POSITION PAPER

INTERNAL AUDIT OVERSIGHT OF OUTSOURCING IN INSURANCE UNDERTAKINGS

Internal audit oversight of outsourcing in Insurance Undertakings

POSITION PAPER

ABOUT ECIIA

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 34 national institutes of internal audit in the wider geographic area of Europe and the Mediterranean basin. The mission of ECIIA is to be the consolidated voice for the profession of internal auditing in Europe by dealing with the European Union, its Parliament and Commission and any other appropriate institutions of influence. The primary objective is to further the development of corporate governance and internal audit through knowledge sharing, key relationships and regulatory environment oversight.

CONTENT

INTRODUCTION:

FUNDAMENTALS:

INTRODUCTION

ECIIA

ECIIA set up an Insurance Committee[1] in 2012 with Chief Audit Executives of the largest European Insurance companies.

The mission of the ECIIA Insurance Committee is: "To be the consolidated voice for the profession of Internal Audit in the Insurance sector in Europe by dealing with the Regulators and any other appropriate institutions of influence at European level and to represent and develop the Internal Audit profession as part of good corporate governance across the Insurance Sector in Europe ».

ECIIA represents around 47.000 internal auditors and around 12.000 are active in the insurance sector. The paper describes best practice, but it is important to note that, depending on the culture, size, business and local requirements (Supervisor, country,…), other options are possible.

Thesis

The internal audit function has an important role to play in providing assurance over the effectiveness and security of key processes outsourced from (re)insurance undertakings to third parties. It is crucial that key stakeholders, including management, the board and the (re)insurance undertaking's supervisors can place reliance on the work of internal audit in respect of the risk management of third parties, while at the same time maintaining a reasonable expectation of the extent of the internal audit function's responsibilities in this area.

This paper sets out the view of the ECIIA Insurance Committee (the Committee). It is based on the position paper on Internal Audit Oversight of external outsourcing issued by the ECIIA Banking Committee, on relevant regulations from EIOPA/EBA/ and on best practices that could be adopted by internal audit functions in respect of the audit of externally outsourced services. This paper was adapted to the specifics of the (re)insurance undertakings, in particular the regulatory requirements of Solvency II. This paper:

- ✓ Does not consider outsourcing of internal audit as a function
- ✓ Does not consider in details internal outsourcing (from one legal entity to another within the same group), albeit many of the same concepts could be applied.

[1] Amaury De Warenghien (Axa), Stephen Licence (Legal & General), Nora Guertler (Generali), Ann-Marie Andtback Beckman (Sampo Group), Martin Studer (Zurich), María Luisa Gordillo Gutierrez (MAPFRE), Manfred Schuster (Uniqa Group), Hervé Gloaguen (Allianz Group)

Background

An organisation retains the ongoing responsibility to ensure that outsourced processes are effectively controlled and cannot 'outsource responsibility'. Further, the outsourcing of material activities can increase the operational risk to which the (re)insurance undertaking is exposed.

Outsourcing of operational activities to third parties by financial institutions is not a new phenomenon. However, in recent years the number of outsourced activities, the importance of the processes outsourced, the complexity of processes outsourced has continued to increase, as has the inherent risk associated with the transfer of client data outside the organisation. Therefore, the importance of strong sourcing and supplier management frameworks within the first line of defence continues to increase, as does the need to ensure adequate monitoring and oversight from the second and third lines.

This paper explores the following fundamental aspects of the internal audit function's role in respect of third-party risk management:

1. **Recognition of outsourced activities within the 'audit universe' and risk assessment**
2. **Key areas of focus for internal audit:**
    a. sourcing process
    b. supplier management framework
    c. third-party audits
    d. Intra-Group outsourcing
3. **Testing of and placing reliance upon:**
    a. first- or second-line assurance functions
    b. the work of the internal audit department of the service provider
    c. the work of external assurance providers

FUNDAMENTALS

1 RECOGNITION OF OUTSOURCED ACTIVITIES WITHIN THE 'AUDIT UNIVERSE' AND RISK ASSESSMENT

The Institute of Internal Auditors (IIA) International Professional Practices Framework (IPPF) outlines under standard '2010 – Planning' the need for the Chief Audit Executive to develop a risk-based audit plan, based on a documented risk assessment. The plan should respond to changes in the organisation's business, risk, operations, programmes, systems and controls.

In practice this is usually achieved by the internal audit function through a representation of the (re)insurance undertaking's activities within a defined 'audit universe' which is then subject to a risk assessment(compliance, financial, operational, IT risks) to determine the relative priorities for the audit plan.

According to Article 274 p 1 (Solvency II) any (re)insurance undertaking which outsources or proposes to outsource functions or (re)insurance activities to a service provider shall establish a written outsourcing policy which considers the impact outsourcing on its business, and the reporting and monitoring arrangements.

Outsourced activities should be fully integrated into the 'audit universe' and subject to the same inherent risk assessment process as those operations undertaken 'in-house' directly by the (re)insurance undertaking.

In determining the residual risk (after considering the effectiveness of the operation of controls), the internal audit function may consider the results of testing by first or second line assurance functions (where they have been tested by internal audit and found to be operating effectively) and the work of external parties (including the service provider's own internal audit function), in line with the provisions outlined under Fundamental 3 below.

An appropriate audit response should then be determined, based on the output of the internal audit annual risk assessment, relative to the perceived risk associated with all other activities within the (re)insurance undertaking (i.e. in line with the usual risk-based planning cycle).

In addition to representation of the outsourced processes itself, the (re)insurance undertaking's own sourcing and supplier management processes should be covered in the 'audit universe' and be subject to risk assessment and regular risk-based audits.

2 KEY AREAS OF FOCUS FOR INTERNAL AUDIT

It is management's responsibility to set up appropriate frameworks to manage supplier risks, and the role of the internal audit function is to assess the effectiveness of the (re)insurance undertaking's supplier risk management frameworks. The risk assessment, the control measures to mitigate the risks and the SLA management should be assessed by internal audit at supplier/outsourced process level In cases where the (re)insurance undertaking does not have an effective supplier risk management framework, the internal audit function should consider what alternative approaches might be necessary. As a

minimum, a test of design should be performed.

a. Sourcing process/outsourcing policy?

The internal audit function should not have a direct role in approving the outsourcing of specific processes as this could impair its independence. Rather, internal audit's role is to review whether appropriate frameworks are in place to select suppliers (including the performance of appropriate supplier due diligence, conflict of interest policy) and to ensure that governance over the decision-making process involves all relevant parties and adequately assesses risk of any potential outsourcing activity. The institution should maintain a register of all outsourcing arrangements that should distinguish between the outsourcing of critical or important operational functions and others.

The internal audit function should establish that there is a written outsourcing policy in place which considers the impact of outsourcing on the (re)insurance undertaking's business and the reporting and monitoring arrangements to be implemented in cases of outsourcing (Solvency II (Delegated Regulation 2015/35), Article 274 Outsourcing 1.) In case of outsourcing any critical or important functions or activities, the criteria set by Article 274.3. for choosing the service provider must be fulfilled.

The internal audit function should, verify the organisation's contractual standards for third party arrangements are in place. Specifically, the written agreement clearly defines the respective rights and obligations of the undertaking. Specifically, the service provider clearly states that all requirements of the Article 274.4, including a 'Right to Audit' in the terms agreed with any service providers.

Compliance with the requirements for outsourcing of critical or important functions or activities as defined by the Article 274.5 should also be considered in the audit review.

In determining whether an outsourced function or activity is critical or important, the undertaking must consider any definition or list of such functions or activities provided under national law or national administrative interpretation. Where functions or activities are partially outsourced it is relevant whether these outsourced parts are per se critical or important (EIOPA System of Governance Guideline 48, Article 49 Solvency II).

b. Supplier management

Internal audit should review and assess the adequacy of the (re)insurance undertaking's supplier management framework, considering whether this provides enough governance and oversight of key outsourced activities.

In practice a (re)insurance undertaking's supplier management process may include several different components including the chain of sub suppliers of the supplier. The internal audit function should consider the relative significance of these, and determine an appropriate audit approach, in the context of the specific circumstances of the institution.

Internal audit should check whether roles and responsibilities are assigned and being exercised. As a minimum the internal audit function should define any areas of the supplier management process where it may seek to place reliance for its own risk assessment as an alternative to undertaking direct third-party testing at the supplier.

Examples may include (a) the supplier risk assessment process (which typically determines the materiality of the supplier and consequently the level of oversight via the supplier management process) and (b) the operation of a first- or second-line supplier assurance function.

Based on Solvency II regulation, on site responsibility is required for outsourcing activities.

In the case of (a), the internal audit function should document that any risk assessment procedures accurately assess the materiality of the processes undertaken by the supplier, especially if the internal audit function intends to leverage this to complete its own supplier risk assessment. They should perform at least a test of design. It is also important to include special mentions in the outsourcing contract (right to audit, check list of processes to audit…).In the case of (b), the internal audit function should consider the adequacy of the scope and quality of the work executed by any first- or second-line supplier assurance function, including where appropriate using reperformance testing.

c. Third-party audits

Based on internal audit's own risk assessment, the internal audit function may choose to perform direct 'third-party audits' on site at the service provider.[2] Typically, these will involve detailed testing of the relevant operational controls executed by the service provider over the outsourced processes as well as considering the general governance arrangements within the supplier to effectively manage the key risks to which the outsourced process is exposed for instance business continuity planning.

Prior to initiating a third-party audit, the internal audit function should also consider the practicalities of such an undertaking (for example having the right skills and capabilities required to perform the third-party audit).

d. Intra-group Outsourcing

The extent to which an undertaking controls the service provider or has ability to influence its actions should be considered when outsourcing critical or important functions or

[2] EIOPA - Guidelines on outsourcing to cloud service providers
Guideline 11
43 g. retain the contractual right to perform individual on-site audits at their discretion with regard to the cloud outsourcing of critical or important operational functions or activities; such right should be exercised in case of specific needs not possible through other types of interactions with the cloud service provider.

activities (Solvency II Commission Delegated Regulation Art. 274 (4)). Intra-group outsourcing is not inherently less risky than outsourcing to external service providers and is not differently treated under current requirements. While compared to the external service provider, the risks subject to due diligence appear lower in an intra-group outsourcing, following are examples of risks which may become more prominent:

i. Risks arising from conflicts of interest, including those associated with the on-going management of the service provider should be identified and managed accordingly. When functions are provided by a service provider that is part of a group, the outsourcing conditions should be set at arm's length. The outsourcing agreement must fulfil all the requirements set out in Article 274 (4) and due to the circumstances might be subject to an external evaluation.

ii. Where the group companies fully rely on sharing a large centralized internal service provider, the concentration risk must be evaluated, including consideration and the extent of coverage in the business continuity planning.

iii. Where the service provider is in a jurisdiction not subject to equally strict data protection rules, the data protection risk needs to be considered.

In case the group operates in multiple countries, local regulatory restrictions in outsourcing whole or parts of key functions and activities must be considered

3 TESTING OF AND PLACING RELIANCE UPON THE WORK OF OTHERS

a. First and second line assurance functions

The Internal audit function may choose to use the work of the (re) insurance first or second line assurance functions to inform their own risk assessments of the control environment at suppliers, where the effectiveness of these functions has been adequately tested. This may result in the internal audit function choosing not to perform detailed third-party audits at suppliers where sufficient testing has already been performed by another assurance function within the (re)insurance undertaking and the internal audit function has satisfied itself of the effectiveness of that function.

b. Internal audit department of service providers

Where the internal audit function intends to place reliance on the work of internal audit at the service provider, the internal audit function should undertake sufficient testing of that function's activities, including completing reperformance testing, to determine the effectiveness of the function. The internal audit function may also enquire as to whether the

service provider's internal audit department has been subject to an external quality assessment in line with the recommendations of the IPPF standard. Joint audits might also be organised.

A key concern in respect of partnerships with vendor's is the security of client data which may be transferred. Wherever possible (re)insurance undertakings should use strong cryptographic measures to protect data residing on and in transit through supplier systems (such as cloud) and retain control of the cryptographic keys. This can allow a (re)insurance undertaking to have strong assurance that data is adequately protected from compromise with minimal testing of the controls operating at the service provider. The internal audit function can then focus testing on specific processes such as cryptographic key management.

The internal audit function also needs to carefully assess whether the (re)insurance undertaking has the capability to understand and manage the risk associated with vendor's. For example, does the (re)insurance undertaking have enough expertise to evaluate the security of cryptographic processes in use at vendor's? If not, then the risk associated with using vendor's and their technology may not be effectively understood or managed. The internal audit function also needs to carefully assess its own capabilities to audit vendor's, cloud providers.[3]

c. External assurance providers

In certain cases, the service provider may commission a third party to complete an independent controls assessment – for example an International Standard on Assurance Engagements (ISAE) 3402 'Service Control Report' (Type II). In assessing the use of controls assessments such as ISAE 3402,[4] the internal audit function should carefully consider whether the scope of the assessment corresponds with the scope of the third-party risk and the insurance undertaking has enough expertise available to assess the assurance reports. In many cases it is necessary to supplement the scope of an ISAE 3402 with additional risk management processes.

In all the above cases (a,b,c), the internal audit function should follow up on the resolution of control issues raised by other assurance suppliers, and this should also form an input to the internal audit function's own risk assessments.

[3] EIOPA – Guideline 11: Guidelines on outsourcing to cloud service providers

[4] Or SOC1 type 2, SOC 3 etc. ,ISAE3000

c/o European
Corporate Governance House
Avenue des Arts 41
1040 Brussels, Belgium
Phone: +32 2 217 33 20
TR: 849170014736-52
www.eciia.eu