Audit's plan must be prioritized over the performance of any consulting activity. In addition, consulting services should not result in operational or management responsibility being taken by Internal Audit. Such responsibilities are not compatible with the assurance role of Internal Audit.

Special attention should be paid to the role of Internal Audit in the Solvency II Project implementation. All European insurance and reinsurance undertaking will have launched major projects aimed at aligning their operations to the new requirements, including the definition, if in scope, of the internal model.

It is the ECIIA's belief that Internal Audit should on the one hand not be completely excluded from these project as they are so central to the structure and performance of the risk management and internal control systems, and on the other hand care must be taken to ensure any involvement in operational activities and the decision-making process does not compromise the requisite independence and objectivity criteria. The Internal Audit function should be prepared to provide support to the company in Solvency II alignment, and in particular in the following areas:

- Governance of the project. Internal Audit should, as a minimum, keep itself informed and updated on the organisation and status of the project and consider certain specific areas for further detailed audit projects. Internal audit may also decide to be more actively involved, e.g. in evaluating the adequacy of the governance of the project and the commitment to the project at the various levels within the organisation.
- Written Policies and Procedures. Normally, Internal Audit includes a review of policies and procedures in its audit plan where appropriate. Internal Audit may, upon request of the project committee, further decide to conduct a review of the adequacy of the proposed procedures and controls. This clearly will not affect the right to conduct an objective ex post audit.
- Data quality. According to existing standards and best practices Internal Audit should consider the adequacy of data quality, irrespective of whether this is Solvency II related or not. The Level 1 text relates data quality to three different criteria: "data used for the internal model shall be accurate, complete and appropriate." (Art. 121(3)). IT auditors or IT auditing expertise are already widely employed in European insurance companies. Internal Audit may decide to develop the audit of this area further, e.g. by evaluating the validation process regarding data quality and/or conducting a specific audit to ensure the quality of the data at an overall or partial level.
- Internal model. Data quality is also an integral part of model validation, "the model validation process shall (…) include an assessment of the accuracy, completeness and appropriateness of the data used by the internal model." (art. 124). Also in this case, an audit of the validation process is consistent with generally accepted auditing standard. This for example means that Internal Audit verifies that the calculations and the algorithms have been prepared from internal/external resources with appropriate competences, that the flow of information and the decisions made are traceable and that an efficient system of controls on subsequent modifications is in place. Too close an involvement in performing the validation exercise (e.g. by the auditors re-performing the calculations, validating the parameters of the algorithms or performing a full or a partial audit on the kernel) could lead to an independence issue.

Once the model is approved, the ECIIA expects that Internal Audit will be asked to support the company by providing assurance in respect of solvency-related topics. The arguments noted above will lead each Head of the Internal Audit Department to evaluate the impact of weaknesses identified in the audited processes in terms of their impact on the solvency of the company. Clearly it would be appropriate for Internal Audit to include specific Solvency II areas (for instance, the third pillar) in the annual audit plan.

Out of the internal audit scope

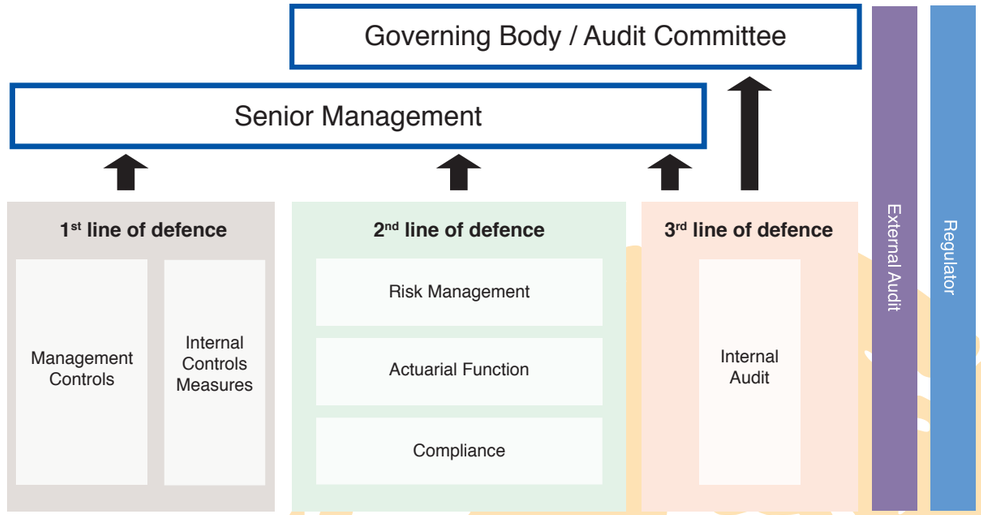
As already noted within the second part of this document, implementation of Solvency II (policies, models, reports, limits, validation etc) is not a mission of Internal Audit. An Internal Audit function will not participate in the design or validation process of the model, nor will Internal Audit participate in the ORSA process (preparing, approving, evidencing and documenting ORSA outcome), nor re-perform the calculation of solvency margins or make quantitative assessments of risk undertaking. Design, implementation, testing and validation of internal models, as stated in article 44 of the Solvency II Directive, are tasks of the risk management function.

The ECIIA also states that Internal Audit will not "prepare, approve, validate, evidence or document the ORSA outcome" to ensure it does not compromise its independent assurance role over the adequacy of processes from an internal control point of view.

"Three Lines of Defence" (3LoD) - model

The ECIIA recognises that, in addition to Internal Audit, senior management and the Board may seek risk and control assurance from other (internal) sources to effectively assume their oversight and monitoring duties. In this respect, the ECIIA supports the "Three Lines of Defence" (3LoD) - model as a benchmark for future regulatory guidance. This model has been increasingly applied to corporate governance, and particularly risk management, over recent years. The ECIIA finds that it is a useful tool to explain and demonstrate the different roles in governance and risk management, the interplay between them and how they fit together to provide stronger corporate governance. This model, which is rapidly gaining universal recognition, can be illustrated as follows:

The three lines of defence model:



- As a first line of defence, operational management has ownership, responsibility and accountability for assessing, controlling and mitigating risks.
- As a second line of defence, the risk management function facilitates and monitors the implementation of effective risk management practices by operational management and assists the risk owners in reporting adequate risk related information up and down the organisation, while compliance is responsible for implementing the necessary procedures to comply with legal and other directives.
- As a third line of defence, the internal auditing function will, through a risk based approach, provide assurance to the organisation's governing body and senior management, on how effective the organization assesses and manages its risks, including the manner in which the first and second lines of defence operate. This assurance task covers all elements of an institution's risk management framework: i.e. from risk identification, risk assessment and response to communication of risk related information (throughout the institution and to senior management and the governing body.)

The document was produced by the following workgroup:

- **Hans Joachim Büsselberg**, ECIIA Board Member, Düsseldorf , Germany
- **Alessandro Busetti**, Head of Group Audit Assicurazioni Generali S.p.A., Trieste, Italy
- **Atila Kas**, Chief Auditor at Generali Belgium SA,Brussels, Belgium
- **Sonia Vicente Alonso**, Directora de Auditoria y Control Interno MMT Seguros, Madrid, Spain
- **Eric Burlot**, Directeur de l'Audit Interne AG2R La Mondiale, Lille, France
- **Enrico Parretta**, Head of Group Audit Cattolica Assicurazioni, Verona, Italy

The publication was overviewed by ECIIA Management Board.