POSITION PAPER

INTERNAL AUDIT OVERSIGHT OF EXTERNAL OUTSOURCING

ENHANCING GOVERNANCE THROUGH INTERNAL AUDIT

2

ABOUT ECIIA

The European Confederation of Institutes of Internal Auditing (ECIIA) is the professional representative body of 35 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.

CONTENTS

ECIIA Head Office:

c/o IIA Belgium
Koningsstraat 109-111
Bus 5, BE–1000
Brussels, Belgium

Phone: +32 2 217 33 20
Fax: +32 2 217 33 20
TR: 849170014736-52

www.eciia.eu

3

INTRODUCTION

ECIIA set up a Banking Committee in 2015 with Chief Audit Executives of European Central Bank Supervised Banks[1]. See the European Central Bank website for a full list of supervised entities.

The mission of the ECIIA Banking Committee is:

"To be the consolidated voice for the profession of internal auditing in the Banking Sector in Europe by dealing with the European Regulators and any other appropriate institutions of influence and to represent and develop the Internal Audit profession and good Corporate Governance in the Banking Sector in Europe"

The paper describes best practice from the practitioners, but it is important to note that, depending on the culture, size, business and local requirements, 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 banks to third parties. It is crucial that key stakeholders, including management, the board and the bank'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 Banking Committee (the Committee) on best practices that could be adopted by internal audit functions in respect of the audit of externally outsourced services. This paper does not consider:

- Outsourcing of internal audit as a function
- Internal outsourcing (from one legal entity to another within the same group), albeit many of the same concepts could be applied, where required due to specific legal entity, country or supervisory requirements.

Background

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

Outsourcing of operational activities to third parties by financial institutions is not a new phenomenon. However, in recent years the complexity of processes outsourced has continued to increase, as has the inherent risk associated with the transfer of, in particular, client data outside the organisation. As a consequence, 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. invasive audits
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
4. Special requirements in respect of outsourcing to 'FinTechs'

[1] Chief Audit Executives from DZ Bank AG, Crédit Agricole SA, ABN AMRO, Grupo Santander, UniCredit S.p.A., KBL European Private Bankers, Nordea, National Bank of Greece.

4

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 bank's activities within a defined 'audit universe' which is then subject to a risk assessment to determine the relative priorities for the audit plan. 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 bank.

The risk assessment should also consider whether the relative risk associated with the outsourced activity has increased or decreased as a result of the outsourcing arrangement.

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 risk assessment, relative to the perceived risk associated with all other activities within the bank (i.e. in line with the usual risk-based planning cycle).

In addition to representation of the outsourced processes itself, the bank's own sourcing and supplier management processes should be represented 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 bank's supplier risk management frameworks. Where it is determined that this is operating effectively, the internal audit function would rarely need to perform a direct 'invasive' on-site audit of a supplier. In cases where the bank does not have an effective supplier risk management framework, the internal audit function should consider what alternative approaches might be necessary.

a. Sourcing process

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) and to ensure that governance over the decision-making process involves all relevant parties and adequately risk assesses any potential outsourcing activity.

The internal audit function should, however, review the organisation's contractual standards for third party arrangements to ensure that a 'Right to Audit' is included in the terms agreed with any material service providers.

b. Supplier management

Internal audit should review and assess the adequacy of the bank's supplier management framework, considering whether this provides sufficient governance and oversight of key outsourced activities.

In practice a bank's supplier management process may include a number of different components. 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.

As a minimum the internal audit function should review any areas of the supplier management process where it may seek to place reliance for its own risk assessment or 'in lieu' of undertaking direct 'invasive 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.

In the case of (a), the internal audit function should satisfy itself 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. 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. Invasive audits

Based on internal audit's own risk assessment, the internal audit function may choose to perform direct 'invasive audits' on site at the third-party service provider. 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.

In addition to an invasive audit, auditing the outcomes of supplier processes can also sometimes provide assurance – without the need to actually audit the third party. For example, if a supplier is delivering an application, the internal audit function can audit the system controls.

Prior to initiating an invasive audit, the internal audit function should also consider the practicalities of such an undertaking, including how potential data privacy restrictions, particularly where a supplier handles data for multiple clients, may impact on the ability to effectively execute the audit.

3 Testing of and placing reliance upon the work of others

a. First and second line assurance functions

Internal audit functions may choose to use the work of an independent first or second line assurance function 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 invasive audits at suppliers where sufficient testing has already been performed by another assurance function within the bank 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.

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, the internal audit function should carefully consider whether the scope of the assessment corresponds with the scope of the third-party risk. In many cases it is necessary to supplement the scope of an ISAE 3402 with additional risk management processes.

In all of the above cases, the internal audit function should, as part of its continuous monitoring programme, 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.

4 Special requirements in respect of outsourcing to 'FinTechs'

In many respects, outsourcing to FinTechs is no different to outsourcing to other providers, and similar controls need to be in place. A key concern in respect of partnerships with FinTechs is the security of client data which may be transferred to the FinTech. Wherever possible banks 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 bank 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 bank has the capability to understand and manage the risk associated with FinTechs. For example, does the bank have sufficient expertise to evaluate the security of cryptographic processes in use at FinTechs? If not, then the risk associated with using FinTechs and their technology may not be effectively understood or managed. The internal audit function also needs to carefully assess its own capabilities to audit FinTechs.

OUR MISSION

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 institution of influence and to present and develop the internal audit profession and good corporate governance in Europe.

IIA Armenia	www.iia.am
IIA Austria	www.internerevision.at
IIA Belgium	www.iiabel.be
IIA Bulgaria	www.iiabg.org
IIA Croatia	www.hiir.hr
IIA Cyprus	www.iiacyprus.org.cy
IIA Czech	www.interniaudit.cz
IIA Denmark	www.iia.dk
IIA Estonia	www.siseaudit.ee
IIA Finland	www.theiia.fi
IIA France	www.ifaci.com
IIA Germany	www.diir.de
IIA Greece	www.hiia.gr
IIA Hungary	www.iia.hu
IIA Iceland	www.fie.is
IIA Israel	www.theiia.org.il
IIA Italy	www.aiiaweb.it
IIA Latvia	www.iai.lv
IIA Lithuania	www.vaa.lt
IIA Luxembourg	www.theiia.org/sites/luxembourg
IIA Montenegro	www.iircg.co.me
IIA Morocco	www.iiamaroc.org
IIA Netherlands	www.iia.nl
IIA Norway	www.iia.no
IIA Poland	www.iia.org.pl
IIA Portugal	www.ipai.pt
IIA Serbia	www.uirs.rs
IIA Slovenia	www.si-revizija.si
IIA Spain	www.auditoresinternos.es
IIA Sweden	www.theiia.se
IIA Switzerland	www.svir.ch
IIA Turkey	www.tide.org.tr
IIA UK & Ireland	www.iia.org.uk
IIA former Yugoslav Republic of Macedonia	www.aiam.org.mk

European Confederation of Institutes of Internal Auditing (ECIIA)

c/o IIA Belgium
Koningsstraat 109-111
Bus 5, BE–1000
Brussels, Belgium

www.eciia.eu

The Institute of Internal Auditors