

Good Practice Guide: the internal audit role in information assurance

February 2009



HM TREASURY



HM TREASURY

Good Practice Guidance:
the internal audit role in
information assurance

February 2009

© Crown copyright 2009

The text in this document (excluding the Royal Arms and other departmental or agency logos) may be reproduced free of charge in any format or medium providing it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

For any other use of this material please write to:

Office of Public Sector Information
Information Policy Team
Kew, Richmond
Surrey
TW9 4DU

e-mail: licensing@ospi.gov.uk

HM Treasury contacts

This document can be found in full on our website at:
hm-treasury.gov.uk

If you require this information in another language, format or have general enquiries about HM Treasury and its work, contact:

Correspondence and Enquiry Unit
HM Treasury
1 Horse Guards Road
London
SW1A 2HQ

Tel: 020 7270 4558

Fax: 020 7270 4861

E-mail: public.enquiries@hm-treasury.gov.uk

Printed on at least 75% recycled paper.
When you have finished with it please recycle it again.

ISBN 978-1-84532-559-6
PU725

Contents

		Page
Chapter 1	Introduction	3
Chapter 2	Assurance roles and responsibilities	5
Chapter 3	The internal audit approach	9
Chapter 4	Typical areas of audit coverage	11
Chapter 5	Skills and competence	13
Annex A	Further guidance	15

1

Introduction

1.1 Following a number of high profile losses of data by central government organisations, a data handling review was commissioned by the Prime Minister to be conducted across departments and steps were taken to strengthen the way in which departments manage their information. As a part of the review, the Cabinet Office (Central Sponsor for Information Assurance) has put in place new measures to protect information, to apply across central Government. These include protective measures, working culture, processes, transparency of arrangements, use of information charters, and guidance on publication of information. Although one of the key risks is safeguarding personal data, the measures are to apply to all information and data on which the government depends or holds in safe custody. From 2008-09 the management of information risk will explicitly feature in an organisation's Statement on Internal Control.

1.2 This has implications for those traditionally involved in the governance process and in the provision of internal audit services. Cabinet Office Guidance on the Annual Assessment of Information Risk Management¹ recognises that both the audit committee and internal audit can make an important contribution to improving information risk management in central government; the audit committee in its role of reviewing the comprehensiveness and reliability of assurances, and internal audit in the coverage it can give to information risk in providing its broader assurances to the Accounting Officer. This guidance clarifies the implications for the internal audit role in the information assurance process.

1.3 Every organisation has established governance and assurance structures and it is important that information assurance fits into these structures. Assurance can be derived from a number of sources. A model that is often deployed to clarify roles is the 'three lines of defence' model, which illustrates that assurance can come from:

- Front-line business, in terms of evidence that policies, processes, controls and checks are in place. This would feature in directors' stewardship reporting arrangements and could incorporate elements of control risk self-assessment.
- A secondary line of assurance can come from separate arrangements that management has put in place to assure itself that procedures and controls are operating as they should be. These could include mechanisms such as quality management arrangements, programme and project assurance and health and safety inspections. In relation to information assurance they could include compliance and accreditation reviews of projects, systems and processes.
- The third line of defence within an organisation is an independent and objective internal audit function. In providing assurance on the framework of risk management, control and governance, internal audit should consider the other mechanisms in place within the first and second lines of defence and the extent to which audit can rely upon them.

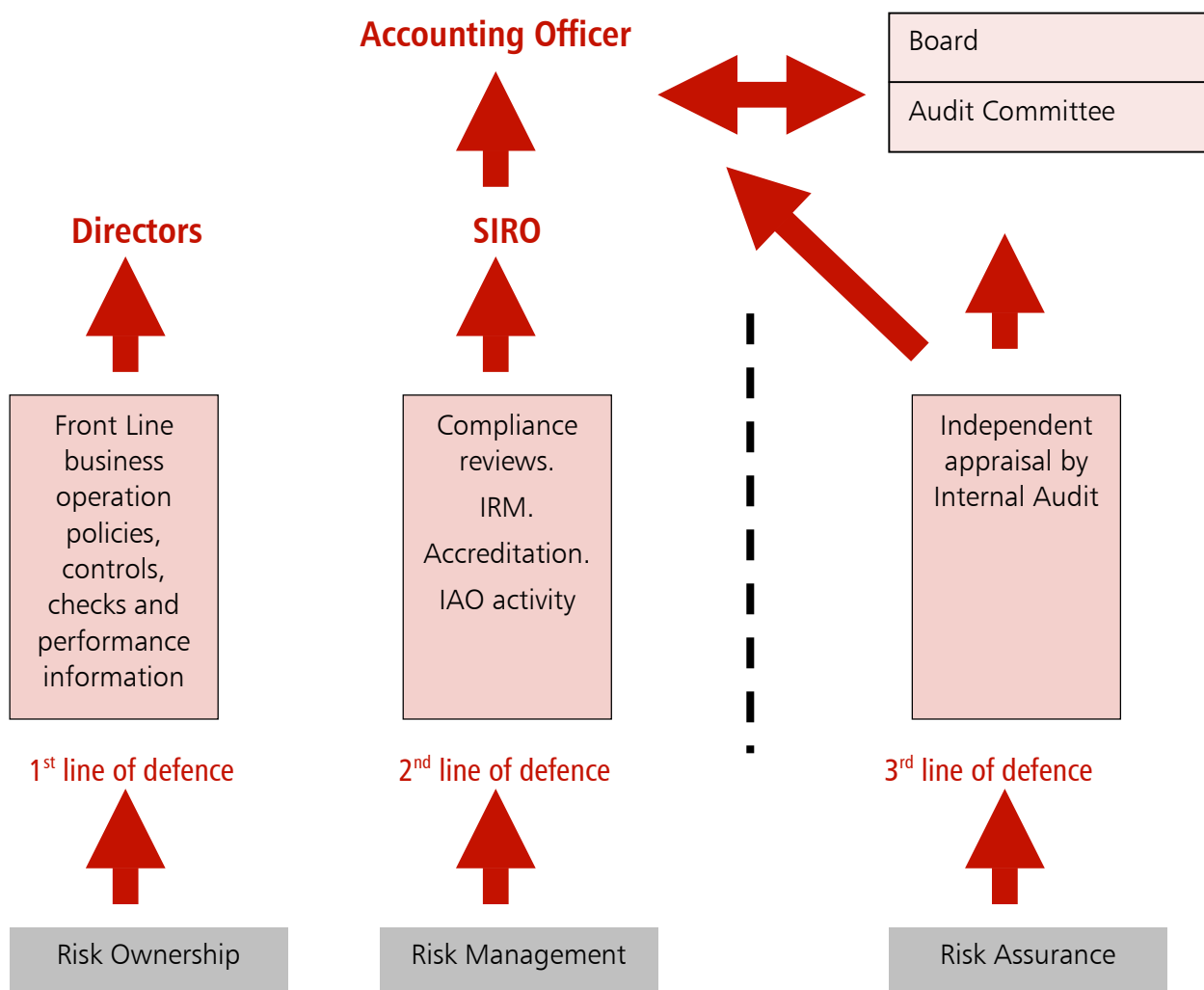
¹ Guidance on the Annual Assessment of Information Risk Management Version 3 (Tier 4 of Security Policy Framework)

1.4 The model in **Table 1.A** below illustrates how the three lines of defence concept can be applied to information assurance needs. The aim of the model is to clarify responsibilities. In reality there may be more interplay in the relationship between the respective parties. Internal audit will seek to support the SIRO with information about the adequacy of control over information and about the reliability of the information assurance process in the way that it would other directors with regard to their respective governance, risk and control arrangements. Similarly the SIRO may seek to draw on the work of internal audit for key components of their assurance need.

1.5 CESG, the national technical authority for information assurance, has developed an Information Assurance Maturity Model (IAMM) to help to regularly monitor a government organisation's information risk maturity capability. This is an evidence-based tool to assist the SIRO in their assessment and reporting obligations. It will also be of use to internal audit, as its approach and level of involvement in information risk management will depend upon the importance of information risk to the organisation, its relative organisational maturity and the controls established in the first and second lines of defence. This document indicates that there is a range of approaches that could be deployed by internal audit in auditing information assurance. Care must be taken, however, not to prejudice the objectivity and independence of internal audit's direct reporting line to the Accounting Officer.

Table 1.A:

Information Assurance



2

Assurance roles and responsibilities

The Accounting Officer

2.1 An Accounting Officer (AO) has a personal accountability to parliament for the propriety and regularity of the public finances for their organisation, for keeping proper records and for safeguarding the respective assets. They must be able to demonstrate that they maintain a sound system of internal control to support the organisation's policies, aims and objectives and have an appropriate framework of risk management. This is captured in the annual Statement on Internal Control (SIC). They are often supported in this role by directors' stewardship reports, objective assurance from internal audit services and constructive challenge from audit committees.

2.2 Following the data handling review, steps have been taken to strengthen the way in which departments manage their information. As a consequence there is now a requirement for Accounting Officers "to explicitly include how risks to information are being managed and controlled" (FReM Annex 3) in their Statement on Internal Control. Similarly paragraph 7.2.11 of the FReM covers the need to identify any 'personal data related incidents' within the Management Commentary of the Departmental Annual Report as part of the business review. This gives greater emphasis to information risk in the assurance process and calls for greater clarity on how this assurance need can be fulfilled. To lead on the required assurances, a Senior Information Risk Owner in each department will provide the focus for the management of information risk at Board level.

The Audit Committee

2.3 The audit committee supports the Board and Accounting Officer by reviewing the comprehensiveness of assurances in meeting the Board and Accounting Officer's assurance needs, and reviewing the reliability and integrity of these assurances. It is, therefore, well placed to assist the Accounting Officer in ensuring that there is a robust assurance arrangement for risk in the widest sense and, more specifically here, to information. The audit committee typically will use a mix of sources from the 'three lines of defence' model, Table 1.A, in fulfilling its obligations to the Accounting Officer and the Board. The committee will be interested to see whether the information they have been receiving from the different sources is consistent and accords with the SIRO's annual assessment and information risk report to the Cabinet Office. Where an assessment has been conducted against the IAMM, this will help to provide a body of evidence to support the current position.

Internal Audit

2.4 The main purpose of internal audit activity within central government is to provide the Accounting Officer with an objective evaluation and opinion on the overall adequacy and effectiveness of the organisation's framework of governance, risk management and control.

2.5 Internal audit may also be used by management as an expert internal consultant to assist with the development of a strategic risk management process for the organisation. *"It is important to note that internal audit is neither a substitute for management ownership of risk nor a substitute for an embedded review system carried out by the various staff who have*

executive responsibility for the achievement of organisational objectives"¹. The same principle applies to information risk management.

2.6 Internal Audit will be concerned with how well the organisation manages information risk as a key component of its wider assurance responsibilities for risk management. The Data Handling Review² recognised the important role that Internal audit can play in examining and assuring actions taken by others. As mentioned at 1.5 above, the degree of direct internal audit coverage will largely be driven by the importance of information risk to the organisation and the respective maturity of the arrangements for information risk management as established in the first and second lines of defence (see Table 1.A above). Internal audit is well placed in this respect to help the SIRO fulfil his/her obligations (see also 3.4 and 3.5) in providing assurance on information risk to the Accounting Officer, but this must be done without prejudice to the objectivity and independence of internal audit's own direct reporting line to the Accounting Officer.

The Senior Information Risk Owner

2.7 Cabinet Office guidance sets out the key concept of a Senior Information Risk Owner (SIRO) role with responsibility for the overall information risk policy and risk assessment process and for advising the AO on the information risk aspects of the SIC. The SIRO is a Board level individual responsible for managing departmental information risks, including maintaining and reviewing an information risk register. The SIRO role may be combined with other security or information management board level roles.

2.8 The SIRO will need a framework for deriving assurance from across the organisation in respect of the various policies, processes, systems, projects, control arrangements and organisational behaviours. The SIRO will need to derive a clear view on the organisation's level of compliance with the mandatory minimum measures in order to complete their annual assessment and the information risk report to the Cabinet Office. The work that will deliver the assurance needs to be planned and monitored throughout the year so that it is clear who is providing the respective assurance and when. This will avoid an expectation gap on completion of the annual assessment. The IAMM will be a key tool to support the SIRO in this work.

Information Asset Owner

2.9 Information Asset Owners are senior, named individuals responsible for each identified information asset (defined as data sets, databases and / or ICT systems). They provide SIROs with annual written assessments on the use and security of the information assets for which they are responsible.

Other Assurance Related Roles

2.10 Other sources of assurance could include:

- Departmental Security Officer (DSO) who has day-to-day responsibility for all aspects of protective security (including physical, personnel and information security);
- Information Technology Security Officer (ITSO): responsible for the security of information in electronic form;

¹ Orange Book

² Data Handling Procedures in Government Final Report June 2008

- Accreditor of the information asset – a suitably qualified and experienced individual responsible for assessing a component against its security requirements resulting in a decision to accept the risks arising from its operation;
- A designated Communications Security Officer (ComSO) if cryptographic material is handled;
- Programme or project assurance providers considering controls being built into new systems; and
- Other quality, configuration, security or fraud prevention processes.

3

The internal audit approach

3.1 The internal audit approach to auditing information risk management needs to be carefully planned and clearly established from the outset of the information assurance assessment year. This will help to avoid false assumptions in the planning process. Internal audit can play a key role in helping to ensure that assurances are robust. The level of engagement could vary subject to the needs of the organisation and a number of factors can influence the role that internal audit will play.

3.2 One of the first decisions to be made is with regard to the scope of coverage and how much effort will be spent specifically on information risk management and how much will be spent on wider protective security arrangements. To set this in context, there are 19 mandatory minimum measures that are associated with information risk management but 70 in total for protective security. Clearly information risk management is a core component of protective security so consideration will need to be given on how this will be approached. This guidance, however, concentrates on information assurance and does not extend to all areas of protective security.

3.3 Two of the key determining factors regarding depth of coverage and approach will be the relative importance of information risk to the organisation and its respective level of maturity for handling it. For example, an organisation that is certified to ISO 17799 or has had a strong and positive IAMM assessment may need less direct attention. A good starting point would be to consider whether such an assessment has been made using CESG guidance¹. Internal audit may wish to see how objectively this was conducted and how well evidenced the review was. What were the key findings and what action is being, or has been taken? Similarly, there may already be assurance arrangements in place for security reviews, penetration testing, security testing, quality compliance, and accreditation of systems, processes and infrastructure, etc. Internal audit should avoid duplication of work, but as with other areas of assurance, should seek to ensure that the work is competently performed where it seeks to rely upon it in providing its own assurance.

3.4 The Head of Internal Audit will need to establish, for example:

- how the SIRO plans to meet his/her assurance needs;
- whether the assurance is clearly planned from the outset and who will be providing it;
- whether internal audit assurances will be reflected as part of the annual assessment or be kept as a separate assurance feed;
- whether internal audit will perform some form of review of the emerging assurance, assessment report or IAMM assessment for the SIRO; and
- the extent to which internal audit will provide a separate, independent review of the information assurance process.

¹ http://www.cesg.gov.uk/products_services/iacs/iamm/index.shtml

3.5 Internal audit may be well placed to consider the adequacy and reliability of the processes in place to deliver the information on which the SIRO's annual assessment is based. This could be an appraisal of the planned inputs to deliver the required assurance, advice on the emerging results, a review to provide advice on the IAMM assessment or SIRO's annual report. It should be made clear that whilst internal audit may advise the SIRO on the strength and validity of the report, this would not preclude internal audit from conducting its own independent review of the information assurance process.

4

Typical areas of audit coverage

4.1 In considering the adequacy of information risk management arrangements as part of the wider internal audit remit, some of the standards and guidance produced by the Cabinet Office should provide a useful backdrop. For example internal audit may wish to consider whether:

- Boards are taking information risk management seriously (e.g. getting regular and sufficient information on the organisation's information risk management obligations and acting on the information received);
- An information risk policy exists, setting out how the organisation plans to implement the mandatory minimum measures for managing information risk in their own activity and that of their delivery partners and that the policy is published and communicated in a manner that is relevant, accessible and understandable to all employees and relevant external parties including delivery partners;
- Key roles have been defined and responsibilities allocated to named individuals (e.g. AO, SIRO, IAOs);
- The organisation has an effective information risk governance framework in place through which Directors articulate the organisation's information risk objectives and set the risk management principles and policy to be followed by all staff (e.g. processes for assessing risks to the confidentiality, integrity and availability of information in delivery chains quarterly and annually);
- The organisation has identified all the information it and its delivery partners hold and carried out a risk assessment of each information asset, set risk tolerances etc;
- Key risks have been identified and are being appropriately controlled;
- ICT systems handling protectively marked information have been accredited to the Government standard, and systems which undergo significant change have been reassessed;
- The mandatory minimum measures have been applied to the organisation and its delivery partners, which include data handling requirements (e.g. protective marking, secure holding, removable media, data transfer and disposal);
- Data security arrangements are underpinned by a culture that values, protects and uses information for the public good (e.g. training programmes all staff particularly AOs, SIROs and IAOs; whistleblowing arrangements; HR processes which make clear that failure to apply control in handling personal data is a serious matter); and
- The organisation has an effective compliance and audit regime so that the board has an accurate picture of the organisation's compliance with legislation, the HMG Security Policy Framework and national policy and standards.

5

Skills and competence

5.1 There may be a need for internal audit teams to review their skill need in relation to information risk. A suitably knowledgeable and competent internal audit service can provide a strong and credible challenge to the information risk management arrangements within an organisation which in turn will help to build external confidence that there is rigour within the internal processes.

5.2 CESA is currently developing a methodology for auditing the management of information risk. This is aimed at providing information assurance reviewers within government organisations the best prospects of finding systemic weaknesses in information risk management processes. CESA is making arrangements for training providers with a national capability to train reviewers and information assurance professionals in the use of the information assurance methodology. CESA expects to publish the methodology in a Good Practice Guide early in FY 09-10.

5.3 The method will involve 3 main stages:

- Auditing the organisation's assessment of its key information risks;
- Auditing the adequacy of the information assurance controls intended to mitigate the information risks; and
- Auditing the maturity of the information assurance controls implemented.

5.4 In the meantime, there will be a 2-day training course on assessing compliance with the HMG Information Assurance Standard No 6 (which relates to protecting personal data and managing information risk). A pilot course will run in February 2009 and will be repeated according to demand.

5.5 Internal auditors appraising information risk management processes may wish to undergo training. CESA will provide details of its future courses on its website and via the Treasury team.

A

Further guidance

A.1 More detailed guidance on information assurance provided by Cabinet Office CSIA can be found on the following link:

<http://www.cabinetoffice.gov.uk/csia.aspx>

A.2 The Final Report on Data Handling Procedures in Government can be found here:

http://www.cabinetoffice.gov.uk/reports/data_handling.aspx

A.3 More detailed guidance on information risk management can be obtained from:

datareviewteam@cabinet-office.x.gsi.gov.uk

A.4 Guidance on assessing IA maturity is provided by CESG and can be found here:

http://www.cesg.gov.uk/products_services/iacs/iamm/index.shtml

A.5 “Managing Information Risk - a guide for Accounting Officers, Board members and Senior Information Risk Owners” is currently available on:

<http://www.nationalarchives.gov.uk/services/publications/information-risk.pdf>

A.6 The “HMG Security Policy Framework” which outlines the mandatory protective security requirements (including physical, information and personal security) that all Government Departments and Agencies must follow can be found at:

<http://www.cabinetoffice.gov.uk/spf.aspx>

ISBN 978-1-84532-559-6



9 781845 325596 >