

CONTENTS

		Page
Chapter 1	Introduction	3
Chapter 2	The audit environment	5
Chapter 3	The audit process	7
Annex A	Sample definitions of report opinions and issue categories	21
Annex B	Glossary of key terms	23



INTRODUCTION

1.1 This guide provides good practice guidance in support of Government Internal Audit Standard 7 – Management of Audit Assignments, with the objective of providing practical guidance on how a risk-based audit should be planned, conducted and managed. This guide has been primarily prepared to support the conduct of assurance assignments, which contribute to the annual audit opinion, but the generic principles are generally applicable to all work likely to be conducted by Internal Audit.

1.2 Risk-based audits direct audit resource towards controls over the risks with the highest probability of the highest impact on the organisation.

1.3 Risk-based audits can be conducted as part of the audit plan or as consultancy work requested by management but should follow the processes set out in this guidance in either case.

1.4 This guide also provides good practice guidance to improve the likelihood of successful delivery of audit objectives through awareness and management of risks specific to audits and, as a consequence, is addressed primarily to people who undertake risk-based audits themselves.

1.6 Definitions of key terms are included in the Glossary at Appendix B.

2

THE AUDIT ENVIRONMENT

2.1 The quality of audit assignments, the personal development of internal audit team members, efficiency and the credibility of internal audit are all enhanced by and dependent on the following:

- clear lines of reporting and advice, including supervision and mentoring;
- clearly understood standards of conduct and ethics;
- access to the skills of specialists, whether in-house or outsourced;
- resource and succession planning;
- ongoing audit team-level risk management;
- the support of senior management and the Audit Committee;
- knowledge-sharing and in-team communications;
- training, development and staff evaluation processes;
- a shared focus on continuous improvement;
- regular communications with senior management and the Accounting Officer; and
- clearly defined quality assurance and authorisation procedures.

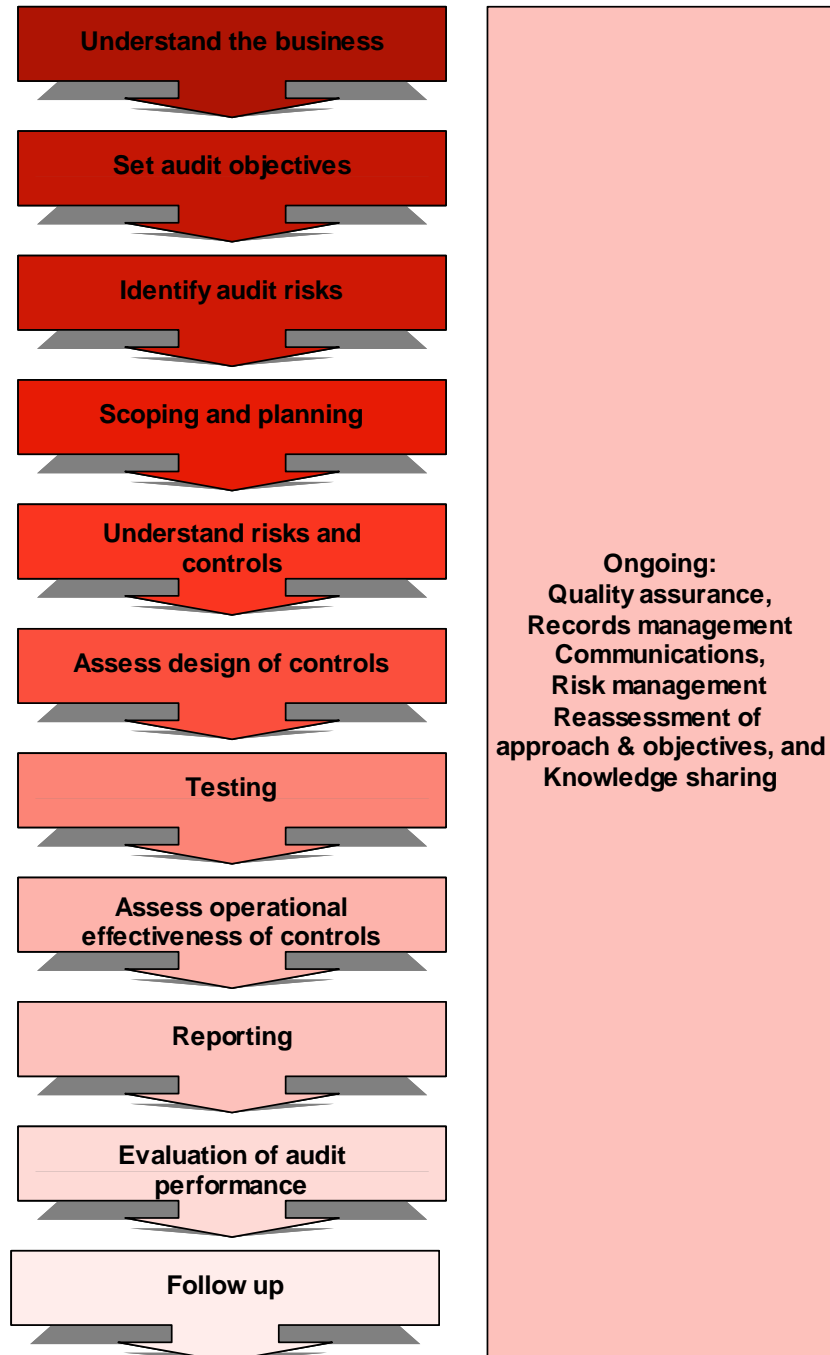
2.2 Every audit team should also put in place appropriate local standards and practices to provide evidence that a risk-based approach has been adopted.

3

THE AUDIT PROCESS

Overview of the Audit Process

3.1 Below is an overview of the Audit Process that is explained in more detail in the following subsections.



Understanding the business

3.2 Risks and controls can only be properly understood in the context of ongoing operations, so you should ensure you have at least a high-level and up to date understanding of the objectives and operational environment of the business area under review at the outset of your work.

3.3 For example, you should enquire about significant recent or planned organisational changes and about the management structure. This is essential for managing sensitivities as well as for planning your work and as a basis for making appropriate judgements and recommendations.

Audit objectives

3.4 The objective of each audit assignment should be clearly documented in all cases and should support Internal Audit's primary objective to provide an independent and objective opinion to the Accounting Officer on risk management, control and governance.

3.5 Other generic, underlying objectives for each assignment are likely to include:

- compliance with the Government Internal Audit Standards including due professional care requirements;
- development of ongoing effective working relationships with clients at all levels;
- the training and development of Internal Audit staff; and
- the development of the Audit function within the organisation.

Audit risks

3.6 Risks to the audit's specific objectives and to generic, underlying objectives ('Audit Risks') will arise during the course of every audit assignment.

3.7 You should document key Audit Risks and relevant action plans at the outset of an assignment and should actively manage those risks throughout the assignment.

3.8 In particular you should, in coordination with the Head of Internal Audit or his or her delegate, consider the importance of the assignment in the context of its significance to the overall audit opinion for the year.

Examples of Audit Risks

Could you prevent any of these generic audit risks impacting your assignment?

- key controls are not properly tested and key issues are missed because of lack of the right **skills, experience, supervision or specialist expertise**
- the audit is **scoped too widely / loosely**, leading to failure to meet resource and timeframe targets / to address the issues on a timely basis
- real or perceived **conflicts of interest** impair audit objectivity and undermine the results of the audit
- audit work is performed in insufficient depth to meet **specific management expectations** or concerns
- audits are unable to progress or audit findings are not acted on because of **lack of senior management support** and buy-in
- audits **duplicate the work of other assurance providers**, wasting audit and client resources
- **lack of progress** or failure to escalate on a timely basis means findings become out of date before the audit is completed
- **access** to third parties or to key people or documents is not granted, meaning that prior work is wasted
- the audit team may be **deliberately misled**
- **client relations** are damaged because management sensitivities are not properly handled, there are personality clashes between auditors and management or because management do not feel properly involved / consulted
- there are **missed opportunities** for improving client relationships and the reputation of Internal Audit or for identifying follow on audit or consultancy requirements

Scoping and planning

3.9 You should meet client management during scoping to ensure that you have a common understanding of processes underlying the controls to be reviewed and of business conditions impacting those processes, and to discuss how you will work together during the audit to achieve the best results.

3.10 Client management involvement in scoping assignments is crucial to ensure that you both understand the reason for performing the audit, what you will require and expect of each other and so that you can plan communications and fieldwork effectively.

3.11 You should also discuss at the outset any specific requirements for providing assurance in greater depth than normal, e.g. in the case of known allegations against individuals or where there is a history of poor controls.

3.12 A scope document should be agreed with client management, and circulated to all interested parties, that clearly sets out:

- the assignment objectives;
- assignment scope and any limitations of scope;
- assignment approach and methodology;
- nature of draft and final deliverables and distribution;
- expectations of client management;
- planned resource requirement;
- key forecast dates;
- assignment team members and quality assurer; and
- assignment sponsor.

3.13 Evidence of approval by the sponsor and the Head of Internal Audit or the Head of Internal Audit's delegate should be retained.

3.14 The scope of work should always include assessment of whether objectives are congruent with higher level corporate objectives and evaluation of management's risk analysis.

3.15 The audit objectives and approach should be reconsidered regularly throughout the assignment and should be adjusted, after agreement with management, if appropriate.

3.16 A team with the right mix of experience, specialist knowledge and skills should be selected and responsibility for leading the team and for delivering a successful outcome should be clear to both the audit team themselves and the sponsor. Sources of specialist skills outside the internal audit team should be considered if appropriate, e.g. potential partnerships with outsourced providers or with operational staff with relevant technical skills.

3.17 A budget should be agreed for the assignment, including allocating the time and expenses to be incurred on each part of the assignment.

Example planning checklist

- Are **specialist skills** available if required (e.g. Information Technology, Statistics, Actuarial)?
- Are there any **limitations of scope**? Are these acceptable, documented and agreed with client management before fieldwork begins?
- Has an appropriately senior **sponsor** been identified for the assignment and has that sponsor agreed to buy-into the process?
- Have all appropriate **interested parties** been informed of the review's objectives, timings and proposed approach?
- Have all **timing restrictions** been identified and addressed (e.g. of key people or systems)?
- Has any required **access to third parties** been obtained?
- Are the **distribution lists** for deliverables clear?
- Are assignment team members sufficiently experienced and skilled to perform the work or have appropriate mentoring arrangements been made to address any **skill / experience gap**?
- Does the proposed approach fully meet the audit assignment's **objectives**?
- Have the audit assignment's objectives, scope and approach been clearly **documented and agreed** with client management, including the sponsor?
- Is there any known **ground for concern** that means that audit testing should be performed in more detail than usual in this case?
- Is there any **overlap** between this assignment and other assurance (e.g. internal or external audit) work that could be exploited?
- Are there any **conflicts of interest** in the audit team or with client management that should be addressed or monitored?
- Are there any opportunities to **add more value** through the audit process?
- Are there any signs or is there any history of **management non-cooperation** / lack of buy-in that should be considered at this point?
- Is the audit **resource budget** adequate or over-generous, considering the risk of the processes to be reviewed?
- Does the audit **resource budget** make provision for management review / quality assurance, for travel time and expenses and for training and supervision needs?
- Is the assignment so **high profile** or so important to the Head of Internal Audit's overall opinion on risk management, governance and control that additional supervision or review is needed?

Understanding the risks and controls

3.18 The objectives of the management unit and their relation to the higher-level objectives of the organisation generally should be understood, and the risks to these objectives and to the objectives of the organisation as a whole should also be understood. This may be achieved through discussions with management, through consideration of previous audit work, through risk workshops and / or through review of relevant documentation.

3.19 Management's own risk analysis should always be assessed, along with the appropriateness of management's level of risk acceptance in comparison to the organisation's documented risk appetite. If the risk appetite is not formally defined, you should use your judgement about whether management's approach is acceptable, based on discussions with management and on your understanding of the business.

3.20 The processes underlying the risks and controls to be audited should also be understood through discussion with management, supplemented by review of documentation and / or walkthrough testing. Processes should be documented in a format that will be quickly understood by a reviewer, e.g. in a process map.

3.21 The key risks to the objectives of the processes to be audited should be documented.

3.22 Controls over these key risks should be identified and documented through discussion with management supplemented by walkthrough testing if required.

3.23 Documentation should clearly show how controls relate to key risks and how both relate to the audit scope and objectives; matrices are often used to document the relationship between risks, controls, work done and audit findings.

Keys to effective interviews

- Have your objectives clear in your mind before the meeting.
- Prepare an agenda or set out what you wish to cover at the beginning of the meeting.
- Ensure that your interviewee understands who you are and the purpose of the meeting at the beginning.
- Stick to timeframes or check that the interviewee is comfortable to overrun.
- Be aware of possible conflicts of interest.
- Ask open questions to gauge interviewees' impressions and to ensure that all areas of potential concern have been covered (e.g. is there anything important that we have not discussed?).
- Ask closed and precise questions to ascertain points of fact. · Demonstrate interest.
- Take notes in order to accurately remember what was said.
- At the end, summarise what the meeting has covered and ask if you can contact the interviewee again if further questions arise later in your work.
- Validate your understanding by re-stating it and asking the interviewee if you have understood.
- Write your notes up soon after the interview while you remember what was said.
- Consider whether it would be appropriate to ask the interviewee to check the accuracy of your notes, process documentation or selected key facts after the interview.

Assessing the design of controls

3.24 You should consider whether the design of controls is such as will, in theory, mitigate the risk to a level appropriate to the organisation's risk appetite. If the risk appetite is not formally defined, you should use your judgement about whether the level of residual risk is acceptable, based on discussions with management and on your understanding of the business.

3.25 You should also consider whether there are any instances of over control (e.g. overly restrictive delegations of authority) or any potential process improvements that would better match management resource to risk.

3.26 Deficiencies in the design of controls should be identified and reported to management as set out below.

Testing

3.27 You should confirm your understanding of the design and operation of a control through testing, i.e. through obtaining objective evidence.

3.28 Testing can consist of:

- checking for evidence that controls have been operated in a sample of cases;
- reviewing documentation; or
- verifying an understanding with a third party.

3.29 It is possible to test controls (compliance testing) or individual transactions (substantive testing). See Glossary for further explanation.

3.30 Compliance testing is generally the first resort for internal audit, because internal audit provide an opinion on 'risk management, governance and control'. However, if controls are known to be poorly designed or not in place, you may need to rely more heavily on substantive testing to provide evidence of whether or not the unmanaged risks to the organisation have materialised into actual issues or not.

Checklist for assessing the effectiveness of testing

- Is the objective of your test clear?
- If applicable, is documentation reviewed original? If not, is there any chance that copies may differ from the original?
- Could Computer Assisted Audit Techniques ('CAATs') be used to test more effectively?
- If applicable, is the proposed sample size appropriate to the risk mitigated by the control, to the frequency of the control's operation/and to the level of confidence required?
- Could your test be redesigned in any way to provide assurance more efficiently or effectively?
- Could a third party re-perform your test based on your documentation and on evidence retained?

Assessing whether controls are operated effectively

3.31 You should consider whether there is sufficient and reliable evidence that controls are operated in practice in the manner and to the extent required to mitigate risks to the level of the organisation's risk appetite.

Reporting

3.32 You should consider, for each failure in the design or operation of a control, whether there is a resultant risk to the management unit's objectives, whether caused by under or over control.

3.33 If there is a resultant risk to the management unit objectives, the exception should be recorded, discussed with management and, if not cleared during this process, included in a formal report.

3.34 Minor issues that do not result in a material risk to business objectives do not need to be reported formally but should be communicated to management and a record of this communication should be retained. Examples could include minor process improvements identified during audit fieldwork or minor control failures that are known to be isolated examples.

3.35 It is good practice to communicate findings to management on a timely basis and to confirm your understanding with them before drafting a formal report.

3.36 Views expressed in writing can be subject to misinterpretation and can be difficult to make major changes to once issued, so you should follow established quality assurance procedures or seek a second opinion on draft reports within the Internal Audit team before first issue to management.

3.37 Management should have the chance to comment on a report in its draft stages and any differences of opinion or factual errors should be resolved, as far as is possible, before the report is finalised. You should consider whether the sponsor has been adequately involved in the report agreement process and whether reporting is targeted at the right levels of management to initiate change.

3.38 It is also good practice to agree statements as to whether management do or do not accept recommendations and action due dates and management owners in the report. This also facilitates follow up (see below).

3.39 Formal reports should be finalised soon after audit fieldwork in order to be of relevance once released. Timeliness of reporting can be of greater importance than detailed editing, provided the content of the report is accurate and clearly presented.

3.40 The objective of a formal report is to document facts of significance for the record, to indicate the level of unmitigated risk and to help engender control and process improvements. Audit report formats should be developed that meet the needs of their different users.

3.41 Consistent definitions should be used to summarise the level of assurance given and the relative priority of individual findings in order that comparison can be made of the relative severity of findings included in different reports. Examples of such definitions are attached at Appendix A.

3.42 Reports should include:

- the audit title;
- date when work was performed and date of issue of the final report;
- the report distribution list;
- an executive summary;
- the audit objectives and scope;
- the audit approach;
- key control deficiencies noted (It may be appropriate to note if any control deficiencies appear to have implications for the annual opinion on the whole of risk management, control and government);
- explanations of why deficiencies result in risk to the organisation;
- recommendations for action; and
- definitions of terms used to indicate the level of assurance given and the relative priority of individual findings.

Keys to successful formal reporting

- An executive summary of 1 or 2 pages should be included in the report so that readers can get a clear overview of the issues identified and the level of assurance provided.
- Issues and recommendations should be clearly identified, e.g. by being set out in a tabular format.
- The risks associated with not acting on an audit recommendation should be clearly stated in the report.
- Terms should be defined and clear language should be used, i.e. avoiding jargon.
- Unconstructive or overly negative language should be avoided as this may prejudice the impression of the objectivity and / or professionalism of the audit team.
- All drafts should be clearly marked with a version number to prevent readers from receiving a false impression of whether the report represents the audit team's final opinion.
- Reports should provide enough information for a previously uninformed reader to understand what was reviewed and why.
- Reports should identify good practice / be a tool for knowledge sharing among management.
- High level issues should generally be set out first, with supporting explanations afterwards.

Records management

3.43 There is no requirement to retain hard copy documents if the Internal Audit team is confident that there are adequate safeguards over electronic documents, e.g. that data is regularly and effectively backed up.

3.44 You should keep evidence of all key stages of the assignment in line with the National Archive guidelines (i.e. for three years normally or for six years if the assignment relates to fraud or to long term contracts).

3.45 National Archive guidelines can be found at:

http://www.nationalarchives.gov.uk/recordsmanagement/advice/pdf/sched_internal_audit.pdf

Quality assurance

3.46 Quality procedures are the subject of GIAS Standard 10 – Quality assurance and are covered in separate good practice guidance.

Evaluation of audit performance

3.47 Management feedback should be sought after each review and lessons learned should be considered to ensure audit processes continually improve.

Follow up

3.48 In order to have a positive impact on the organisation's risk profile, audit reports must be acted on by management. While action to remedy deficiencies or to improve processes is the responsibility of management, an Internal Audit follow up process should be used to verify that progress has been made to implement agreed actions and to highlight areas where management are not fulfilling their agreed responsibilities.

Follow up process checklist

When defining the Internal Audit team's follow up process you should address the following questions:

- How soon after fieldwork or the final report issue will follow up occur?
- How will management expectations about the depth and timing of follow up be set and managed?
- How will management be notified that follow up work is due?
- How much assurance will be required over the implementation of recommendations of different priorities, e.g. will management self-assessment or detailed testing be required?
- How will the overall results of follow up and any significant exceptions be recorded, agreed with management and reported?
- Who is responsible for overseeing and initiating the follow up process? Who will perform the follow up work?
- Are there any recommendations or types of audit work that will not be followed up?
- What approach will be taken to management requests to extend deadlines or to change action plans?

A

SAMPLE DEFINITIONS OF REPORT OPINIONS AND ISSUE CATEGORIES

Audit assurance or opinion

	Opinion	Definition
Green	Substantial assurance	Appropriate controls are in place and should be effective in mitigating risk to the level of the organisational risk appetite.
Amber	Limited assurance	A system of internal control is in place that is satisfactory in part, but which contains a number of weaknesses that are likely to undermine the achievement of system objectives and leave it vulnerable to material error / abuse or threatening risk above the level of the organisational risk appetite
Red	No assurance	Controls are ineffectively designed and / or are operated ineffectively such that risk is not mitigated to the level of the organisational risk appetite. Significant improvements are required.

Severity of findings categories

Category 1: A weakness where there is a substantial risk of loss, fraud, impropriety, poor value for money, or failure to achieve organisational objectives. Such a risk could lead to an adverse impact on the business and standing of the department and expose the Accounting Officer to criticism. Remedial action must be taken urgently.

Category 2: A weakness in control which, although not fundamental, relates to shortcomings which expose individual business systems to a less immediate level of threatening risk or poor value for money. Such a risk could impact on operational objectives and should be of concern to senior management and requires prompt specific action.

Category 3: Areas that individually have no major impact, but where management would benefit from improved controls and/or have the

opportunity to achieve greater effectiveness and/or efficiency. Potential for undesirable effects at the process level, which combined with other weaknesses could give cause for concern and require specific remedial action.

B

GLOSSARY OF KEY TERMS

Accounting Officer	A person appointed by the Treasury or designated by a department to be accountable for the operations of an organisation and the preparation of its accounts. The appointee is, by convention, usually the Head of a department or other organisation or the Chief Executive of a non-departmental public body (NDPB).
Audit objective	Specific objective of the particular assignment or generic, underlying objectives of the internal audit team.
Audit plan	List of planned audit assignments for a set period, prioritised according to the organisational risk profile.
Audit risk	Risk to the audit's specific objectives and / or to generic, underlying audit objectives.
Assignment	Piece of audit work from planning through to reporting that is designed to produce a specific deliverable or opinion.
Compliance testing	Tests to evaluate application of controls (i.e. are controls complied with?)
Computer Assisted Audit Techniques	Software utilised in testing IT controls or in performing high volume substantive audit testing.
Exception	Instance of a poorly designed or ineffectively operated control, of an error or of an inappropriate transaction.
Head of Internal Audit	The organisation's most senior member of internal audit with responsibility for providing an annual opinion on 'risk management, governance and control'.
Resource	Costs, often driven by staff or management time (in this document).
Risk appetite	Level of unmitigated risk that an organisation is prepared to accept. The risk appetite may be documented statements about the level of different types of risk considered acceptable and may include a financial value. If the risk appetite is not formally defined, you should use your judgement to determine it, based on discussions with management and on your understanding of the business.

Risk-based audit	Audits that direct resource towards controls over the risks with the highest probability of the highest impact on the organisation.
Risk-based approach	auditAn approach to audits that includes explicit early consideration and ongoing management of audit risks. Examples of appropriate risk management actions include quality assurance and approvals as well as actions specific to the particular assignment being undertaken.
Scope document	Document used for planning audit work and for communicating those plans to management.
Sponsor	Named member of management with sufficient authority for the area under review to take responsibility for resolving issues of debate and for agreeing audit findings.
Substantive testing	Tests of actual transactions, usually done when control compliance is poor, in order to evaluate the extent of loss or damage.
Testing	Obtaining objective evidence as a basis for your opinions.
Walkthrough testing	Tracing a transaction through a process in order to understand the process and the design of controls.