ECIIA
presents

Internal Audit *in the insurance industry Guidance*

ECIIA

Internal Audit in the insurance industry Guidance

June 2019

00 Foreword

The ECIIA is the voice of internal audit in Europe. Our role is to enhance corporate governance through the promotion of the professional practice of internal auditing. Our members comprise 34 national institutes of internal auditing from countries that fall within the wider European region, representing 47 000 members. The ECIIA mission is to further the development of good Corporate Governance and Internal Audit at the European level, through knowledge sharing, developing key relationships, and impacting the regulatory environment, by dealing with the European Union, its Parliament and any other European regulators and associations representing key stakeholders.

The Insurance Committee

The Committee is made up of CAEs from the insurance sector in Europe. The Committee is responsible for ensuring the internal audit profession for the insurance sector in Europe is heard by the EIOPA, the European Insurance Regulator.

The Committee promotes the professionalism of the internal audit function in the European insurance sector through knowledge sharing between the member Institutes and practitioners.

Contributors

This paper was prepared by the ECIIA Insurance Committee.
The delegates from the different countries are:

Hervé Gloaguen, Chair (Germany, Allianz SE)
Thierry Thouvenot (Luxembourg, ECIIA Vice President)
Sonia Vicente Alonso (Spain, MMT Seguros)
Martin Studer (Switzerland, Zurich Insurance Company Ltd.)
Ian Robinson (France, AXA Group)
Stephen Licence (UK & Ireland, Legal and General)
Manfred Schuster (Austria, Uniqa)
Ann-Marie Andtback (Sweden, AMF)
Pascale Vandenbussche (Belgium, ECIIA Secretary General).

We would like to thank everyone involved.

01 Introduction

The Internal Audit function is one of the four key functions identified as material elements of the expected governance system for Insurance undertakings under Solvency II.

The European Confederation of Institutes of Internal Auditing (ECIIA) has issued this document to help interpret the high-level principle-based requirements for Internal Audit functions in Insurance undertakings set under the Solvency II framework[1].

The document aims to enhance the overall effectiveness of Internal Audit, and its impact, in the European Insurance Industry. The intended audience for this pa per is i) individuals heading internal audit functions, ii) executive and non-executive directors (particularly those who are members of Audit Committees), and iii) regulatory and supervisory authorities. The document takes into account existing professional standards and developments in individual European Union member states as well as international bodies and different industry sectors, most notably the banking sector[2].

The guidance provided recognises that significant differences exist in local legislative frameworks and also between different types of insurance undertakings. In this guidance the terms 'Supervisory Body' and 'Executive Management' are used not to identify specific legal constructs but to label the two distinct decision-making functions within all insurance undertakings – most commonly these would equate to a Board of Directors and Executive Management at Board level respectively[3]. The term 'Management' is used to refer more broadly to the wider body of

"The European Confederation of Institutes of Internal Auditing (ECIIA) has issued this document to help interpret the high-level principle based requirements for Internal Audit functions in Insurance undertakings set under the Solvency II framework."

1 In a Group context with entities that are not covered by the EU Solvency II Directive it is for the Head of the Group Internal Audit function, through their documented policies, to determine if the expectations detailed in this paper apply equally to those Internal Audit functions outside the scope of the EU Solvency II Directive. It is a requirement of Article 41 of the Solvency II Directive that these policies be appropriately approved.

2 See source reference

3 Whilst this is one possible split, it is not universal across all countries or entities – it is equally possible that the Management Board be defined as the Supervisory Body thus Executive Management and Supervisory Body may be one and the same in some instances.

within an Organisation and is not limited to Executive Management. The guidance also references the 'Audit Committee' which is the governance body providing oversight of the Insurance undertaking's Internal Audit function on behalf of the Supervisory Body (although it needs not necessarily be termed the 'Audit Committee' in the Organisation); 'Organisation' is used to refer to the legal entity regardless of its actual legal construct and 'Chief Executive Officer' is used to refer to the most senior member of Executive Management.

'Supervisory Body' should not be confused with 'Supervisory Authority' which is the body established by the member state to supervise the insurance industry (e.g. BaFin in Germany, ACPR in France, etc).

The principles and guidance set out in this document should be applied in accordance with the national legislation and corporate governance structures applicable in each country and should be applied in conjunction with the existing International Professional Practices Framework published by the Institute of Internal Auditors (IIA) and other applicable codes.

This guidance applies to all Insurance undertakings subject to the Solvency II Directive, regardless of the nature and status of the wider Group within which those activities may reside. Where modifications are felt to be needed for the size or risk profile of insurance undertakings, this is specifically referenced in the guidance.

This guidance is intended to set the high-level expectations and should be viewed as a benchmark of good practice to help strengthen corporate governance. It is anticipated that further guidance on more granular subjects will be issued by the ECIIA in the future.

Role of Internal Audit

The Internal Audit function provides independent assurance to the Supervisory Body and Executive Management on the adequacy of the design and effectiveness of the Organisation's systems of internal control, including risk management, governance and operational processes, thereby helping them protect the assets, reputation and future sustainability of the Organisation.

The core features expected of an Internal Audit function are:

Independence

1.1 The Audit function must have sufficient standing and authority within the Organisation to carry out its activities with independence and objectivity. This should be demonstrable through the formal authority given to the Internal Audit function by the Supervisory Body; the reporting line of the Head of the Internal Audit function; the remuneration arrangements of the Internal Audit Staff; the activities performed by the Internal Audit function; the reporting of Internal Audit's findings; and Management's response to those findings.

1.2 The Head of the Internal Audit function must have a reporting line to a senior non-executive director (e.g. the Chair of the Audit Committee) with periodic meetings to maintain an ongoing dialogue and enjoy unfettered access to the members of the Supervisory Body (e.g.

through the Audit Committee) as required. In the Executive Management structure, the reporting line of the Head of the Internal Audit function is expected to be to the Chief Executive Officer[4], although in a Group context the CEO reporting line is expected to be secondary to a functional reporting line to the Group Head of the Internal Audit function.

1.3 Subject to ratification by the Supervisory Body, the Audit Committee[5] is responsible for the appointment of the Head of the Internal Audit function who, in line with the fit and proper requirements under Solvency II (Directive 2009/138/EC, EU 2015/35 Article 273) is suitably qualified to perform the role with no conflicts of interest and of suitable character; as well as the removal of the Head of the Internal Audit function. It is also expected that the Chair of the Audit Committee[2] be aware of, and endorses, the objectives of the Head of the Internal Audit function and the Internal Audit function, and be involved in the assessment of the Head of Internal Audit against these objectives on at least an annual basis.

1.4 Subject to ratification by the Supervisory Body, the Audit Committee is responsible for the approval of the plan of Internal Audit work to be performed[6] and, inter alia, for the budget for the running of the Internal Audit function.

1.5 As a key part of the governance structure of the Organisation, it is expected that both Executive Management and the Supervisory Body ensure that the Organisation has an Internal Audit function resourced in a manner commensurate with its operations and the complexity of the Organisation (the proportionality principle).

1.6 The Head of the Internal Audit function provides the Audit Committee[7] with a professional view on the adequacy of both the quantity and quality of the resource available to the Internal Audit function on at least an annual basis.

1.7 Remuneration is often cited as one of the areas where independence and objectivity are most at risk. It is expected that the remuneration policy be demonstrably in line with the remuneration principles set out in the Solvency II Directive.

1.8 Similarly, the tenure of the Head of the Internal Audit function is often cited as a factor that could impair objectivity. It is expected that the Chair of the Audit Committee considers this each year when appraising the performance of the Head of Internal Audit.

1.9 The Internal Audit function does not perform any operational functions and internally recruited Internal Audit staff do not audit the operational functions from which they came for a period defined within the policies and procedures of the Internal Audit function. The Solvency II Directive (EU 2015/35 Article 271) does allow the Internal Audit function to perform operational functions under specific circumstances. These expectations do not preclude the Internal Audit function from performing 'ad-hoc' advisory or investigative work[8] at the request of the Audit Committee or Executive Management.

1.10 Whilst the Head of the Internal Audit function is permitted to plan and perform their work with due regard to Executive Management's comments, ultimately they must do this without undue interference or influence from them. It is expected that all Organisations have an Internal Audit Charter that articulates the purpose, responsibilities and authority of the Internal Audit function within the Organisation. Expectations around the Charter are provided in Appendix I.

1.11 The Head of the Internal Audit function is allowed to present the findings of Internal Audit's work to the Audit Committee without interference from the CEO or other members of Executive Management.

1.12 The Head of the Internal Audit function has open and unfettered communication lines with the External Auditors of the Organisation.

1.13 The Head of the Internal Audit function has open communication lines with the relevant Supervisory Authorities covering the Organisation[9].

1.14 The Internal Audit function has a demonstrable and open two-way sharing of the results of its respective work with the second line of defence functions, subject to this not impairing any duties or activities of the Internal Audit function.

1.15 The Head of the Internal Audit function defines the strategy and determines the organisation of the function. In a Group context, it is expected that the Group Head of the Internal Audit function defines the strategy and determines the organisation of the Internal Audit function both at the parent and subsidiary levels in the Organisation[10]. It is expected that the strategy sets out the audit methodology, quality assurance and sourcing strategy measures as a minimum.

1.16 Where the Internal Audit function uses external resource, either to alleviate temporary resource constraints or to provide access to particular specialisms, it is expected that the Head of the Internal Audit function requires that the other party (within the same Group or external) complies with the Internal Audit Charter and Internal Audit policy applicable to the Organisation's Internal Audit function.

4 The reporting line may also be solely to the non-Executive Chairman if a reporting line to the CEO is not considered appropriate.

5 Where the Supervisory Body has delegated this authority to the Audit Committee; where the authority is not delegated then the Audit Committee is expected to propose a course of action to the Supervisory Body. In a Group context it is expected that the Group Head of the Internal Audit function assist in this matter.

6 In a Group context at the consolidated level this need not replicate the work performed by subsidiary audit committees.

7 Alternatively this may be presented directly to the Supervisory Body.

8 The independence afforded to the internal audit function, as well as its access and insight into the Organisation, mean that it may be an appropriate candidate to perform triage on whistle-blowing incidents in addition to investigations arising from them.

9 Although the frequency and content of the communications are to be initiated by the relevant local Supervisory Authority it is expected that the Head of the Internal Audit function equally consider when communications are required given the applicable regulatory environment: as a minimum providing the Supervisory Authorities with the information that they request.

10 In line with local laws and regulations and in consultation with the relevant Audit Committees.

1.17 If an Internal Audit function is outsourced in its entirety to an external party then it is the responsibility of the Supervisory Body to ensure that the external party complies with professional standards and guidance as if it was an internal Internal Audit function.

1.18 Where an external party is used to perform internal audit work, it is expected the external party has not previously performed an engagement that would be the subject of an internal audit review unless a "cooling off" period that is explicitly acceptable to the Audit Committee has elapsed[11].

Professional competence and due professional care

2.1 It is expected that the Head of the Internal Audit function demonstrably meets the requirements of being a fit and proper person for the role and that there be documented procedures to assess this in accordance with Articles 41 and 42 of the Solvency II Directive 2009/138/EC. It is expected that, as a minimum, the proposed appointment and replacement of the Head of the Internal Audit function be communicated to the Organisation's relevant Supervisory Authority together with the rationale for the change being made.

2.2 Where the Head of the Internal Audit function changes, it is recommended that a representative of the Audit Committee conducts a documented exit interview with the outgoing Head of the Internal Audit function (in addition to, and separate from, the CEO).

2.3 The Head of the Internal Audit function is expected to consider the qualifications, skills and experience of internal audit staff to ensure that there are competent resources available to cover all the areas within the plan of Internal Audit work to be performed. Confirmed access to resource from outside the Internal Audit function (whether that be within the Organisation or from external providers) should be noted and factored into the consideration behind the Head of the Internal Audit function's periodic confirmation on the adequacy of resource to both Executive Management and the Audit Committee in terms of qualification and quantity. Adequacy of resources should be formally confirmed on at least an annual basis with any significant shortfalls arising between annual confirmations also highlighted.

2.4 The Head of the Internal Audit function is expected to ensure that Internal Audit staff receive appropriate ongoing training in order to maintain competence, meet the changing nature of the Organisation's activities and the evolving risk environment, the diversity of tasks that need to be undertaken and the need to be able to make an appropriate impact in the Organisation.

2.5 It is expected that the Internal Audit function documents and demonstrably follows a policy for ensuring the quality of its own work (and that of third parties where audit work is outsourced). As a minimum, it is expected that an external review of the performance of the Internal Audit function be performed at least once every 5 years. Such a review would be expected to be against the IIA Standards and Code of Ethics and applicable local laws and regulations as a minimum. It is expected that, subject to ratification by the Supervisory Body, the Chair of the Audit Committee oversees and approves the appointment of the independent assessor and receives the resultant report. In a Group context, it is acceptable for the review of subsidiary Internal Audit teams to be performed by independent staff from the Head Office team or a peer internal audit team who are not directly involved with the Internal Audit activity being reviewed when overseen by the Group Internal Audit function.

2.6 It is the responsibility of the Head of the Internal Audit function to discuss and confirm with the Audit Committee (or directly with the Supervisory Body) the programme of internal assessment work required to provide assurance on the quality of its work between external reviews[12]. A summary of the results of internal quality assurance work are expected to be presented to the Audit Committee.

Professional Ethics

3.1 The Head of the Internal Audit function is expected to ensure that the Internal Audit function applies the Organisation's code of ethics where there is one or the Global IIA code of ethics where the Organisation has none. Should the codes conflict, or should the Organisation's code not cover the key areas set out in the Global IIA code, then it is expected that the Head of the Internal Audit function documents a code of ethics for the Internal Audit function in line with that of the IIA and requires staff to adhere to it.

"It is expected that the Head of the Internal Audit function demonstrably meet the requirements of being a fit and proper person for the role and that there be documented procedures to assess this(...)"

11 A cooling off period of at least 12 months would be expected.

12 This may be achieved through a more frequent external review.

Internal Audit Work

The Internal Audit function fulfils its role by assessing whether the significant risks of the Organisation are appropriately identified and reported by Management[13] to the Supervisory Body, assessing whether those risks are mitigated appropriately and assessing whether the Organisation operates in an efficient and effective manner.

The Internal Audit function is expected to document the policies and procedures that it follows. It is expected that these encapsulate, but do not contradict, requirements set by the IIA and that the high-level policies therein be reflected in an Internal Audit Charter[14] which must be formally reviewed and approved by the Supervisory Body on at least an annual basis.

It is expected that the Head of the Internal Audit function agrees with the Audit Committee goals and measures to objectively assess and report upon the performance of the Internal Audit function to the Audit Committee.

The following expectations are not intended to provide a comprehensive summary of IIA, SII or other requirements but are highlighted as areas to be specifically considered by Internal Audit functions within Insurance organisations:

Planning

1.1 Demonstrably consider a scope that covers all legal entities and activities under the control of the Organisation and ensure that, in the first year that an activity or legal entity falls within the scope of an Internal Audit function, an assessment be performed to allow the audit universe to be established and a plan of work established.

1.2 Form its own judgement on the risk profile of the Organisation. This view should be informed by the views of other Management areas including the second line activities, but not determined by them. It is expected that, as a minimum, this view be presented to the Audit Committee when the principal planning decisions are to be made for the work of the Internal Audit function.

1.3 Maintain awareness of changes in the Organisation, strategy and other relevant factors, such as changes in regulations or emerging risks in the industry, to ensure that their risk assessment and plan of work remain appropriate.

13 Including the second line functions.

14 See Appendix I.

1.4 Ensure that the plan be sufficiently flexible to allow the Internal Audit function to respond to specific events or changes in the structure or risk profile of the Organisation. It is expected that material changes to the plan of work be communicated to and approved by the Audit Committee.

1.5 Ensure that the scope of work includes all the systems of governance and control, including the Key Control Functions (Risk Management, Actuarial, Compliance – not least to determine if reliance can be placed upon their work

"The Internal Audit function is expected to document the policies and procedures that it follows. It is expected that these encapsulate but do not contradict requirements set by the IIA and that the high-level policies therein be reflected in an Internal Audit Charter which must be formally reviewed and approved by the Supervisory Body on at least an annual basis."

to limit audit sampling) and the controls operated within support functions such as IT, Human Resources and Finance.

1.6 Have a policy and process to establish, implement and maintain an audit plan setting out the audit work to be undertaken in the upcoming years, taking into account all activities and the complete system of governance of the Organisation.

1.7 Have access to all the Organisation's records (including sensitive information such as staff and client information and Board or Management Committee papers) where they are necessary to discharge its responsibilities.

Performance

2.1 Evaluate the design and operating effectiveness of the Organisation's key policies, procedures and controls including, but not limited to:

Procedures and controls in place to ensure appropriate levels of adherence to applicable laws, regulations and Supervisory Authority requirements that are significant to the Organisation.

The risk and control culture of the Organisation and agree with the Audit Committee if and how this should be reported upon[15].

The control framework ensuring the reliability, effectiveness and integrity of key management information systems and processes (including relevance, accuracy, completeness, availability, confidentiality, integrity and comprehensiveness of data).

The control framework over modelling and management of the Organisation's capital and

15 This should include assessing whether the processes, actions, and observed behaviours (including the 'tone from the top') are in line with the spirit of the espoused values, ethics, risk appetite and policies of the Organisation

liquidity risks, as well as evaluating the means of verifying the liabilities of the Organisation.

The means of safeguarding and verifying policyholder assets as well as those of the Organisation and ensuring that the assets of the two remain appropriately segregated.

2.2 For material outsourced activities the Internal Audit function must ensure that the activity is included in its Audit Universe and, as a minimum, perform audit work on the Organisation's management of the outsource relationship. Additionally, it is expected that, as a part of the scoping of an audit assignment where there is a significant aspect of the operation that has been outsourced, there be formal consideration of the level of internal audit work (if any) required to be performed on the work performed by the outsource provider.

2.3 Have a written policy regarding the approach to significant projects/ business change programs and the types of Internal Audit work that are undertaken upon them.

2.4 Verify, though testing, the resolution by Management of internal audit issues raised before they are closed in the records and reporting of the Internal Audit function.

2.5 Have a written policy regarding record retention to ensure that, subject to applicable local laws, evidence of the work performed to support the results and opinion of the Internal Audit function is maintained.

Reporting

To ensure a meaningful dialogue with the Audit Committee and other stakeholders the following items should be considered and discussed with stakeholders to determine a reporting set that is both comprehensive and best suited to the Organisation.

3.1 Planning

The scope of the audit universe (legal entity and activity based).

An assessment of the inherent risk and control environment of the audit universe.

The methodology to determine the risk based audit cycle to cover the scope.

A summary of the plan of work proposed and the resource required to cover it (including any resource required from outside the Internal Audit function)[16].

A summary of any significant assignments that are added or removed from the plan[17].

3.2 Findings

A summary of the reports issued in the period under review and the rating (where applicable) of each of the reports[18].

16 In a Group context this summary would not be expected to cover every audit to be performed so long as that is covered at the entity Audit Committee level.

17 In a Group context this summary would not be expected to cover every audit to be performed so long as that is covered at the entity Audit Committee level.

18 In a Group context this may be a simple list of audit reports issued and the rating of the reports – with a summary of those reports or issues considered significant enough to bring to the attention of the Group Audit Committee.

Significant findings arising from Internal Audit work performed in the period.

On at least an annual basis, a summary of any thematic and/or recurring issues and root causes of the issues identified across the Organisation.

3.3 Resolution of Issues

A list of any audit reports where Management action plans in response to audit reports have not been received or are not considered appropriate[19].

A summary of any issues arising from Internal Audit reports where Management propose not to perform any remedial action but to continue to operate with the weakness identified by Internal Audit[19].

A summary of those issues where the original target date set for resolution is no longer applicable because of fundamental changes in the operating environment[19].

A summary and aging of those issues that remain unresolved after the date proposed by Management for resolution (i.e. overdue issues).

19 In a Group context the level of detail in the summary reporting is not expected to be at a granular level, but rather directional to allow the Group Audit Committee to discern if there are any particular issues in the Organisation's entities below the Group level.

3.4 Overall Opinion

On at least an annual basis an assessment from the Head of the Internal Audit function on the overall effectiveness of the governance and risk and control framework of the Organisation.

3.5 Resourcing[20]

A summary of the actual audit resource deployed compared to the budgeted amount required to complete the audit plan.

A statement from the Head of the Internal Audit function on at least an annual basis regarding the adequacy of resources afforded to the Internal Audit function.

Annual confirmation of the independence and objectivity of the Internal Audit function and staff (disclosing any potential conflicts of interest that may have arisen).

A summary of the professional skills held by, and the training provided to, the staff of the Internal Audit function.

Whilst the Internal Audit function is responsible for the findings of its reviews, it is expected that Management be held accountable for responding to the matters identified and setting both the actions to be performed and the target dates for completion of those actions.

20 It is expected that this would cover both financial and staffing information to reflect the ability to use external resource where internal staffing is not available

Appendix I

*Internal Audit Charter **

03

*Appendix I Internal Audit Charter**

It is expected that the Internal Audit Charter be reviewed and approved at least on an annual basis by the Audit Committee or Supervisory Body.

It is expected that the Internal Audit Charter establishes, as a minimum, the following:

i. A clear description of the role of Internal Audit within the Organisation and the governance framework.

ii. A statement as to the independence of the function detailing its reporting lines and any other mechanisms in place to ensure its independence.

iii. A summary on the scope of the work of the Internal Audit function detailing any limitations imposed.

iv. A summary of the responsibilities of the Internal Audit function.

v. A statement as to the authority granted to the Internal Audit function and the permissions it entails[1].

vi. A statement regarding the process to engage external resource where required.

vii. A requirement to comply with IIA standards, ECIIA guidance and any other applicable professional requirements.

viii. A statement on cooperation with the Organisation's External Auditors.

ix. A statement that allows the Internal Audit function to perform a review of any area or any function consistent with its mission on its own initiative

x. A statement on the process and conditions whereby the Internal Audit function can be called upon to provide non-audit assignments such as consulting, advisory or investigation assignments.

For listed Organisations, it is expected that this Charter be made available on the Organisation's website, or be accessible to staff, shareholders and stakeholders upon request if no website exists.

1 The Charter should empower the Internal Audit function, whenever relevant to the performance of the assignment, to initiate direct communication with any member of staff, to examine any activity of the Organisation, and to have full access to any records, files, data or physical property of the Organisation.
*As defined in IG 1000 of IPPFs

Source Material

European Banking Authority – 'Guidelines on internal governance'.

Basel Committee on Banking Supervision – 'The internal audit function in banks'.

Chartered Institute of Internal Auditors – 'Guidance on Effective Internal Audit in the Financial Services Sector' (Second Edition).

International Association of Insurance Supervisors – 'Insurance Core Principles, Standards, Guidance and Assessment Methodology' (including ComFrame material integrated into ICPs 5, 7 and 8 for consultation March 2017).

Global Institute of Internal Auditors – 'International Standards for the Professional Practice of Internal Auditing' (January 2017).

European Parliament – EU Solvency II Directive (2009/138/EC).

EIOPA – Guidelines on System of Governance.

Design by **Alentexas Design Co.**

Head Office
Rue Royale 109–111
Bus 5, BE–1000
Bruxelles, Belgium
www.eciia.eu

Contacts
Email: info@eciia.eu
Twitter: @EciiaInfo

Team
Pascale Vandenbussche
Carolina Baltazar