Appendix 1 Detailed Internal Audit Strategic Planning Process

AUDIT RISK ASSESSMENT AND PLANNING

Introduction

The objective of this paper is to explain the assessment criteria and methodology employed in formulating an Audit Risk Assessment and how this is used to produce strategic and operational plans that allow us to conclude on the overall systems of internal control within the Annual Internal Audit Report. The requirement for the Chief Internal Auditor to provide a clear statement of assurance on the adequacy and effectiveness of internal control in the Annual Audit Report provides a clear focus for the audit plan. To plan for such an assurance it is therefore necessary to consider the whole internal control system and the magnitude and incidence of the risks, which the control system is designed to mitigate.

The audit risk assessment is an essential part of the audit planning process used to ensure there is a proper link between the level of risk associated with a particular area and its relative priority within the strategic audit plan.

Internal control

As Accountable Officer, the Chief Executive is responsible for reviewing the adequacy and effectiveness of the system of internal control. At a minimum, this review should comprise an assessment of the overall effectiveness of governance, risk management and internal control arrangements and four specific strands of governance:

- Clinical Governance
- Staff Governance
- Financial Governance
- Information Assurance.

Whilst focused on specific elements, these strands of governance are not mutually exclusive and should be linked through an integrated risk management and internal control framework which should incorporate the following guidance:

- Scottish Public Finance Manual (SPFM);
- Accountable Officer Memorandum;
- Good Governance Standard for Public Services;
- Staff Governance Standard and Self-Assessment Audit Tool;
- Standards for Clinical Governance, Risk Management and the NHSScotland Quality Strategy;
- Information Assurance Standards;
- Scottish Government Audit Committee Handbook.

Audit Planning Methodology

For optimum effectiveness, internal audit should operate in partnership with the client health organisation. Securing joint ownership of the internal audit plan is a key ingredient of such a partnership and therefore a common understanding should exist between the Audit Committee, Management and Internal Audit, of the audit risk assessment process as a basis for informing the Strategic Internal Audit Plan and for the appropriate use of credible external review evidence.

Appendix 1 Detailed Internal Audit Strategic Planning Process

The overall planning process is set out below:

STAKEHOLDERS

Step 1 Identification of auditable areas (The Audit Universe)	Identify all the functions, activities, systems and processes within the operation of the organisation
Step 2 Review of Risk Register	Review of risk register to ensure complete Audit Universe, inform control risk & highlight potential gaps
Step 3 Assessment of Materiality	Management score auditable areas through assessment of corporate importance and corporate sensitivity.
Step 4 Assessment of Inherent and Control Risk	FTF score inherent risk annually Score Control risk based on previous audit knowledge
Step 5 Calculate Audit Risk Index	Assign scores based on materiality and risk and prioritise audits accordingly
Step 6 Update Strategic Plan	Formulate the strategic audit plan within the planning constraint of the agreed number of audit days per year
Step 7 Produce and Scope Operational Plan	Produce the operational plan relevant to year in strategic plan including any adjustments to the strategic plan
Step 8 Determine Areas for departmental review	Senior Management determine areas in accordance with agreed principles (Appendix 2)
Step 9 Review and Approval	Audit Committee approves the Audit Plan

RISK REGISTER

Appendix 1 Detailed Internal Audit Strategic Planning Process

The Audit Universe

The Audit Universe simply collates the Board's the functions, activities, systems and processes grouped by governance requirements, strategic objectives and key control systems. This list of auditable areas is updated annually and mapped to the clients own corporate objectives, heat targets and risk register.

Relationship with client's Risk Management processes

Prior to scoring process, the Regional Audit Manager (RAM) reviews the clients Risk Register to:

- ensure that the Audit Universe is complete for their organisation;
- inform their view of control risk;
- highlight potential gaps in the risk register.

Assessment categories

The model takes account of four assessment categories to produce a risk index for each auditable area, which are fully defined in assessment criteria based on the HIS Risk Assessment Matrix. The auditable area is scored on a sliding scale in each category using assessment criteria to gauge the degree of risk or materiality associated with the particular area. The table below summarises the four assessment categories and what each is intended to measure.

	Assessment category	**Measure**
A.	Corporate Importance	Corporate consequence
B.	Corporate Sensitivity	Political consequence
C.	Inherent Risk	Inherent likelihood
D.	Control Risk	Control effectiveness

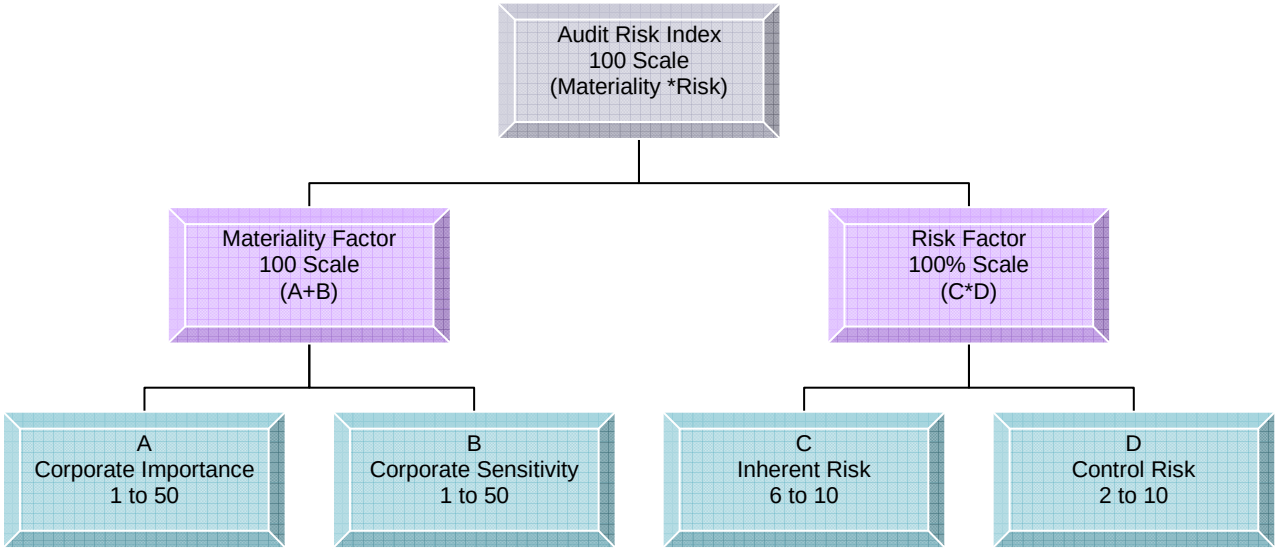
Assessment process

Corporate Importance and Sensitivity criteria are issued to the Director of Finance who scores them in consultation with other Directors and the Chief Executive. Where possible the Directors are asked to provide information on recent, current and forthcoming external reviews of the auditable areas.

Inherent risk is consistent across FTF and updated annually by the FTF Management Team.

Control risk is based upon previous audit knowledge and known developments in the management control environment, including the relevant areas of the organisation's own Risk Register and key external reviews e.g. External Audit & HIS.

The Audit risk index is calculated as follows



Cyclical coverage determined by Risk Index

The risk assessment which ranks the relative risks of the organisation's activities and systems is then used to determine the audit coverage of each system within the five year strategic audit plan. The scores are banded into natural grouping based on the pareto principle so that the top 20% of scores are ranked as high risk with the next 40% shown as medium and the final 40% as low.

In this way, the risk assessment process determines the frequency with which systems are to be audited in the 5 year strategic planning cycle; in general high priority areas are audited 3 times, medium priority areas twice and low priority areas once. When considering the timing of reviews in detail, coverage by External Audit and other formal review processes (management or external) is taken into account as well as client views on when Internal Audit work is likely to add most value.

Items outside of the Risk Assessment process

An allocation of internal audit resources is reserved within each year of the strategic audit plan for audit management, planning, reporting (including annual and interim reviews) and follow-up, and Audit Committee preparation and attendance.

In addition we are required to undertake Post-Transaction Monitoring every year and, Internal Audit may undertake work which will reduce External Audit input in areas such as Endowment Funds and Patients Funds.

Areas subject to external review

Many auditable areas, will be subject to external review. It is the duty of the auditor to ensure that audit effort does not duplicate work already undertaken. Therefore, where credible work has been undertaken, Internal Audit activity will be confined one or more of the following areas:

- Confirming the scope and quality of the work undertaken;

- Ensuring that the review has been reported properly within the organisation and appropriate action taken where required including updating of the risk register where necessary;
- Ascertaining whether there are any issues which require highlighting to the Audit Committee and/or inclusion within the annual report;
- Updating the audit risk assessment for the area in question;
- At client request, assisting in preparing for a forthcoming review or in implementation of the action plan;
- Where an external body requires the client to have internal audit review of the area e.g. infection control.

Allocation of resources

The strategic audit plan is formulated from the audit risk assessment within the planning constraint of the agreed number of audit days per year. The quantum of resource required for an area is not a function of the risk index. The risk index only indicates the frequency of audit attention that is appropriate. Professional judgement is therefore required in allocating necessary resources to each auditable area and in doing so opportunities will be found for identifying audit themes where a number of related auditable areas could be addressed within the scope of a particular audit assignment.

The approach will involve the targeting of the high and then medium priority areas to provide a balanced cyclical cover for the period of the plan before considering the low priority items.

It is possible be that some low risk areas cannot be visited at all during the strategic cycle due to resource constraints. These will be identified to the Audit Committee and Accountable Officer with a clear explanation of the impact on the Governance Statement.

The audit plan reflects the need for continuous improvement by showing reductions in days allocated to audit process as well as demonstrating efficiencies where stable systems are re-visited and in areas subject to ongoing review, wherever possible.

Relationship between strategic and operational planning

A full strategic plan and Audit Universe update is produced once every 5 years or following a major NHS re-structuring that renders previous strategic plans obsolete. The first year's operational plan is simply Year 1 of the approved strategic plan, detailing the expected scopes of the reviews, in consultation with the focus lead and highlighting where the audit is expected to add value.

In subsequent years the strategic plan is revisited by updating scores e.g. revised control risks based on actual audits, updated Director of Finance scores and changes to inherent risks. The operational plan will then be based on the respective year of the approved strategic plan, adjusted for any significant changes arising from revisiting the strategic plan and any in-year amendments to prior operational plans.

Generic scopes are available for each auditable area but these will be adjusted in the first instance by areas highlighted within the Board's Risk Register and through discussions with management. More detailed consideration of the control environment, risks and objectives is undertaken within the detailed assignment planning at the start of each audit.

Appendix 1 Detailed Internal Audit Strategic Planning Process

Departmental Reviews

Time is set aside for Departmental reviews, which consider an area holistically across a range of defined elements of the audit universe. The departments/wards/areas are determined by senior management in accordance with an agreed set of principles (see Appendix 3).

Cross-cutting themes

The process for considering the exact scope of each audit includes a number of cross-cutting themes which are considered for every audit including:

- Performance Management;
- Data quality;
- Communication and engagement;
- Waste, variation and harm;
- Risk;
- Equality and diversity;
- Quality of Care;
- Health of the population;
- Compliance with regulations, policies and procedures;
- Best value;
- Stock Management;
- Values and whistleblowing.

Review and approval

The first draft plan produced by the RAM is discussed with the Chief Internal Auditor before being issued to the Director of Finance and where required, further discussion with the External Auditor shall take place.

Once agreed with the Director of Finance the plan should be presented to the Audit Committee for approval. Any significant subsequent amendment to the approved plan must be notified to the Audit Committee and wherever practicable, be approved in advance.

Post approval meetings

Discussions are held with key directors, collectively and individually as soon as possible in order to:

- maximise efficiency;
- ensure the purpose and scope of the audits is understood;
- agree timings;
- agree which areas will be selected for departmental reviews.

Once approved the draft plan will be circulated to all relevant Directors/senior managers to allow for appropriate discussion, identification of external reviews, key risks etc, with approval of the plan being given by the Director of Finance.

Annex A
Public Sector Internal Audit Standards

2010 Planning

The chief audit executive must establish risk-based plans to determine the priorities of the internal audit activity, consistent with the organisation's goals.

Interpretation:

The chief audit executive is responsible for developing a risk-based plan. The chief audit executive takes into account the organisation's risk management framework, including using risk appetite levels set by management for the different activities or parts of the organisation. If a framework does not exist, the chief audit executive uses his/her own judgment of risks after consideration of input from senior management and the board. The chief audit executive must review and adjust the plan, as necessary, in response to changes in the organisation's business, risks, operations, programs, systems, and controls.

Public sector requirement

The risk-based plan must take into account the requirement to produce an annual internal audit opinion and the assurance framework. It must incorporate or be linked to a strategic or high-level statement of how the internal audit service will be delivered and developed in accordance with the internal audit charter and how it links to the organisational objectives and priorities.

2030 Resource Management

The chief audit executive must ensure that internal audit resources are appropriate, sufficient and effectively deployed to achieve the approved plan.

Interpretation:

Appropriate refers to the mix of knowledge, skills and other competencies needed to perform the plan. Sufficient refers to the quantity of resources needed to accomplish the plan. Resources are effectively deployed when they are used in a way that optimises the achievement of the approved plan.

Public sector requirement

The risk-based plan must explain how internal audit's resource requirements have been assessed.

Where the chief audit executive believes that the level of agreed resources will impact adversely on the provision of the annual internal audit opinion, the consequences must be brought to the attention of the board.

2050 Coordination

The chief audit executive should share information and coordinate activities with other internal and external providers of assurance and consulting services to ensure proper coverage and minimise duplication of efforts.

Public sector requirement

The chief audit executive must include in the risk-based plan the approach to using other sources of assurance and any work required to place reliance upon those other sources.

Appendix 1 Detailed Internal Audit Strategic Planning Process

Public sector definition: Assurance Framework

This is the primary tool used by a board to ensure that it is properly informed on the risks of not meeting its objectives or delivering appropriate outcomes and that it has adequate assurances on the design and operation of the systems in place to mitigate those risks.

Added Value

The internal audit activity adds value to the organisation (and its stakeholders) when it provides objective and relevant assurance, and contributes to the effectiveness and efficiency of governance, risk management and control processes.