A Question of Balance

Independent Assurance of Information Governance Returns

Summary of Guidance

Department of Health

audit commission

NHS Mersey Internal Audit Agency

NHS South Coast Audit

DH INFORMATION READER BOX

Policy	Estates
HR / Workforce	Commissioning
Management	IM & T
Planning /	Finance
Clinical	Social Care / Partnership Working

Document Purpose	Best Practice Guidance
Gateway Reference	14988
Title	A Question of Balance - Independent Assurance of Information Governace Returns
Author	DH/Informatics/Information Governance Policy Branch
Publication Date	November 2010
Target Audience	PCT CEs, NHS Trust CEs, SHA CEs, Care Trust CEs, Foundation Trust CEs , PCT Chairs, NHS Trust Board Chairs, Directors of Finance
Circulation List	
Description	The NHS Informatics Planning Guidance Annex 1 stated that: "An IG audit utilising the centrally provided audit methodology should be included within the work plans of each organisations' auditors". To ensure a common approach to such an audit across the NHS, the Department of Health commissioned an internal audit assurance framework for the Information Governance Toolkit (IGT) self-assessments.
Cross Ref	N/A
Superseded Docs	N/A
Action Required	Best practice
Timing	**N/A**
Contact Details	exeter.helpdesk@nhs.net
For Recipient's Use	

Contents

Foreword

Giles Wilmore, Director of Policy & Planning, Informatics Directorate, Department of Health

The NHS is learning from the experiences of recent years and has begun to realise that we cannot harness the potential of information technology if we fail to establish a culture that understands the importance of information and the importance of effective information governance.

The NHS Constitution provided a clear articulation of the patient right to confidentiality and the expectation that the NHS will hold information securely. The recent White Paper 'Equity and excellence: Liberating the NHS' articulates the vision of an NHS where patients have far greater control over information. We need to sustain momentum on information governance and ensure that the trust that patients have in those who provide them with care is not misplaced.

Of equal importance are those areas of information governance – information quality, integrity and availability resulting from good records management – that not only contribute to effective and efficient working but also help to save lives, improve health outcomes and build our understanding of health needs and the effectiveness of service provision.

This audit framework will help NHS organisations to focus on what they need to do to respect patient rights, sustain public trust, improve healthcare outcomes and maximise the benefits that can be gained from high quality information and modern information technologies.

Andy McKeon, Managing Director for Health, Audit Commission

Transparency and trust are important to the challenges facing public services today; especially in health where we manage millions of personal and sensitive records. The public need confidence that their information is secure, used for the purposes for which it was collected and only shared when appropriate.

Since 2007, important work has taken place across all parts of government to improve our management and governance of information. The NHS has played an important part in that improvement, but continuing data losses shows there is still scope to improve.

No health body can guarantee it will never experience data loss. However patients and the public expect high standards; scrutiny remains high and failures will rightly continue to attract the attention of regulators and criticism in the media.

The objective of everyone involved in the use and governance of information in the NHS must be to meet and exceed the demands of government and the expectations of patients. This audit framework represents part of an evolving process to improve the consistency of information management and governance in the NHS to help meet that objective.

I am delighted the Audit Commission has been able to support this work, assisted by colleagues in Internal Audit and the Department of Health. It is consistent with our strategic agenda that includes recent national studies on the use of information, trust and transparency. I believe the management and governance of information will increase in significance as we work together to address future public service challenges.

Assuring IG Toolkit Assessments

Why information assurance is important

1 As public awareness of information assurance increases; tolerance of poor performance, mishandling, data losses and breaches of confidentiality decreases. Confidence in public data and information handling is at an all-time low. It is against this backdrop the NHS needs to carry out robust, consistent and credible scrutiny and validation to uphold public trust and meet patient expectations of confidentiality.

2 The NHS has shown its commitment to improving and upholding standards in handling information through the Information Governance Toolkit (IGT); a self-assessed submission against best practice criteria.

3 However, audits of IGT self-assessments by NHS internal auditors and external security consultants have found that it is not uncommon for scores to be overstated or unsubstantiated. NHS organisations also continue to suffer several data and information security breaches involving personal and sensitive information.

4 Reports published in 2009 by the Audit Commission and the Care Quality Commission on the use of information in the NHS support these findings. In "Taking It On Trust", the Audit Commission highlighted deficiencies in wider self-assessment and cited several Healthcare Commission examples suggesting that trust self-assessment of compliance with standards was often inaccurate:

> *"Trusts may indeed be meeting all these requirements but it is not evident from the material presented to the Board. This is an important issue for regulators and the regulatory framework is increasingly dependent on self-assessments and self-certification."*[I]

5 Also, in April 2010, in his keynote address[II], the Deputy Office of the Information Commissioner David Smith stated that:

> *"More serious data breaches have taken place within the NHS than any other UK organisation since the end of 2007. A total of 287 breaches were reported, accounting for more than 30% of the total number."*

6 Against this background, and following guidance on independent validation of IGT scores by the Chief Executive of the Department of Health in May 2008[III], the Care Quality Commission study on information governance in trusts recommended that:

> *"External validation and audit (by NHS internal audit or external auditors) of healthcare organisations' self-assessments using the IG Toolkit should be mandatory"*[IV]

7 The NHS Operating Framework 2010/2011, through the NHS Informatics Planning Guidance, subsequently incorporated this recommendation.

I "Taking It On Trust", Audit Commission, April 2009
II Speaking at the Infosec Security Conference on 27th April 2010
III David Nicholson Letter to Chief Executives dated 20 May 2008
IV "The Right Information, In The Right Place, At The Right Time", CQC, September 2009

8 To ensure a common approach to such an audit across the NHS, the Informatics Directorate of the Department of Health commissioned an internal audit assurance framework for IGT self-assessments. The Department asked the Audit Commission to lead on the development, supported by Mersey Internal Audit Agency and South Coast Audit & Consultancy Services.

Who is responsible for information assurance in your organisation?[I]

9 The UK Government (Cabinet Office) mandated new information governance requirements, following the HMRC data loss in 2007. Chief Executives and named senior staff in organisations now have formal information risk roles and responsibilities to protect and secure sensitive and personal information.

10 The roles are:

- The Accounting Officer (AO)
- Senior Information Risk Owner (SIRO)
- Information Asset Owners (IAO)

11 The NHS Information Risk Management Guidance, issued in January 2009, covers these roles in detail.

What does the internal audit comprise?

12 The internal audit framework comprises:

- **A series of audit requirements:** (matched to the Toolkit requirements), these note the assurance required and the potential sources of evidence across three levels of compliance. They also contain mapping to other parts of the audit framework.
- **Evidence review guides:** These are generic guides that cover common evidence items such as minutes, strategies, policies, intranet content and job descriptions and are there to support the auditor in reviewing these types of evidence.
- **The questions for a staff survey:** designed to provide a perspective on the evidence from document review and interviews. The survey should take no longer than 15 minutes to complete.

The framework allows the internal auditor to reach an opinion and triangulate the results from:

- the organisational self-assessment;
- the auditor's assessment of the toolkit scores; and
- the staff survey.

[I] Information in this section reflects published Cabinet Office guidelines: "Guidance on Mandatory Roles: AO, SIRO, IAO" dated April 2008

What is the internal audit process?

13 The organisation's internal audit provider will normally undertake the audit. Often, internal audit plans already include this work as part of assessing information assurance risk. The audit should take up to ten days in internal audit plans, which is in line with existing arrangements and should not represent an added burden. Where internal audit plans do not address information assurance risk, these will require adjustment to accommodate the IGT audit either in place of, or as well as, other planned work.

14 Figure 1 summarises the three tier approach that shows how the high-level review incorporates the key requirements. Organisational risk determines the need for extra work.

Figure 1: Three Tier Model

This sets out the risk-based approach

Source: South Coast Audit

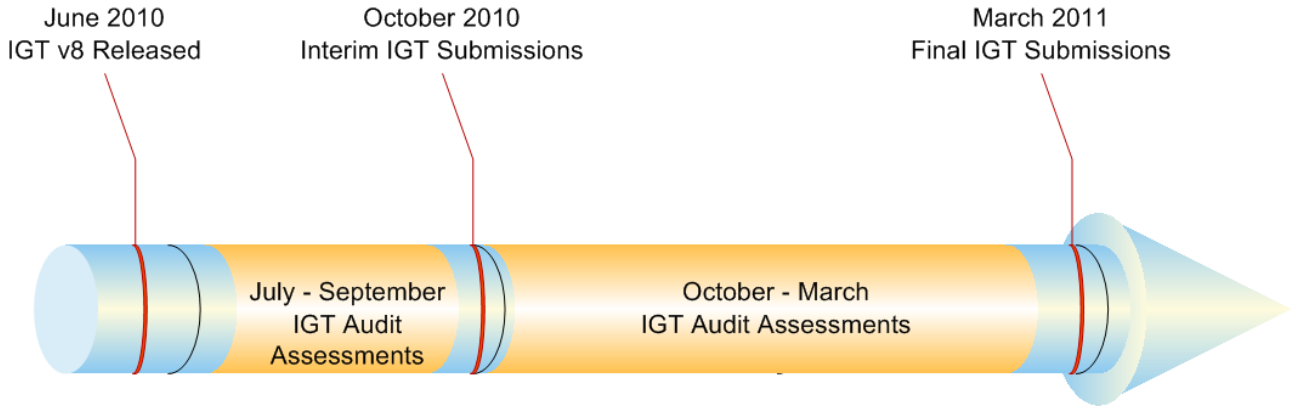
15 It is important to recognise that this internal audit framework covers a high-level validation of the IG Toolkit self-assessment. Significant wider risk exposures may call for more detailed risk-based reviews as appropriate to the needs of the organisation.

16 Internal audits should be carried out before interim or final toolkit submissions to allow organisations time to respond to and act on the findings. The IG Toolkit comprises many requirements spread across six strands. Each year, the Department of Health will choose several IG Toolkit requirements as 'key' and will mandate these as the minimum audit scope. These will change year-on-year to reflect national priorities and changing risks.

17 Figure 2 outlines the timeline for 2010/ 11.

Figure 2: IG Toolkit Assessment Submissions Timeline

This represents the timeline for 2010-11 only, later years may vary



Source: Department of Health, Informatics Directorate

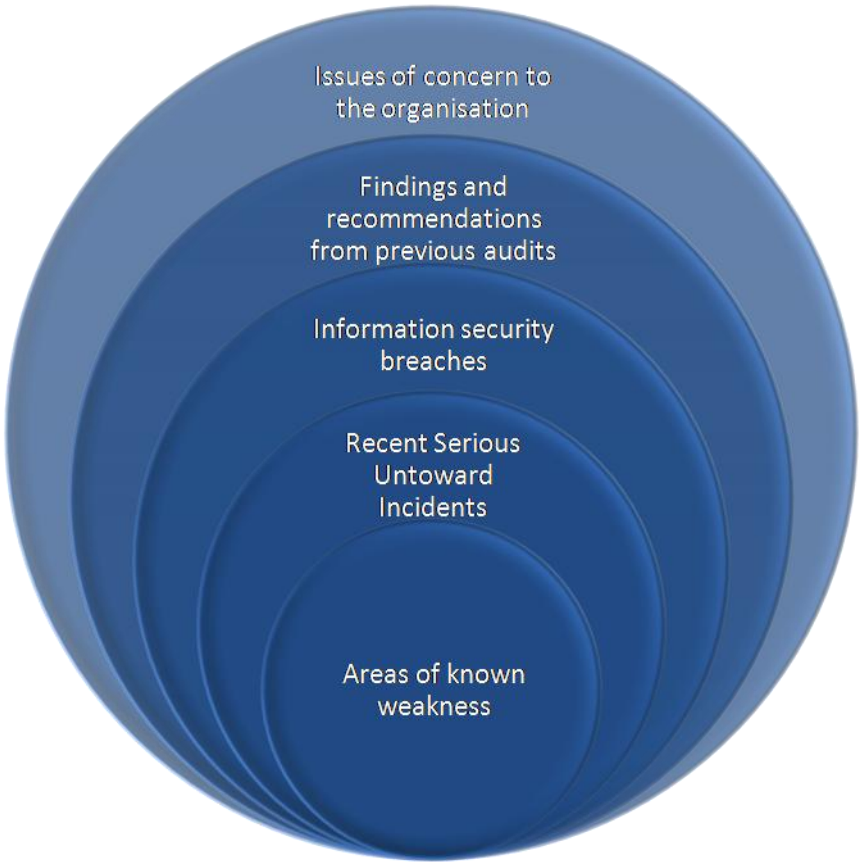
18 Internal auditors will complete audit assessments before either interim or final assessments. This will enable internal audit suppliers to manage their workloads and report findings in good time to allow organisations to respond and take action before their submissions. In later years there may be more than one interim submission date.

What is my organisation's role in deciding the internal audit scope?

19 The internal audit scope must include all key requirements. A risk assessment should determine any addition to the internal audit scope. The organisation's officers, responsible for information assurance, should work with internal auditors on a risk assessment that considers the issues in Figure 3 overleaf:

Figure 3: Risk Assessment

Consider the following to determine any additions to the scope



Source: Audit Commission

20 These considerations will help you decide what extra requirements, if any, should be added to those earmarked as key and fits in with the three tier approach described earlier.

What is the purpose of the staff survey?

21 The staff survey is designed to have a minimal impact on staff time (expected maximum completion time is 15 minutes). Internal auditors will either send the survey to all staff, or they will select a sample of staff to use. The survey results will often challenge assessment scores and occasionally will contradict other evidence. Extensive guidance has been provided to internal auditors on the subjective nature of survey evidence and how to use this correctly to triangulate other findings.

22 It is important the organisation owns the survey and in particular that senior management sponsor its distribution to encourage a good response rate.

What are the potential outcomes of the audit?

23 The internal auditor will reach two conclusions, one for the scored IGT assessments and the other an overall assurance or internal audit opinion.

24 IGT assessments will be one of the following as shown in table 1:

Table 1: IGT requirement scores

Internal auditors will select from one of the following four assessments

Assessment	Explanation
Agree	From the evidence available we are able to agree the score recorded as a reasonable assessment of current performance.
Understated	From the evidence provided it is our assessment the organisation is performing at a level higher than recorded.
Overstated	From the evidence provided it is our assessment the organisation is performing at a lower level than recorded.
Unsubstantiated	The organisation has not provided enough evidence to confirm the score recorded.

Source: Mersey Internal Audit Agency and South Coast Audit

25 Internal auditors define the difference between overstated and unsubstantiated as the availability and quality of the evidence. For example:

- Where an organisation has provided all the evidence it possibly can and this does not sufficiently support the score; auditors will assess this as 'overstated'.
- Where an organisation has not provided or does not have supporting evidence, auditors will assess this as 'unsubstantiated'.

Although overstated and unsubstantiated do vary in context, their effect on the overall internal audit opinion is the same.

26 The opinion ratings will be consistent with those agreed by the organisation's Audit Committee. Typically this will be one of the following as shown in Table 2:

Table2: Example overall audit opinions

Internal audit opinions typically take the following form but exact wording may vary.

Overall Opinion	Description
Full Assurance	A sound system of internal control designed to meet the organisation's objective with controls applied consistently in all the areas reviewed.
High Assurance	Some low impact control weaknesses that, if addressed would improve overall control. However, these weaknesses do not affect key controls and are unlikely to hinder achievement of the objectives of the system. Therefore we can conclude the key controls have been adequately designed and are working effectively to deliver the objectives of the system, function or process.
Significant Assurance	Some weaknesses in the design and/ or operation of controls that could hinder achievement of the objectives of the system, function or process. However, either their impact would be minimal or they would be unlikely to occur.
Limited Assurance	Weaknesses in the design and/ or operation of controls that could have a significant impact on achievement of the key system, function or process objectives but should not have a significant impact on achievement of organisational objectives.
No Assurance	Weaknesses in the design and/ or operation of controls that [in total] have a significant impact on achievement of key system, function or process objectives and may put at risk achievement of organisational objectives.

Source: Mersey Internal Audit Agency and South Coast Audit

Basis of the opinion

27 The internal audit opinion is based on the self-assessed scores supplied by the organisation and does not represent a comprehensive review of the detailed controls. The following wording is suggested to support and accompany the internal audit opinion.

Information Governance requirements and scoring criteria represent a high-level self-assessment of performance within the organisation. Our review and opinion is based upon the evidence provided to us to substantiate the scores submitted in relation to these high-level requirements and criteria. Our opinions are based on the reasonableness of the scores in these circumstances and do not, therefore, infer assurance that detailed controls are adequate to meet business needs. It is possible, therefore, that more detailed audits of specific areas contained within the IGT may uncover control weaknesses that subsequently appear to contradict the opinions herein.

Incorporating the opinion in the statement on internal control

28 The overall opinion should be included in the statement on internal control (SIC) as part of the requirement to include an explicit reference to information risk. This can be supported with a narrative report the SIRO will supply.

Conclusion

A note from the authors

29 This internal audit framework has drawn on extensive experience of internal and external audit suppliers and will bring much needed consistency to the independent validation of IG Toolkit assessments.

30 Designating a limited number of mandated key requirements focuses on key risks while minimising the regulatory burden. Extra requirements may be included but this is a risk-based approach involving both the organisation and its internal auditors.

31 The internal audit framework supports a wide range of initiatives to deliver effective security of personal and sensitive information in the NHS. Government demands it; patients have a right to expect it; together we must deliver it.

Phil Walker	**Andrew Ball**	**Tony Cobain**	**Paul Merison**
Head of IG Policy	Head of IT Performance	Head of IM&T Assurance	Head of IT Audit Services
Informatics Directorate Department of Health	Audit Commission	Mersey Internal Audit	South Coast Audit