A Question of Balance

Independent Assurance of Information Governance Returns

Guidance for Internal Auditors

Department of Health

audit commission

NHS Mersey Internal Audit Agency

NHS South Coast Audit

Contents

Summary

About the internal audit framework

1 The Informatics Directorate of the Department of Health (DH) commissioned this internal audit framework in response to the requirement in Annex 1 (National Expectations) of the NHS Informatics Planning Guidance 2010/11:

> *"An IG audit utilising the centrally provided audit methodology should be included within the work plans of each organisations' auditors."*

2 The audit framework provides a basis for the efficient and consistent delivery of independent audit of self-assessed Information Governance Toolkit (IG Toolkit) returns.

3 It is applicable from version 8 onwards.

4 It is for use by an independent internal auditor. This will be the internal auditor provider in the significant majority of cases but may be an alternative provider (for example an external consultant or auditor[I]) where no suitable internal audit capacity exists.

5 The DH appointed the Audit Commission, South Coast Audit and Consultancy Services and Mersey Internal Audit Agency as the joint authors of the framework.

Which organisations does the framework apply to?

6 The framework applies to the following organisations:

- Primary Care Trusts
- Acute trusts
- Foundation trusts
- Mental Health trusts
- Ambulance trusts
- Strategic Health Authorities.

7 This internal audit tool is not for use in a social care environment and would need adapting for social care and secondary use organisations. A separate audit tool is available for secondary use organisations, produced by the NHS Information Centre for Health and Social Care.

[I] For independence reasons, an audit provider cannot provide internal audit services at a client where they are also the appointed external auditor.

Who is this framework for?

8 This framework is for use by:

- **Accounting Officers (Chief Executives) and Senior Information Risk Owners:** to ensure that internal audit addresses key information governance risks and contributes to assurance for their annual report and the annual statement of compliance and statement of internal control.
- **Internal Auditors:** to conduct audits in line with recommended guidance, consider suitable evidence and risks and ensure that audits are suitably tailored in line with national and local risks.
- **Caldicott Guardians, Non-Executive and Executive Directors:** to inform their understanding, awareness and monitoring of the organisational response to information governance and wider assurance risks across the organisation.
- **Governing health bodies:** for example Strategic Health Authorities, Monitor, External Audit and the Care Quality Commission, as assurance that the basis on which they are performance managing organisations is sound.[I]

What does the framework comprise?

9 The internal audit framework comprises:

- **A series of internal audit requirements:** (matched to the IG 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 respondents no longer than 15 minutes to complete. Details on running the survey follow later in this report.

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

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

[I] It is not a requirement for Internal Auditors to provide copies of reports to governing health bodies; it is the responsibility of governing health bodies to request these assessments directly from the organisations concerned.

When is the audit carried out?

11 The organisation and the audit provider should agree the timing of the internal audit review. In planning the audit, the organisation and the audit provider should consider their ability:

- to complete the assessment; and
- to act on recommendations arising
- before interim or final toolkit submission dates.

How long will the audit take?

12 The internal audit should take up to ten days in most environments, although this may vary depending on organisational arrangements or other local reasons. For example, the implications of provider-commissioner splits within PCTs or where it is necessary to involve shared informatics services or other third parties.

Will this represent extra work?

13 Internal audit plans are risk-based and auditors consider information governance as part of this planning. Typically, plans will include information governance assurance and this framework provides a consistent approach for this work; it does not, necessarily, represent a new internal audit requirement.

14 Where internal audit plans do not include information governance assurance, this will result in extra cost or a revision to those plans.

Are all requirements audited every year?

15 The new framework is a risk-based approach but contains a set of key requirements, defined and mandated by the Department of Health; these will typically reflect national risks and priorities and may change from year to year. The internal audit must include these key requirements every year. For 2010-11, there are 23 key requirements in total as shown in Table 1, though all 23 do not apply to every organisation-type, e.g. acute trusts have 22 key requirements and Strategic Health Authorities have 19:

Table 1 IG Toolkit

Key Requirements for 2010[I]

IG Management (8100 Series)		Confidentiality & DP Act (8200 Series)		Information Security & Clinical Information Assurance (8300 - 8400 Series)	
8101	IG Framework	8200	Confidentiality & DP Act Skills & Experience	8300	Information Security Skills & Experience
8110	Contractual Arrangements	8201	Staff Guidance	8301	Risk Management Programme
8111	Employee Contracts	8202	Consent Prior to Use	8302	Event/ Incident Management
8112	Training	8203	Proposed Use	8303	Registration Authority
		8209	Processing Outside UK	8304	Smartcards
		8210	Information Asset Security Compliance	8305	Access Controls
				8307	SIRO Role
				8308	Information Transfers
				8313	Network Security
				8314	Mobile Security
				8315	Airwave Security
				8323	Protection of Assets
				8401	NHS Number Use

Source: Informatics Directorate, Dept of Health

16 The internal audit provider may recommend more requirements. This will refer to past performance and other cumulative audit knowledge and experience. Local security incidents and recommendations from other IT and information related audit work will also influence selection of these requirements. Inclusion in the audit scope will be subject to discussion and agreement with the organisation.

[I] Requirement 8113 on Training is also a key requirement but this applies to Social Care organisations only and therefore is out of scope.

Introduction and background

External context

17 The profile of information governance in the public sector rose significantly following the HM Revenue and Customs data loss of 25m child benefit records in 2007. Public and media interest remains high and shows no sign of dying down. Health records are among the most sensitive items of personal information in the public domain. With many thousands of healthcare interactions taking place every day; the governance and assurance required to protect these records and manage information securely is a priority for the NHS and the public. Given the sheer size and scale of UK healthcare, the NHS complies relatively well with basic standards for information governance[I]. However despite this some high-profile data losses continue. These data losses, variable levels of compliance with the IG Toolkit, increased use of digital records and the ambitions for better data sharing across public sector means the NHS cannot afford to be complacent. All healthcare organisations need to be as good as the best.

18 As public awareness of information governance increases; tolerance for poor performance, mishandling, data losses and breaches of confidentiality decreases. Confidence in public sector 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 maintain public trust and meet patient expectations of confidentiality.

The IG Toolkit process

19 All NHS organisations submit an annual IG Toolkit return, supported by interim submissions. Organisations submit online following a self-assessment. Many organisations subject their IG Toolkit returns to independent scrutiny, usually from their internal audit provider.

20 Internal audit reviews carried out so far have identified differences between self-assessed and independently validated scores, for example through overstatement of scores, misinterpretation of requirements or the absence of supporting evidence.

21 The Audit Commission report "Taking It On Trust[II]" highlighted deficiencies in the wider self-assessment process and cited several Healthcare Commission examples which suggested that trust self-assessments of compliance with standards were often inaccurate. The report went on to conclude that for self-assessments:

> *"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 as the regulatory framework is increasingly dependent on self-assessments and self-certification."*

[I] "The right information, in the right place, at the right time" Care Quality Commission report, Sept 2009

[II] "Taking It On Trust", Audit Commission, April 2009

22 The Care Quality Commission national study on information governance in trusts[i] recommends that:

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

23 The Department of Health has accepted this recommendation in full and this framework is part of its response to improving the validation of IG Toolkit assessments across healthcare organisations.

What's new in version 8

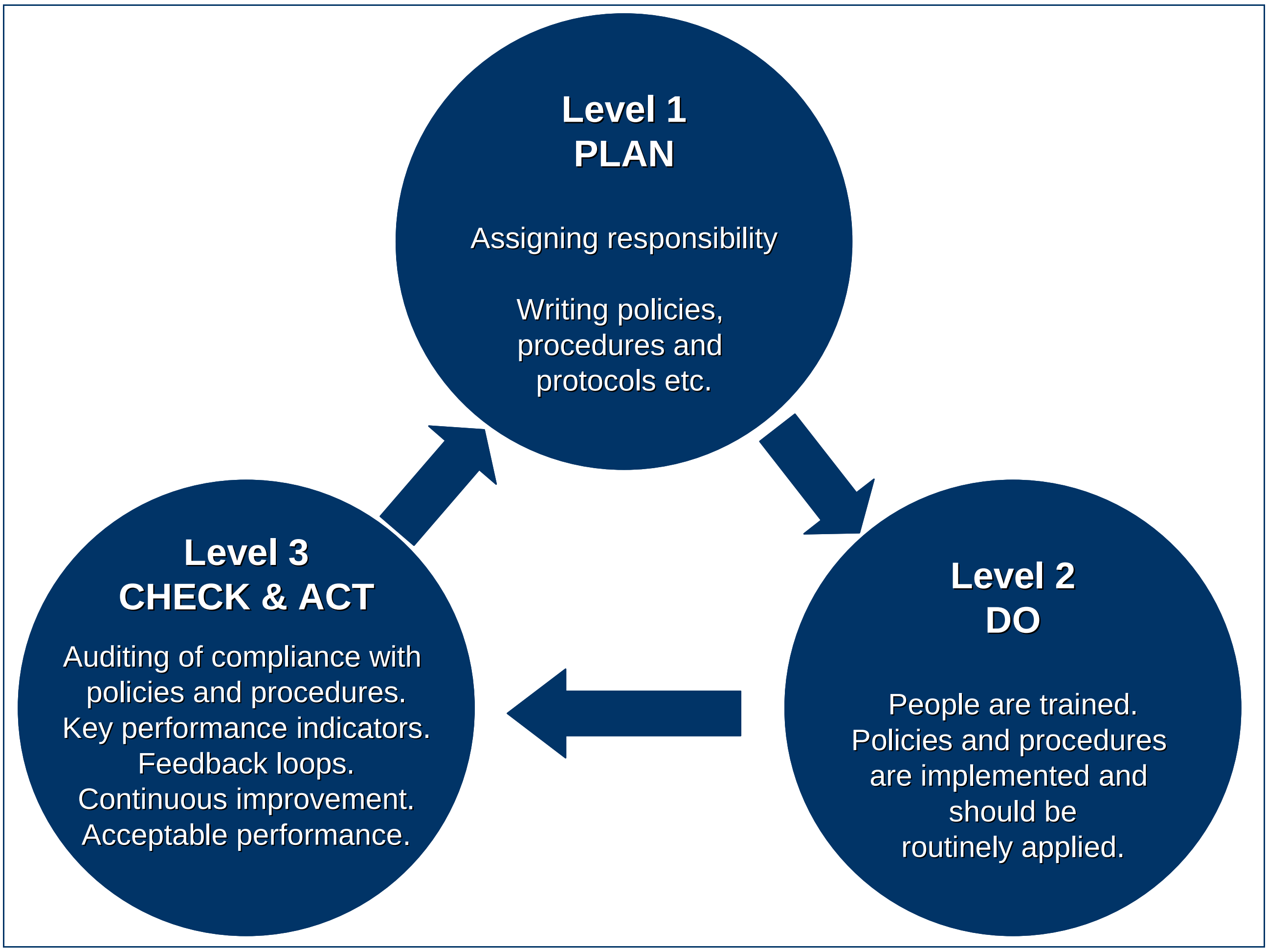
24 The newest version of the IG toolkit has a significantly different look and feel to previous versions. Importantly, the ability to link evidence directly to toolkit returns should improve the clarity and quality of the audit trail. However, auditors are not restricted to the evidence submitted as part of the toolkit and may ask for additional material and interviews to support their assessments.

25 The IG Toolkit remains based around a plan, do, check, act model and these broadly correlate to the assessment levels defined within the toolkit. (See Figure 1).

[i] "The Right Information, In The Right place, At The Right Time - a study of how healthcare organisations manage personal data", published in September 2009.

Plan Do Check Act Model

As aligned to IG Toolkit assessment levels



Level 1
PLAN
Assigning responsibility
Writing policies, procedures and protocols etc.
Level 2
DO
People are trained.
Policies and procedures are implemented and should be routinely applied.
Level 3
CHECK & ACT
Auditing of compliance with policies and procedures.
Key performance indicators.
Feedback loops.
Continuous improvement.
Acceptable performance.

Source: Mersey Internal Audit Agency

Scoping the review

Scope of work

26 Appendix 1 sets out an example template for terms of reference or a project brief. This describes the scope of the framework, in summary this comprises:

Internal governance process

- how information is collated from across the organisation to assess the IG toolkit scores;
- how the organisation is structured to assess compliance against requirements;
- how the returns are made to the IG coordinator;
- how returns are validated or moderated;
- how returns are evidenced; and
- how returns are signed off for submission.

Validity of returns

Considering the validity of the scores for submission at a given date, for requirements defined by the Department of Health as 'key'; given the evidence available to support them.

Wider risk exposures

Identifying any risk exposure highlighted by current performance or practice.

Approach

27 The review and opinions are based on:

- discussions with relevant officers involved with information governance;
- review of available evidence presented in support of the IG scores;
- data from a staff survey to assess awareness and workplace practice;
- examination of information governance related 'Serious Untoward Incidents'; and
- review of information governance improvement plans to meet NHS Informatics Guidance and the Operating Framework.

28 Internal auditors should document all findings and opinions in line with professional internal audit standards and local working practices.

Mandated key requirements from the Department of Health (DH)

29 These are the key requirements prescribed and reviewed yearly by the DH. Table 1, on page 7 of this report, lists the key requirements for 2010/11.

Risk assessment of remaining requirements

30 Internal auditors should refer to previous assessments, relevant audit work and cumulative audit knowledge and experience to decide whether to include more requirements in scope for review. Where suitable, internal auditors should draw up a recommended set of requirements based on this risk assessment and discuss and agree their inclusion in scope with the organisation.

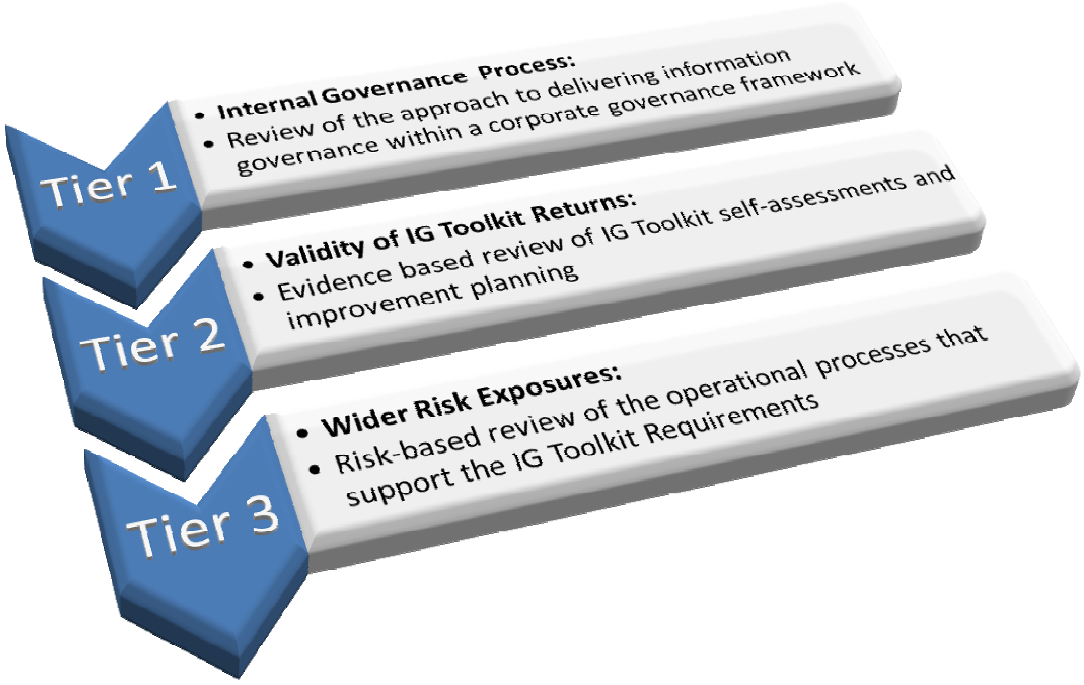
Requirements of concern or interest to the organisation

31 There may be certain requirements considered out of scope where they are of particular concern or interest to the organisation. Where this is the case, and there is capacity within the audit plan, these should be included where appropriate following discussion and agreement with the organisation.

32 Figure 2 summarises the three tier approach that shows how the high-level review incorporates the key requirements, and that organisational risk determines the need for extra work; this may be additional to this IGT audit.

Three Tier Model

This sets out the risk-based approach



Tier 1

- **Internal Governance Process:**
- Review of the approach to delivering information governance within a corporate governance framework

Tier 2

- **Validity of IG Toolkit Returns:**
- Evidence based review of IG Toolkit self-assessments and improvement planning

Tier 3

- **Wider Risk Exposures:**
- Risk-based review of the operational processes that support the IG Toolkit Requirements

Source: South Coast Audit & Consultancy

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

Internal governance process

Organisational challenge

34 Information governance remains prominent in both the private and public sector. Internal auditors require assurance that self-assessment is integral, inclusive and embedded.

35 The following questions will help internal auditors challenge those responsible for the oversight of organisational compliance with information governance requirements:

- how is information governance embedded within the culture of the organisation?
- how is information security and patient confidentiality upheld?
- how does information support management decisions - how can organisations be certain the underlying data is accurate enough and complete?
- is there an IG improvement programme in place that meets organisational needs and if so, how does the organisation manage and control this?
- how does the organisation set priorities for the highest risks and manage these effectively?
- how does the organisation ensure the correct interpretation of agreed strategies and policies in the workplace?
- how are information governance issues reported and discussed at board level?

IG as part of a corporate governance framework

36 The objective of this part of the review is to obtain assurance that the culture of the organisation embeds information governance.

37 Internal auditors should cover the following areas through document review and interview or discussion with key staff:

- Board level leadership, roles and responsibilities;
- Senior Information Risk Owner (SIRO) and Caldicott Guardian roles;
- Statement of Internal Control (SiC) and Serious Untoward Incident (SUI) reporting;
- integration within the Board assurance framework and corporate risk management;
- relevant strategies, policies, standards, practices and procedures; including assurance arrangements;
- organisational roles and groups for delivering information governance (for example, committees, steering groups, programme boards, job descriptions, roles and responsibilities);
- oversight of IG improvement planning and performance management;
- communication to and understanding of good IG practice by staff in the organisation.

38 Internal auditors will typically gather evidence to support how well IG is working within the organisation. Findings from the staff survey support this part of the review.

Validating the scores

Accessing the toolkit

39 Ask the IG Lead in the organisation to set you up with **read only** access to the IG toolkit return. Ensure that this is an individual and unique user ID and not a generic audit or other shared account.

40 This will provide you with access to the score and the underlying evidence base.

41 Evidence referenced outside the online system should also be collated in readiness for the audit or separate access provided.

Reviewing the audit requirements

42 Each IG Toolkit requirement has an associated audit requirement. These are provided in MS Word and PDF format for ease of reference.

43 The internal audit requirement summarises the IG Toolkit requirement and gives examples of assurance required and potential sources of evidence to satisfy three levels of compliance (1 through to 3). The evidence is consistent with that included in the IG Toolkit requirement but is not limited to this where the auditor believes that more evidence may help to justify the score. Internal audit requirements are available from the IG Toolkit website.

44 Where suitable, the internal audit requirements reference evidence review guides that set out good practice principles for reviewing common types of evidence. Evidence review guides are also available from the IG Toolkit website.

45 A worked example of an internal audit requirement and evidence review guide is included at Appendix 2.

46 Evidence review guides comprise:

Characteristics

This sets out key features of the evidence in question. For example, for an intranet this might include availability, searchability, currency of information, ability to challenge and comment and personalisation.

Tasks

These suggest potential audit work to test the evidence. It is not a prescriptive list and is for guidance only.

Questions

These suggest potential questions to ask as part of interviews to test the evidence. As above, these are not prescriptive and are for guidance only.

Validating the scores

47 Following review of all the available evidence, the internal auditor will be in a position to make an initial assessment about the validity of individual scores. However, this assessment needs to be triangulated with data from the staff survey.

The staff survey

Why use a survey?

48 The survey seeks to capture individual knowledge, opinions and behaviours about handling of confidential and sensitive information. It is a tool for challenging corporate perceptions and informing improvement planning. Given the subjective nature of the survey, the outcome should not be taken as a definitive statement of workplace practice and compliance. The survey questions are available from the IG Toolkit website.

Web or paper based

49 The survey is web-based. Unless you have enough people to undertake the analysis from a paper based survey, we strongly recommend opting for a web-based solution. Not only is this easier to manage for larger sample sizes, it automates the analysis and increases audit efficiency by saving time and cost. It is also significantly more environmentally sound by reducing paper used.

Selecting a hosting solution

50 Hosting is the responsibility of the internal audit provider and two choices will typically be available to you.

- Host on your own servers using a licensed version of your chosen survey software. Several suppliers are available.
- Host externally through a web survey provider. Annualised or pay as you use alternatives exist.

51 The survey provided is anonymous and therefore not classed as personal data. The Head of Information Governance Policy at the Informatics Directorate of the Department of Health has undertaken a privacy impact assessment of the survey. He has decided that responses to the questions do not form sensitive data. Therefore, no restrictions on hosting it as a web-based survey apply.

A documented privacy impact assessment must follow any change to the survey to ensure that no personal or sensitive data has been added. Examples might include: asking respondents for their names or adding an organisational identifier. Combined with others survey responses, such changes could be sensitive; which imposes legal obligations where an external web survey provider uses a non-UK hosting environment.

52 If a decision is made to alter the survey so that personal or sensitive information is collected, internal audit providers must assure themselves of the location of the hosting environment if an external web survey provider is selected. If the data is to be hosted outside the UK, both the Data Protection Act 1998 and Department of Health (DH) guidelines must be adhered to. The Data Protection Act requires that personal information is not transferred to countries outside of the European Economic Area

unless that country has an adequate level of protection for the information and for the rights of individuals. More stringently, the DH requires that personal identifiable information is not transferred outside the UK unless appropriate assessment of risk has been undertaken and mitigating controls put in place. Therefore, internal audit providers should think carefully before making any additions or changes to the survey.

53 In addition, you cannot assume that a UK registered company will host in the UK. You will need written confirmation of this before continuing with the survey. This is only required if you have changed the original survey and your changes represent the addition of personal or sensitive information.

Why is the survey anonymous?

54 Extensive research and experience shows that anonymity improves response rates. This is true where questions are controversial and could be self-incriminating. For these reasons we strongly suggest conducting the survey anonymously. Avoid any 'back door' techniques to identify respondents retrospectively.

What about vexatious completion?

55 Vexatious completion is where respondents use the anonymity as an opportunity to answer questions in a way that they believe will damage the organisation. Selecting suitable sample sizes to give high levels of confidence and low error rates help to guard against this. Research and experience suggests that this problem is widely overstated and respondents answer such surveys honestly.

How many surveys do I need to send out?

56 In most organisations it will be desirable to send the survey to all staff with a work email and internet access. This avoids the requirement to sample a cross-section of the organisation.

57 If you wish to use a sampled approach, Appendix 2 of this report provides detailed guidance on sampling.

Notifying respondents

58 Notify respondents by email, containing a link to the survey. The text of the covering email is important for three reasons:

- staff need to know what the survey is for and why or how they have been selected;
- staff need to know the survey is important to top management, ideally the email should come from the Chief Executive or the senior board member leading on information governance;
- staff need to understand clearly how the data will be used, shared and stored. They also need confirmation of whether the survey is anonymous.

59 Appendix 3 of this report provides suggested content for a covering email.

Timing of the survey

60 Issue the survey in good time to allow for analysis of the results and incorporation into the audit findings. Allow an extra week in case of poor response rates and try to schedule the survey to avoid main leave periods such as school holidays and half-term periods.

61 The survey will normally run for two weeks, check responses and issue reminders after one week where response rates are low.

What response should I expect?

62 Response rates can be difficult to predict, web surveys typically see response rates of between 5 and 30 per cent. The issue of reminders, coupled with strong senior corporate sponsorship, can increase this to between 59 and 83 per cent.

Analysis and interpretation of results

63 Paragraph 48 highlighted the subjective nature of the survey, the results provide a sign of potential risk areas or where workplace practice conflicts with organisational policy.

64 It may be useful to group analysis under similar issues - for example training and guidance. Responses that conflict with self-assessment scores do not mean the self-assessment is wrong. For example, an organisation may score itself positively for training delivery but the survey may show that staff feel they have not been adequately trained. This does not directly challenge that training has been carried out (though this may be the case) but could point to the content of the training, suggesting lack of focus, or understanding of the training by staff.

65 Internal auditors should not discount statistically small returns or outliers that challenge self-assessments; it is worth bringing these to the attention of the organisation because it only takes one individual to cause a serious untoward incident.

66 The use of charts based on the survey data to challenge or support self-assessments can be included as part of a report or presentation.

Secondary use of survey data

67 If you plan to undertake comparative analysis between organisations using anonymised survey data, you must have the consent of the organisations concerned and we strongly recommend that you amend the covering email to advise staff of this use.

Wider risk exposure

Additional risks

68 During the work, internal auditors may identify issues that, in their professional opinion, widen the organisation's information governance risk. Examples may include:

- IG Toolkit improvement plans that are unrealistic (for example, objectives or time);
- inadequate resources to improve;
- an accurate self-assessment that represents a poor overall performance or isolated areas of non-compliance;
- a high number of serious untoward incidents (SUIs);
- a failure to investigate and learn lessons from security incidents and events;
- observed poor practice during the audit (for example a failure to use suitable physical controls).

69 These risks may or may not feature as part of the evidence set for one or more requirements. Where it is the internal auditor's view that such risks compromise effective information governance and undermine compliance with one or more requirements; the overall internal audit opinion should take account of this.

Forming a judgement

Assessing each requirement score

70 The review of each scored requirement should reach one of the following four assessments in Table 2; based on the information, evidence and survey results provided.

Table 2 Assessing each requirement score

Select 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

71 The key difference between overstated and unsubstantiated is 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; this is assessed as **'overstated'**.
- Where an organisation has not provided or does not have supporting evidence, this is assessed as **'unsubstantiated'**.

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

The overall audit opinion

73 The overall opinion is based on internal audit assessment of:

- internal processes for completing IG returns;
- validity of returns; and
- wider risk exposures.

74 The opinion should be in the local format agreed by the organisation's Audit Committee. Table 3 provides example overall audit opinions.

Table 3 Example overall audit opinion

Internal audit opinions generally 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 which, 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 which 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 which 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 which [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

75 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 upon 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 which subsequently appear to contradict the opinions herein.

Reporting and action planning

Options

76 Reporting should be in line with local internal audit protocols but would typically include:

- overall internal audit opinion;
- assessment of individual scores;
- action plans - agreed management action arising from the internal audit.

Timing

77 Internal auditors should present reports and action plans to management in good time to allow for any action required on the scores by the next required submission date.

Follow on action

78 The internal audit represents a snapshot and while reports may acknowledge management action, these should not be extensively revised on a continuing basis. Should management require more detailed review or follow-up, this should be revisited with the organisation's Audit Committee as part of internal audit planning.

Appendix 1 – Example terms of reference

Introduction and background

79 Information, its supporting systems and technology are critical to the successful delivery of corporate objectives. Systems and technology need to be robust, well-maintained and effectively used to protect the confidentiality, integrity and availability of the information that they provide.

80 High-profile public sector data losses have brought these issues into the public spotlight in the last two years; including in the NHS. <*insert organisation name*> needs adequate assurance that it has robust systems, technology and processes to minimise the risk incidents affecting day-to-day operations, or adversely affecting its public reputation.

81 As part of the Department of Health commitment to ensuring the highest standards of information governance, it has developed an Information Governance Assurance Framework supported by the Information Governance Toolkit (IG Toolkit). The IG Toolkit is a self-assessment and reporting tool that organisations must use to assess local performance; in line with the requirements set out in the NHS Informatics Guidance and Operating Framework 2010/2011.

82 All NHS organisations need to demonstrate compliance with the key IG Toolkit requirements through achievement of at least Level 2 attainment and should be achieving Level 2 against all the requirements by 31 March 2011.

83 As part of their IG Toolkit final submission organisations must also confirm their acceptance of the IG Assurance Statement. The Statement is an agreement to comply with the additional terms and conditions that apply to organisations that have access to NHS CFH services and an acknowledgement that failure to maintain compliance may result in the withdrawal of these services.

84 In addition, from 2010/11 all organisations must ensure that their IG Toolkit submission is subject to independent audit.

Objective

85 The objective of our review is to provide an opinion on the adequacy of policies, systems and operational activities to complete, approve and submit the IG Toolkit scores. We will also provide an opinion on the validity of the scores based on the evidence available.

Scope of work

86 The scope of our work is limited to those requirements within the Information Governance Toolkit that have been mandated as ‘key’ for 2010/2011 by the Department of Health. In arriving at our opinion we will consider:

Internal governance process

87 We will review of the processes for the collation of information from across the organisation for the assessment of the IG toolkit scores including:

- how the organisation is structured to assess compliance against requirements;
- how the returns are made to the IG co-ordinator;
- how the returns are validated and moderated;
- how the returns are evidenced; and
- how the returns are signed off for submission.

Validity of returns

88 We will consider the validity of the scores to be submitted for <*insert date*> for those requirements defined by the DH as "key"; based on the evidence to support them.

Wider risk exposures

89 We will identify any risk exposure highlighted by current practice.

Approach

90 Our review and opinions will be based on:

- discussions with relevant officers involved in the IG process;
- review of available evidence presented in support of the IG scores;
- data from a staff survey to assess awareness and workplace practice;
- examination of information governance related Serious Untoward Incidents;
- review information governance improvement plans to meet NHS Informatics Guidance and the Operating Framework.

Key contacts

91 The key contacts for this review will be:

<Enter contact details>

Proposed timetable

92 The review will be undertaken during <*insert timescale*>*.* We expect that agreement of the dates below will enable the review to complete within the allotted time. Should any urgent matters arise from the review, we will report these to you immediately, so you can agree and undertake any necessary work as a priority.

Action	Planned dates
Fieldwork start	dd/mm/yyyy
Discussion document to client	dd/mm/yyyy
Responses by client	dd/mm/yyyy
Final report	dd/mm/yyyy

Information requirements

93 This is not an exhaustive list, but we require the following to support the review:

- signed Information Governance Statement of Assurance;
- read-only access to the online IG Toolkit assessment and the evidence included in it;
- copies of any additional policies and procedures and supporting evidence relating to the Information Governance toolkit not accessible through access to the online IG Toolkit assessment;
- access to staff with relevant roles and responsibilities to allow liaison and interview.

Survey administration

94 The audit includes the use of a staff survey and some assistance to identify and target an appropriate sample population will be required.

Feedback and reporting

95 Subject to the availability of information requirements, and on completion of our fieldwork, the auditor will hold a discussion meeting with officers subject to your availability. This will provide an opportunity to corroborate the factual accuracy of the matters identified and to discuss and agree possible practical solutions to any matters identified.

96 We will issue the final report as follows:

Name	Title

Appendix 2 – audit process

Summary

The evidence in the internal audit requirement expands on the evidence in the attainment levels of the IG Toolkit requirement. Good practice pointers for evidence and challenges through tasks and questions are included where appropriate in the relevant evidence review guides. Internal auditors should review the evidence in order to attempt to satisfy the assurance levels in the audit requirement and finally these should be reviewed in the light of relevant survey data, relevant issues and inconsistencies highlighted.

Requirement 8302 has been used as an example to show how the various elements connect together to form a judgement.

Worked Example: Requirement 8302 - information security incident/ event reporting

Evidence in the IGT Requirement (summarised)

Level 1 documented and approved procedures

Level 2 implementation activity - communication to staff and inclusion in contracts

Level 3 Monitoring of compliance, analysis and review

Organisations may have uploaded key electronic evidence to the IG Toolkit against relevant requirements.

Examples of 'assurance required' in the internal audit requirement

Level 1

- policies and procedures have been documented, reviewed and approved;
- approval and review is by senior management or suitably delegated group and includes the Senior Information Risk Owner, Board (or formally delegated sub-group) and Information Asset Owners or equivalents;
- date of last review and approval is recorded;
- approval is by a nominated signatory; and
- period since last review does not exceed 12 months, (or if greater, if supported by an approved policy which states the required time for review).

Level 2

- relevant policies and procedures have been disseminated to all staff and staff understand how to follow them; and
- relevant training has been provided to all third party contractors to explain how policies and procedures should be followed; and
- an ongoing programme of security/ event reporting awareness is in place for all employees of the organisation, both permanent and contract.

Level 3

- compliance reviews and monitoring (e.g. spot checks) are carried out and learning is captured;
- event and incident reports are analysed for trends as well as evidence of compliance and non-compliance;
- relevant policies; and procedures are regularly reviewed to take account of learning from compliance reviews and monitoring.

Examples of 'sources of assurance' in the audit requirement

Level 1

- relevant, up to date and controlled, policies and procedures;
- an up to date register or record of third party contracts;
- up to date staff data as the basis for disseminating procedures and delivering training;
- minutes from meetings or discussions with key staff as evidence that the policies and procedures contribute to and are incorporated within governance structures.

Level 2 (all of Level 1 plus)

- sampled incident and event reports;
- corporate training plans;
- examples of awareness material (i.e. posters, e-mail campaigns, network log-in script messages, intranet articles);
- relevant web survey data.

Level 3 (all of Level 2 plus)

- documented learning from organisational spot-checks on staff, to ensure compliance with incident and event reporting policies;
- trend analysis and other management reports from event and incident reporting system;
- changes to relevant policies and procedures (with derivation);
- changes to arrangements and governance structures (with derivation).

Examples of a relevant evidence review guide (Intranet content)

Characteristics

- Effectiveness of search
- Currency of information

Tasks

- Check effectiveness of a search for “SIRO” - are the top 10 search results relevant?
- Check currency of information - when was information last updated?

Questions

- When was the relevant intranet information last updated or reviewed?
- How are staff in need of reasonable adjustments catered for?

Examples of relevant survey questions

Qu. 1 Has what you were told about information security when you first joined the organisation been relevant and useful in your job?

- Yes
- Somewhat
- No
- I received no guidance on this when I joined

Qu. 2 If information security has been compromised (for example if information is missing or has been accessed inappropriately), I know who to inform and what to do.

- Strongly agree
- Agree
- Neither agree nor disagree
- Disagree
- Strongly disagree

The survey data does not override other evidence; it seeks to capture individual knowledge, opinions and behaviours about handling of confidential and sensitive information. It is a tool for challenging corporate perceptions and informing improvement planning. Given the subjective nature of the survey, the outcome should not be taken as a definitive statement of workplace practice and compliance.

Auditors to note

This appendix contains sampled and summarised extracts of the internal audit approach.

Appendix 3 – Survey sampling

A sampled approach

97 Three factors affect this. The sampling frame, the required confidence level and the error level, these terms are explained in more detail below. For ideal results we recommend a confidence level of 95 per cent and an error level not exceeding five per cent.

What is a confidence level and level of error?

Sampling frame

98 The sampling frame is all staff in the organisation that have a work email address and access to the internet.

Confidence level

99 This is how confident you feel about your error level expressed as a percentage. Imagine you were running the survey multiple times; this figure represents how often you would expect to get similar results.

Error level (also known as the confidence interval)

100 This means that you feel confident that your results have an error of no more than your chosen percentage.

101 These two concepts work together to determine how accurate your survey results are. For example, consider a survey with 95% confidence with an error of 5%. This means that if you were to conduct the same survey 100 times, the results would be within +/-5% of the first time you ran the survey, 90 times out of 100.

Is sampling necessary?

102 There is no requirement to sample; you can choose to ask everyone in the sample frame to complete the survey. However, for a variety of reasons you may choose to use a sample of staff. The following section explains how to use a sampled approach.

Calculating your sample

103 For this survey, your sampling frame is all organisational staff (clinical and non-clinical), including contractors that have a work email and access to the internet.

104 Log on to the following website to calculate your sample size. http://www.surveysystem.com/sscalc.htm

105 Example sample sizes are shown in the tables below. You can take a higher error level or reduce the confidence level to reduce sample sizes. However 5% and 95% are considered to be industry standard and therefore optimal levels.

Sample sizes

Examples of samples for typical populations at optimum confidence and error rates

Confidence (%)	Error (%)	Population	Sample	Percentage of Population (%)
95	5	500	217	43
		1,000	278	28
		1,500	306	20
		2,000	322	16

Alternate sample sizes

Effect of changing the error level on sample sizes

Confidence (%)	Error (%)	Population	Sample	Percentage of Population (%)
95	10	500	81	16
		1,000	88	9
		1,500	90	6
		2,000	92	5

Selecting respondents

106 A stratified sample is recommended and the stratification criteria should be clinical and non-clinical. Select half the required sample from each stratum and use either a random or systematic sample to identify respondents.

Appendix 4 – Survey email

The following text is recommended as the basis of a covering email from the organisations Chief Executive or Board Level Director leading on Information Governance:

Dear Colleague,

As part of ensuring <<Organisation Name>>'s commitment to information governance and improved compliance with the NHS Information Governance Toolkit, we are undertaking an internal audit review of information governance.

One part of this review comprises completion of a survey by staff; this will help us to assess the effectiveness of our arrangements.

Your response is anonymous, but we do ask you to give details of your job area as this helps us to put the results into context.

Please answer the questions honestly and from an individual perspective and avoid the temptation to give what you think is the 'right' answer. Read the questions carefully as some require more than one response. The survey will remain open for two weeks until <<insert date>> and should take no more than 15 minutes to complete.

Data from the survey will be available only to the organisation's internal auditors and kept in line with their retention policies.

Thank you for your help

<<Chief Exec>>

Appendix 5 – Acknowledgements

107 This framework was commissioned by the Department of Health Informatics Directorate.

108 The following people and organisations contributed to the completion of this framework:

Name	Role	Organisation
Andrew Ball	Head of IT Performance	Audit Commission
Tony Cobain	Head of IM&T Assurance	Mersey Internal Audit Agency
Ian Hitchmough	IT Performance Specialist	Audit Commission
Paul Merison	Head of IT Audit Services	South Coast Audit & Consultancy Services
Philip Reynolds	IT Assurance Manager	Audit Commission

The authors would also like to acknowledge the support of Marie Greenfield (Information Governance Policy Manager) and Phil Walker (Head of Information Governance Policy) at the Department of Health.