

European Governance

THE OFFICIAL MAGAZINE OF THE ECIIA

May 2013 · Issue 24



Devil in the detail

New guidance by the ECIIA helps put detail into Solvency II's corporate governance proposals

INSIDE: Maximizing internal audit value, EU fraud and the UK's House of Lords, the European Commission's corporate governance action plan and more



Maximizing internal audit value

Boards of directors and audit committees can maximize the value of internal audit to corporate governance by following three fundamental principles, according to recent guidance.

Internal audit should have a reporting line within its organization that ensures it is able to operate with sufficient independence, says a joint publication by ECIIA and ECODA – *Making the most of the internal audit function: Recommendations for directors and board committees*.

It also says internal audit

should take a risk-based approach to developing and executing its audit plan, and that the function should operate with a high level of professionalism.

“These three conditions are key issues for directors to consider when monitoring the effectiveness of the organization’s internal audit function,” says the report.

It says that internal audit is uniquely positioned to provide each organization with global assurance on the effectiveness of internal governance and risk processes. In addition, internal

audit can play an advisory role when the board wishes to improve its process and implement recommendations to do so.

The paper advocates the “three lines of defence” model for corporate governance, comprising; operational management, internal governance functions and, finally, internal audit. It also proposes ten further recommendations designed to help boards and non-executive directors get the most out of their internal audit functions.

Download a copy of the report here.

“Big response” to internal audit consultation

Over one hundred chief executives, audit committee chairs, heads of audit and corporate governance professionals have responded to draft guidance issued for consultation by the

Chartered Institute of Internal Auditors in the UK.

The document – *Effective Internal Audit in the Financial Sector* – has been produced to help create “voluntary guidance that enhances existing international standards on internal auditing” in that sector, according to Phil Gray, director of communications at the Institute.

A key element of the initiative

was to find ways of preserving the independence and objectivity of internal audit functions. It also wanted to suggest what a good internal audit function might look like, says Gray.

The Institute is expected to present the final version of the document to its Council for approval this summer.

Download a copy of the consultation document here.



ECIIA Conference
2013

The Sound of Audit




Here beats the heart of audit 2013:

**02. – 04. October
Vienna / Austria
Hofburg**



www.ecia2013.at (open from January 2013)

UK Lords: EU fraud “understated”

The European Union’s anti-fraud system has serious weaknesses that contribute to an understatement of the amount lost to its budget each year, according to a report published in April by the UK’s House of Lords.

“We conclude that the figure of €404m cited by the Commission in its annual report offers only a glimpse of the levels of fraud perpetrated against the EU’s budget,” said the document, *The Fight Against Fraud on the EU’s Finances*. It said the true loss was closer to €5bn, “but it may be more.”

It said that member states showed a “lack of enthusiasm” in reporting fraud to the Commission, a factor that was made worse because of the lack of a clear definition of fraud.

“Evidence suggests that some Member States do not take their anti-EU fraud responsibilities seriously,” it concluded.

It recommended that member states should look for fraud against the EU’s budget, inform the relevant EU authorities when they found it, and act on referrals from the EU’s own anti-fraud body OLAF, which, it said, “remains an agency of limited powers.”

Under EU law, Member States have primary responsibility for preventing, detecting and following up on irregularities and fraud. They are responsible for managing almost 80% of EU expenditure. The vast majority of the problems of both fraud and error identified in reports by the EU’s Court of Auditors occur at member state level, rather than in “Brussels”.

The Commission said that it welcomed the report as a positive contribution to further stepping up the fight against fraud on the EU budget. It said that it would shortly make a proposal to set up a European Public Prosecutors Office “...to investigate, prosecute and bring to justice those who commit fraud involving EU funds.”

Download a copy of the Lords report.

THOMSON REUTERS
ACCELUS™

WE KNOW AUDIT TRUSTED INTERNAL AUDIT SOFTWARE

RISK ASSESSMENT » SCHEDULING » WORKPAPERS » REPORTING » ISSUE TRACKING



As an internal audit management software pioneer, Thomson Reuters Accelus™ delivers an end-to-end audit management solution with the best-in-industry implementation. Trust your investment in our proven software and reliable implementation, training and support. Developed by internal auditors for internal auditors, Thomson Reuters Accelus internal audit software improves audit efficiency and productivity throughout the entire audit process including risk assessment, scheduling, workpapers, reporting and issue tracking, helping thousands of corporate and government clients.

For more information: accelus.com/audit



© Thomson Reuters. GRC00230

Commission launches action plan on corporate governance



Source: The Council of the European Union

Michel Barnier

The European Commission has adopted an action plan that it says will modernize Europe's company law and corporate governance.

Businesses could be made more competitive and stable by improving long-term shareholder engagement, increasing transparency and simplifying cross-border operations in Europe, the Commission believes.

"Shareholders should receive additional rights, but also fully assume their responsibilities to make sure that the company

remains competitive over the longer term," said Michel Barnier, Internal Market and Services Commissioner.

"Companies should also become more transparent in several respects. This will contribute to effective governance of companies."

In particular, companies needed to be more open about the diversity of boards and their risk management policies. It said that they needed to improve corporate governance reporting and identify

shareholder issues more effectively. The Commission would look to strengthen transparency rules for institutional investors on their voting and engagement policies.

The Commission also wanted more transparency on remuneration policies, the individual remuneration of directors, as well as a shareholder's right to vote on remuneration policy and the remuneration report. Large payouts to the directors of loss-making banks have caused controversy in Europe since the financial crisis of 2008.

On the legislative side, it announced a number of initiatives aimed at improving cross-border transactions for companies operating in Europe.

"The action plan foresees merging all major company law directives into a single instrument," said Barnier. "This would make EU company law more accessible and comprehensible and reduce the risk of future inconsistencies."

The action plan comes after two years of consultation with industry,

shareholders and the public. It is part of the Commission's 'Europe 2020' Strategy, which calls for improvement of the business environment in Europe.

Separately, the Commission is considering putting forward a legislative proposal requiring companies to publish information

on their management of environmental and social issues. The move follows publication in October 2011 of the Commission's 2011-14 Strategy for Corporate Social Responsibility (CSR). The reporting requirements will apply to large companies but not to small and medium-sized enterprises.

Round up

IIA Cyprus is to hold a joint training event with the Institute of Chartered Accountants of England and Wales (ICAEW), following a successful meeting of the two organisations in December 2012. Present at the meeting was Christiana Diola of the ICAEW and president of IIA Cyprus Soteroulla Savvidou, vice-president Michael Zevlaris former president Onisiforos Onisiforou.

Serbia and Montenegro have passed laws that could pave the way for accession

to the EU. Serbian Company Law now requires an internal audit function in listed companies, defines the roles and responsibilities of an audit committee and the internal auditor function, says Jozefina Beke-Trivunac, member of the IIA Serbia management board. The Law on Accounting and Auditing in Montenegro requires internal audit and audit committees only in "large companies" and introduces definitions for the audit committee and internal audit, according to Slavko Rakocevic, chairman of IIA Montenegro.

Devil in the detail

Solvency II could provide insurers with sounder balance sheets and better corporate governance regimes. Hans-Joachim Büsselberg tells Arthur Piper how the ECIIA is adding the detail that could help make the directive a success



Insurers have been gearing up for new solvency rules since the European Commission decided to revise them in its Solvency II Directive (2009/138/EC) back in 2009. The directive aims to beef up the way that insurers cover their risks and lays down principles that businesses need to adopt to bolster their balance sheets against potential losses.

But the Commission was forced to revise the framework in its so-called Omnibus II Directive, which takes account of changes made to the financial industry in the Lisbon Treaty and to the zone's changing regulatory system. Once the European Parliament approves the Omnibus II Directive, Solvency II will come into effect. That is expected to happen on 1 January 2014 – although some industry insiders told *Post Online* this April that they do not anticipate

actual implementation until 2016.

Solvency II is not just about balance sheets. The rules will also “for the first time compel insurers specifically to focus on and devote significant resources to the identification, measurement and proactive management of risks,” says the Commission. Regulators, under the Supervisory Review Process, will be checking both solvency capital and making sure the “risk management and governance systems are adequate to the nature, scale and complexity of the insurer in question,” it says.

Getting ready

Insurers have been aware that they need to reorganize their existing risk management systems since 2009 and have been working in this area. But Solvency II only describes in outline how they might comply with the new regime – leaving »



Hans-Joachim Büsselberg

» much of the detail to be worked out by the board and management of individual businesses.

“The governance requirements for insurers mean that they will have to establish ‘functions’, or specific area of responsibility and expertise, to deal with risk management, risk modeling, compliance, internal audit and actuarial issues,” according to an explanatory memo published by the Commission. That does not mean that these “functions” have to be dealt with by separate people, or even carried out in-house.

Given that four of these functions provide assurance to the board on the effectiveness of their risk management processes, the European Confederation of Institute’s of Internal Auditing is concerned that the guidance is too vague, will lead to duplication of effort and confusion among boards over their risk assurance. It has published its own guidance – *The role of internal audit under Solvency II* – to shed light on these issues.

“We think the Solvency II Directive is fine in general, but we think its important to be more »

The TeamMate Revolution is here

Team•Mate rev•o•lu•tion *noun* \tēm-māt re-və-loo-shən

1. a. a thorough reversal of outdated technology and complete adoption of TeamMate
- b. a fundamental change in your audit approach; especially the overthrow or renunciation of one system substituted by TeamMate
- c. a changeover in use or preference especially in Audit Management Systems <the *TeamMate Revolution*>

TeamMate is still the Innovation Leader after all these years:

The first Windows based Audit Management System in the world

The first Audit Management System to introduce Smart Device functionality



The Global Leader in Audit Management



# of audit departments adopting TeamMate each day	1
# of Languages in which TeamMate is available	14
# of Countries in which TeamMate is Licensed	105
# of auditors using TeamMate daily	90,000
# of CPD delivered in the past 3 years	104,000

Risk Assessment
Risk Based Planning
Scheduling
Extensive Audit Content
Electronic Workpapers
Surveys
Checklists
Image Scanning & Annotation
Automated Report Generation
Full Issue Remediation Tracking
Time & Expense Tracking

» precise in what the role of internal audit is in the Solvency II context,” Hans-Joachim Büsselberg says, one of the ECIIA report authors.

He says that the guidance has two main aims. First, it will

the global IIA Standards.”

He says that for most insurance companies, the governance system proposed by the directive is quite new in the way it combines different

“It is important that the board takes responsibility and having an independent internal audit function is a good way of doing so”

help internal auditors in Europe understand their role in Solvency II. Second, its broader objective is to start a discussion with the European Union, European Parliament, the European Insurance and Occupational Pensions Authority and others over the role of internal audit and what it means in practice.

Internal audit role

“The role of internal audit is not well understood by some stakeholders,” says Büsselberg. “We think it’s important to introduce them to the three lines of defence model of corporate governance and

functions – risk management, internal audit, actuaries and compliance. It is not clear how the assurance needed by the board is specifically to be divided between the function without the potential of creating some potential omissions and duplication.

“The functions operate a lot within silos,” he says, “and each function has its own definition of risk, its own risk analysis techniques, different reporting processes and formats, so there is no real co-operation. Being new for many insurance undertakings the functions may be trying to build their

own kingdom’s in the business without considering the roles and responsibilities of the others.”

The three lines of defence model shows where the separate functions operate within the corporate governance structure of the business, which, together with the framework and guidance of the Committee of Sponsoring Organizations of the Treadway Commission, can help clarify those responsibilities (See *Three lines of defence model*).

“The main role of internal audit is as the independent assurance function within the insurance company – undertaking assurance to the board that amongst others the governance system is in place, accurate and efficient,” Büsselberg says.

Independence

The ECIIA’s guidance clarifies exactly how internal audit can achieve the independence it needs to fulfill this role – something that Solvency II does not pay specific attention to. The ECIIA recommends that internal audit reports functionally to the board and administratively to the chief executive officer. That is because

Internal audit’s role in Solvency II alignment

Although businesses need to make sure internal audit’s independence is not compromised, heads of internal audit should be able to assist in the following areas:

- **Governance of the project.** Internal audit should, as a minimum, keep itself informed and updated on the organization and status of the project and consider certain specific areas for further detailed audit projects.
- **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.
- **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.
- **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 standards.

Source: *The role of internal audit under Solvency II*

Solvency II makes the whole board responsible for enabling an adequate governance system.

“It is important that the board takes responsibility and having »

» an independent internal audit function is a good way of doing so,” Büsselberg says. “If the board agrees the internal audit plan, receives internal audit reports it helps it meet its responsibility.”

Companies should also allow internal audit to include all activities of the undertaking, inhouse and outsourced, in its risk based plan

not want them in, or they don't feel it's necessary,” he says. “For us, it is the whole company that should be subject to internal audit and no activity can be excluded a priori if the risk based approach is to work properly.”

The ECIIA's guidance also shows how the head of internal audit can help insurers with their

“It is the whole company that should be subject to internal audit and no activity can be excluded if the risk-based approach is to work”

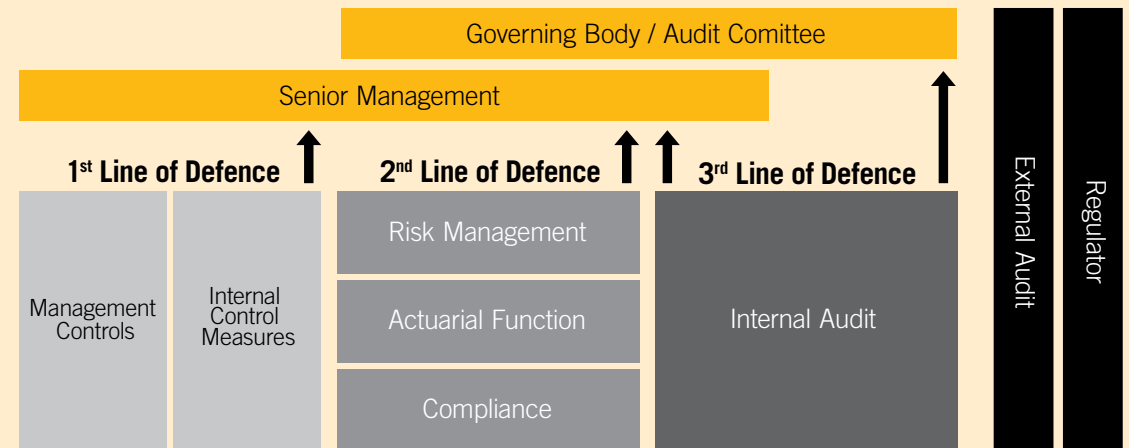
and to conduct any audit, if it considers it necessary due to its risk assessment. This may require a culture change among certain insurers. Büsselberg says that some companies still have blind spots which are not part of the audit universe as it is not considered as an appropriate audit field.

Büsselberg says that it should be internal audit's decision what to audit and when following its independent risk assessment. “It may be that management does

alignment to the requirements of Solvency II (See *Internal audit's role in Solvency II alignment*), although they will need to take care they do not jeopardize internal audit's independence. Insurers that take Solvency II to heart could end up with both a boosted balance sheet and a better corporate governance regime. And if that happens, implementation of the directive will have been worth the wait.

The document will be available shortly from here.

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.)

Data Protection Regulation in a nutshell

The Commission's proposals aim to bring up-to-date its 1995 Data Protection Directive that guarantee privacy rights to individuals. The directive is meant to give people more control over their personal data, make it easier to access and beef up its protection even outside of the European Union.

Individuals

- A reinforced “right to be forgotten”: people will be able to delete their data if there are no legitimate reasons for retaining it.
- Consent for data processing will have to be given explicitly, rather than assumed as is sometimes the case now. People will be able to transfer personal data from one service provider to another more easily.
- There will be increased responsibility and accountability for those processing personal data.
- People will be able to refer cases where their data has been breached or rules on data protection violated to the data protection authority in their country, even when their data is processed by an organisation based outside the EU.
- EU rules will apply even if personal data is processed abroad by companies that are active in the EU market.

Businesses?

- A single set of rules on data protection across the EU will replace the current patchwork of national rules in 27 Member States. The Commission estimates this will lead to a net saving for companies of €2.3bn a year.
- A simpler regulatory regime should save businesses around €130m a year.
- Companies will only have to deal with a single national data protection authority in the EU country where they have their main base – not up to 27 different national authorities of data processing.
- The new rules will create advantages for EU companies in global competition, as they will be able to offer their customers assurances of strong data protection whilst operating in a simpler regulatory environment.

Source: *European Commission*

» harmonization around the principle of protecting an individual's data rights while allowing smoother flows of information – something that is not possible under the existing directive.

Wide-ranging

The reforms are wide-ranging (See, *Data Protection Regulation in a nutshell*). The commission says the exercise would save industry €2.3bn annually. But they have not been without controversy. The draft regulation received over 3,000 responses when it was put out for consultation. And in an effort to reach some sort of consensus, more than 4,000 changes to the draft text have been put forward in Parliament.

In a published statement, digital rights group La Quadrature du Net said that

as it currently stands, the regulation would significantly strengthen citizens' rights. But it added that in response to the Commission proposal, “powerful companies, mainly based in United States (banks, insurances and Internet services), have led an unprecedented lobbying campaign.”

“Their goal is to withdraw from the final version of the regulation those proposals aimed at protecting citizens' personal data. Before this vote, we have to make certain that civil liberties MEPs will not break under lobby pressure,” said organization spokesman Jérémie Zimmermann.

One area that has proven particularly contentious is the ability of the regulation to protect data held on US cloud servers.

Press reports at the beginning of 2013 claimed that US »

“We have to make certain that civil liberties MEPs will not break under lobby pressure before the vote”

» government agencies may be using powers originally designed to fight the Cold War to access information held in the cloud by foreign corporations, individuals and potentially government bodies for purely political reasons.

The trigger was a report written for the European Parliament – *Fighting cyber crime and protecting privacy in the cloud*. The authors said that the European Union had neglected to protect the rights of European citizens from potential “misuses and abuses by law enforcement actors and agencies.” They include the US Central Intelligence Agency, the Federal Bureau of Investigations and the National Security Agency.

Under provisions contained in FISAAA – the Foreign Intelligence Surveillance Act of 1978, Amendment Act of 2008 - these organisations can gain access to any data held on computer servers that fall under US jurisdiction. Even though the legislation “authorised mass-surveillance of foreigners” on such cloud services, the report says that neither the EU Commission, national Data Protection Authorities (DPAs) nor the European Parliament

“had any awareness of FISAAA 1881a until mid-2011.”

US-based companies, including Amazon, Apple, Google and Microsoft, offer most popular public cloud services. Any data loaded onto clouds under technical control from the US could be subject to politically-motivated surveillance. Even data hosted by US-owned subsidiaries of such companies based in Europe can be analysed without warrant.

Unnoticed

“It’s amazing that no one working in the DPAs of Europe noticed this for over four years. They still don’t recognise the problem – only one oblique paragraph offering a flawed remedy,” said Caspar Bowden, one of the report authors and an independent privacy advocate.

Bowden says that the practice breaks with the forty-year-old legal model for international data transfers. Until now, the ideal has been to have an international treaty with full reciprocity of rights – so each jurisdiction is on an equal footing when it comes to accessing foreign information. Any exceptions – derogation – would be dealt with separately with safeguards

in place to protect rights.

“Cloud computing breaks this golden rule,” the report said. “Once data is transferred into a cloud, sovereignty is surrendered. It is hard to avoid the conclusion that the EU is not addressing properly an irrevocable loss of data sovereignty, and allowing errors made during Safe Harbour negotiations of 2000 to be consolidated, not corrected.”

There are various types of cloud services on offer, some of which are securely owned, controlled and hosted by the businesses that use them. The most dynamic form – Platform as a Service – provides organisations with potential access to hundreds of thousands of machines as their needs arise and is only provided by US cloud businesses.

Hamann believes the new Regulation should protect the data rights of European citizens against excessive government prying within the European Union. But agrees that FISAAA circumvents the usual Safe Harbour arrangements between the European Commission and the US Government. That means that even if there

were contractual agreements with US cloud companies, for example, not to divulge the data of European citizens, they would not be effective.

“An American data importer may sign a contract not to give data to the US government,” he says, “then along comes a federal agency and simply

“It’s amazing that no one working in the data protection authorities of Europe noticed this for four years”

puts a pistol to the temple of the CEO and says, ‘give me the data.’ This is not a problem EU regulation can solve unilaterally.”

Given the huge range of competing interests at play about the future of data privacy, it is not surprising that the European Parliament has missed the original 29 May deadline for voting on a final draft of the Regulation. Getting it right is likely to be a once in a generation opportunity. Getting it wrong with so much at stake is not an option. ■

Our mission

- » To be the consolidated voice for the profession of internal auditing in a widely defined Europe by promoting sound corporate governance with the European Union, its Parliament and Commission and any other European or global institutions of influence.
- » To promote corporate governance and the profession in economically emerging countries, as appropriate, within the wider geographic area of Europe and the Mediterranean basin.
- » To promote the mission of the Global IIA.

IIA Austria	www.internerevision.at	IIA Latvia	www.iai.lv
IIA Azerbaidjan	www.audit.gov.az	IIA Lithuania	www.theiia.org/chapters
IIA Belgium	www.iiabel.be	IIA Luxembourg	www.theiia.org/chapters
IIA Bosnia and Herzegovina	www.interni-revizori.info	IIA Montenegro	www.iirg.co.me
IIA Bulgaria	www.iiabg.org	IIA Morocco	www.theiia.org/chapters
IIA Croatia	www.hiir.hr	IIA Netherlands	www.iaa.nl
IIA Cyprus	www.iiacyprus.org.cy	IIA Norway	www.nirf.org
IIA Czech	www.interniaudit.cz	IIA Poland	www.iaa.org.pl
IIA Denmark	www.iaa.dk	IIA Portugal	www.ipai.pt
IIA Estonia	www.theiia.org/chapters	IIA Romania	www.aair.ro
IIA Finland	www.theiia.fi	IIA Serbia	www.theiia.org/chapters
IIA France	www.ifaci.com	IIA Slovakia	www.skia.sk
IIA Germany	www.diir.de	IIA Slovenia	www.si-revizija.si/ia/
IIA Georgia	www.theiia.org/chapters	IIA Spain	www.iai.es
IIA Greece	www.theiia.org/chapters	IIA Sweden	www.internrevisorerna.se
IIA Hungary	www.iaa.hu	IIA Switzerland	www.svir.ch
IIA Iceland	www.fie.is	IIA Tunisia	www.iiatunisia.org.tn
IIA Italy	www.iiaweab.it	IIA Turkey	www.tide.org.tr
		IIA UK & Ireland	www.iaa.org.uk

Corporate Governance Citizens:



Director of the publication

Marie-Hélène Laimay

Editor

Arthur Piper
arthur@sdw.co.uk
Direct 0115 958 2024

Produced by

Smith de Wint for the ECIIA

Smith de Wint
95 Harlaxton Drive
Lenton, Nottingham
NG7 1JD
www.sdw.co.uk

Views and opinions presented in this newsletter are the writers and do not necessarily represent the official positions of ECIIA.



European Confederation of
Institutes of Internal Auditing
Koningsstraat 109-111 Bus 5
BE – 1000 Brussels, Belgium.

www.eciia.eu