

Merseyside Fire and Rescue Service
Internal Audit Plan For The Year 1 April 2010 to 31 March 2011

Background

The 2010/11 audit plan amounts to a total resource of 150 audit days (incorporating a flexible budget of 10 computer audit days). The audit plan reflects internal audit's assessment of the assurance requirements for the Authority and is risk-based. The aim of the plan is to focus on an assessment of the risks to the achievement of the Service's objectives, and the provision of assurance that the actions planned to mitigate these risks are adequate and effective. In deriving this plan we have:

- Considered the Merseyside Fire and Rescue Authority's risk management process;
- Considered the results of previous internal audit work;
- Reviewed all relevant Audit Commission reports;
- Made our own assessment of the risks facing the Merseyside Fire and Rescue Authority.

Deployment of audit resources

The Audit Plan at this stage provides an overview of the key areas. These areas will be refined on the issue of individual job specifications, which will be discussed with the Authority's Executive Director of Resources, and the Director of Finance. At the end of quarter two we will formally review the remaining half of the plan to assess its appropriateness.

The planned deployment of audit resources is as follows:

Proposed work	Estimated audit days
Fundamental systems	40
Supporting finance systems	33
Non-financial systems	40
Contingency	10
Follow up reviews	5
Audit management	12
Computer audit – subcontracted	10
Total audit days	150

Each of these areas is explained in more detail below.

Fundamental systems

Any assessment of Merseyside Fire and Rescue Authority risks generates a requirement to consider the fundamental systems under-pinning their operations, including payroll, creditors, budgetary control, general ledger and treasury management. We will also consider the arrangements in place to ensure reliable medium term financial planning (MTFP).

In undertaking any fundamental systems work we may make use of computer assisted audit techniques to interrogate the systems and the data they hold more effectively.

Supporting financial systems

We have identified income and debtors, stores & inventory/assets, grants and insurance and overall governance for inclusion in the plan as supporting finance systems. We will also consider the arrangements in place around IFRS.

Non-financial systems

We plan to continue to undertake work on partnerships to build on our work in 2009/10 to ensure that the processes and procedures have been fully embedded within the Authority. We are to include in the plan for this year business continuity and fraud risk management. We are also likely to perform further work on the PFI project building on the work performed in 2009/10.

Computer Audit – subcontracted

Appropriate use of the 10 days allocated will be agreed during the year with the Director of ICT.

Contingency

A number of days have been allocated to contingency, including responsive work and advice and assistance.

Follow up reviews

Audit resources have been allocated to ensure that all two star and three star recommendations are followed up within one month for three star recommendations, and within three months for two star recommendations of the agreed implementation date.

Audit management

An allocation of 12 days has also been made to cover other management and tasks in support of the internal audit service to the Authority:

- Strategic Planning;
- Central reporting (annual and periodic progress).
- Liaison with Senior Management; and
- Liaison with the Audit Commission;

After each assignment we will produce a report which will be sent in draft to the managers who have a direct responsibility for the function being audited and who have the authority to take action on our recommendations and to those others necessary to check factual accuracy. Each report will be discussed with the relevant management and their comments and action plan for addressing recommendations will be included in the final version. Internal Audit will require a formal response within seven days of issuing the draft.

Our reports on each audit will:

- State our overall opinion (see Appendix 1);
- State the conclusions reached;
- Make recommendations which are appropriate and relevant (see Appendix 2); and
- Acknowledge the action taken, or proposed, by management.

OVERALL AUDIT OPINION levels explained

Appendix 1

This audit report contains an opinion on the overall level of assurance that can be given on the internal control environment / systems. It will be one of four levels:

LEVEL	Explanation	Guidance
Substantial	<i>There is a sound system of control and governance in place to achieve the system objectives, controls are being consistently applied and the relevant risks to the Service are well managed.</i>	No recommendations have been made, or 1 star recommendations made that cumulatively do not warrant 'adequate status'.
Adequate	<i>The control environment / systems are operating effectively to ensure that the majority of relevant risks are managed. Slight improvements need to be made in order to provide substantial assurance that all of the objectives of the system are met.</i>	A 2 star recommendation made, or a large number of 1 star recommendations that cumulatively could meet the criteria for a 2 star recommendation.
Limited	<i>Weaknesses and/or non-compliance with procedures are placing system objectives at risk. Heads of Business Units should consider whether they should refer to this assessment in their annual assurance statement on internal controls together with any actions agreed and/or taken to improve the system.</i>	Improvements could be made to a number of areas within the control environment so that the relevant risks are managed more effectively, or a 3-star recommendation made, or several 2-star recommendations that cumulatively could meet the criteria for a high priority action.
Little/None	<i>There are control weaknesses and / or non-compliance with basic controls that are so significant the relevant risks are not being managed at all. The system is open to significant error or abuse. In light of this assessment, Heads of Business Units should review their risk register and refer to this assessment in their annual assurance statement on internal controls together with any actions agreed and / or taken to improve the system.</i>	More than one 3-star recommendation made.

Appendix 2

AUDITOR GUIDANCE ON RECOMMENDATION RATING – Explanation

<u>Essential / Strategic</u> <u>(3 star)</u>	<u>High (2 star)</u>	<u>Operational (1 star)</u>
Absence or failure of <u>fundamental</u> (i.e. no recovery action on arrears, no bank reconciliation, failure to clear significant reconciling items appropriately, no Treasury Management Strategy) where there is no compensating control.	A weakness in <u>fundamental</u> control (i.e. not carried out on time, not authorised). Absence or failure of <u>key</u> controls i.e. orders not authorised, no review of bank reconciliation.	General weakening of the control environment.
Failure or absence of a control which would <u>probably</u> result in a direct risk of serious injury to staff, customers or third parties.	Failure or absence of a control which would <u>possibly</u> result in a direct risk of serious injury to staff, customers or third parties.	Failure or absence of a control which would possibly result in an indirect risk of serious injury. Localised failure of a control which would possibly result in a direct risk of serious injury to staff, customers or third parties.
Any illegal operation. Any failure to comply with regulatory requirements.	Widespread non-compliance with policy.	Localised non-compliance with policy.
	Absence of procedure notes. Absence of clear organisation policy.	Procedure notes not updated.
Any national reputation impact.	Any local reputation impact.	
		Other actions which will improve operational efficiency.