Milton Keynes
City Council

Internal Audit Manual

December 2023

Jacinta Fru – Chief Internal Auditor

Foreword

The purpose of this manual is to provide audit staff with a source of reference for general audit procedures and methodology. We, as professional Internal Auditors need to conform to the *IIA Code of Ethics*, and the *UK Public Sector Internal Audit Standards* (PSIAS).

The service maintains other key documents, for example the Audit Charter, accessible on the IA website.

All auditors must also comply with these processes which are summarised by the PSIAS *Core Principles* as set out below:

- Demonstrates integrity
- Demonstrates competence and due professional care
- Independence – objective / free from undue influence
- Aligns with the strategies, objectives, and risks of the organisation
- Appropriately positioned and adequately resourced.
- Demonstrates quality and continuous improvement
- Communicates effectively
- Provides risk-based assurance
- Insightful, proactive, and future-focused
- Promotes organisational improvement.

The Manual has been drafted to also provide guidance on how these processes are progressed through our audit software, Sword Audit Manager (SAM).

I fully appreciate that some circumstances will not ‘fit’ the processes scripted within this Manual. Professional competence and proactivity within the above principles support my confidence that audit staff will know when the situation requires variation to these processes and where to obtain the necessary Chief Internal Auditor (or in their absence the Audit Manager) approval.

I welcome any suggestions for improvements to this manual.

We have highlighted the key actions audit staff should adopt within the document to aide its use as an operational manual.

Jacinta Fru BA (Hons) FCCA

Chief Internal Auditor

1 Audit Committee

The Audit Committee is responsible for overseeing the Council's risk, controls and governance arrangements and for ensuring the effectiveness of internal and external audit.

The Audit Committee's Terms of Reference can be found here 03. Committee Terms of Reference.pdf (moderngov.co.uk) the Council's website. The service promotes the adoption of the CIPFA best practice Terms of Reference whilst respecting the Council's right to determine this for themselves.

The Audit Committee has a clear role in oversight of Internal Audit. It approves the Charter, Audit Plan, receives updates, monitors key performance indicators and considers high profile matters.

Internal Audit has direct access to the Audit Committee Chair should matters of a serious nature arise. During the year, the Chief Internal Auditor (and/or Audit Manager) will meet with the Chairman of the Audit Committee on an informal basis.

The Chief Internal Auditor (and/or Audit Manager) presents the IA team's progress report to the Audit Committee on a quarterly basis (see Section 3 – Performance Measures).

Auditors should be aware of this KEY stakeholder and their role to ensure every assignment enables the Audit Committee to properly discharge its functions.

OUTCOMES/ASSURANCE:

The IA service provides the Audit Committee (and senior management) with the following outcomes/assurances:

- **Internal controls -** Ensure the integrity and reliability of the Council's financial and operating information, quality of performance management, safeguarding of assets, and the economic, effective and efficient use of resources, and compliance with external regulations, legislation, internal policies and procedures.
- **Risk Management** – Assurances that key risks for the Council's objectives are being managed.
- **Governance** – Audit reports contribute to improvements in control and governance processes.

2 Internal Audit Charter

The Charter is a formal document that defines our vision, purpose and how the service will be provided. It is reviewed and approved annually by the Corporate Leadership Team and Audit Committee.

The 'Internal Audit Charter' is available on the IA website or via the Chief internal Auditor.

Each member of the IA team is expected to be aware of the Charter and adhere to it.

3 Performance Measures (and Sword Audit Manager)

Performance measures[1] are monitored by the Chief Internal Auditor, reviewed at IA team meetings and reported quarterly to the S151 Officer and Audit Committee. This data is derived from our audit software, Sword Audit Manager (SAM) and it is essential that information is kept up to date.

[1] PSIAS ref 2000 Managing the Internal Audit Activity

Auditors must ensure time recording and audit progress is kept up to date and properly recorded into SAM. Whilst measures are reported monthly auditors should update this data at least weekly.

Performance Measures include:

Proportion of Plan completed and work in progress

(100% target to Draft by 31/3)

Proportion of agreed actions implemented

(100% target of Essential Recs implemented)

Weak/Limited opinion reports

(detail of each to be reported)

Productive/direct time as a % of total time

(90% Target)

Proportion of Weak/Limited opinion reports to improve to at least 'satisfactory' at follow up (100% target)

Customer satisfaction levels

(90% good feedback target)

The service also needs to manage the progress and quality of individual audit assignments.

Auditors need to ensure the Chief Internal Audit/Audit Manager has:
- approved the Terms of Reference
- is made aware of any significant finding identified during the audit
- has quality assured the work before issuing the report

The completion of every audit is monitored against:

End to end time

Days taken to complete (compared to planned time)

Time between key audit stages e.g. draft issue to final report issue

Customer satisfation

4 Annual Audit Plan

Whilst an Annual Audit Plan is developed (and approved) it is an indicative and flexible plan of work to reflect the assessed risks and key systems across the Council[2].

The plan is developed in consultation with key internal and external stakeholders with the aim of a 1st draft plan being submitted to Corporate Leadership Team in January for comment / initial approval and then Audit Committee approval before 31st March each year.

The development of the plan includes:

- Risk assessment of areas and thus their comparative risks
- Timing of the audits with a commencement QUARTER proposed to align with seasonal / other service pressures.

The risk assessment methodology determines priorities for audit coverage based as far as possible on management's view of risk in conjunction with other internal sources such as the corporate risk register, audit risk scores etc. External assurances sources are also used including:

[2] PSIAS ref 21010 Planning

- External audit reports (both local and national)
- Local Government Ombudsman reports (individual and annual)
- Office of the Surveillance Commissioner
- Information Commissioner
- Professional best practice e.g. IIA, CIPFA etc
- National Anti-Fraud Network

The Plan is approved annually by the Corporate Leadership Team and Audit Committee (preferably before the start of each financial year).

The Plan remains flexible and may change during the year as risks are re-assessed and new issues emerge.

Auditors should highlight any emerging risk they become aware of to include within the Audit Plan

Audits are allocated regularly by the Chief Internal Auditor/ Audit Manager.

The Audit Manager will allocate new audits to auditors; auditors must manage their workloads and request additional audits in advance to avoid any dips in productivity.

Auditors are responsible for discussing the time allocation for each assignment with the Audit manager and completing the work within the time allocated. If you feel that the time allocated is not sufficient for the service under review, please discuss this with the Chief Internal Auditor/ Audit Manager.

Auditors must flag up any audit likely to exceed its allocated days at the earliest opportunity, at the same time proposing any opportunities to mitigate such overspend.

Target completion stages are managed by the monitoring of progress target and actual dates on SAM, therefore it is important to maintain these on an ongoing basis.

5 Audit Methodology

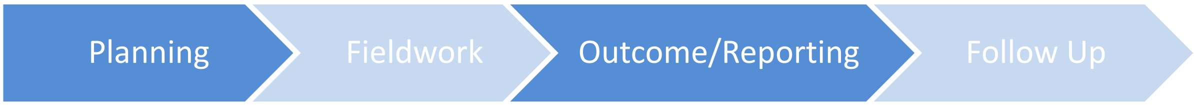
The role of and authorisation for Internal Audit is derived from the Accounts and Audit Regulations, Local Government Act and the Public Sector Internal Audit Standards (PSIAS). The Council also provides unfettered access to records for the Section, to enable it to define and perform its duties via an approved Charter, Annual Plan, Financial Regulations, etc. This authorisation allows Internal Audit full, free and unrestricted access to all functions, records, assets, property and personnel necessary for the proper discharge of its responsibilities. No operational area or levels within the organisation are excluded from Internal Audit review.

Auditors should approach any reluctance to provide documentation or information tactfully. It is likely that reluctance may be because the information is sensitive / confidential. If following a tactful explanation of the reasons and basis for requesting that information it is still refused, the Auditor should seek to discuss the matter with senior management and if that fails, highlight the issue promptly to Audit Management.

If at any time matters are uncovered or brought to your attention that are of significance to management, or if you believe that the resulting exposure is serious, Audit management should be informed promptly.

The Audit Process

The process of performing an audit has four key stages. These are collectively referred to as the Audit Cycle as shown below:



Planning → Fieldwork → Outcome/Reporting → Follow Up

5.1 *Planning*[3]

Audits will be allocated by the Chief Internal Auditor/ Audit Manager from the Annual Plan. Assigning auditors to an audit within SAM enables time to be coded to that audit within SAM.

In this phase, the system or operation to be audited is reviewed and documented (i.e. flow chart or detailed systems notes, identifying controls and any gaps/risks), risks and controls identified, and a preliminary evaluation undertaken of the adequacy of these controls.

The Terms of Reference (ToR) document is an important stage as it sets out for client agreement, what we will audit. The ToR summaries the scope of the audit, detailing the objectives to be used in developing the audit programme, and is agreed with the Chief Internal Auditor/ Audit Manager and the client /sponsor.

PSIAS compliance requires a consistent format for the ToR that ensures key considerations are always assessed (for example risk of Fraud)[4]. An approved ToR template is saved in within folder ref B in Standard Docs on the SharePoint folder.

The agreed ToR should be saved into the SharePoint 'Audit Management docs' folder. Evidence of the Chief Internal Auditor (or Audit Manager) and client's agreement should be saved in the 'Correspondence' folder.

Planning Steps:

1.01	Input '**Activity Planned**' date on SAM, if not already inserted
1.02	Complete the Assignment Declaration of Interest form in SharePoint and send to manager for counter signature for every audit[5]. **Note:** If during the audit you become aware that there is a conflict of interests, you must complete, sign, resubmit and file the form again.
1.03	Contact Auditee (Head of Service) and arrange commencement meeting
1.04	Research (consider key risks - review GRACE, recent legislation, service changes, previous audit file including process flow, etc.) including whether a previous audit folder already contains a past ToR that can be used / updated.
1.05	Create the draft ToR using the MS Word template for Chief Internal Auditor/Audit Manager and Client agreement
1.06	Commencement Meeting (to agree ToR with Client)
1.07	Finalise and issue Terms of Reference - obtain management approval prior to this).

[3] PSIAS Ref 2200 Engagement Planning

[4] PSIAS ref 2210 Engagement Objectives and 2220 Engagement Scope

[5] PSIAS ref Impairment or Independence to Objectivity

1.08	Complete target ('planned') completion dates for each of the key stages of the audit in the SAM Progress control screen (ToR refers to key stages) Note: 'Revised' dates should not normally be inserted

Planning Outputs:

A	Auditor to ensure a fully completed and countersigned Declaration of Interests form is received and is uploaded on Sharepoint (Correspondance folder**)**
B	Research documents/notes (saved in SharePoint Background Docs folder)
C	Commencement Meeting notes (saved in SharePoint Correspondences folder)
D	Agreed ToR (saved in Sharepoint Audit Management docs folder) and upload to SAM
E	Chief Internal Auditor/Audit Manager and clients' agreement of ToR (filed in Sharepoint Correspondences folder)
F	Email ToR to auditee (saved in SharePoint Correspondences folder)
G	Input '**ToR Issued**' date on SAM
H	Process Flow including walk through test (saved in SharePoint System Notes folder)
I	Identify objectives, risks and controls and develop a draft test programme/control matrices[6]

5.2 Fieldwork

During the fieldwork phase, the test programme is followed and assessments made based upon the results of further investigation and testing.

Auditors should only contact Directors at the start (email issuing Terms of Reference) and conclusion of an audit (email issuing Final report). It is not appropriate to contact directors regarding operational matters. If you think contact is necessary during your audit please clear this with the Audit Manager beforehand.

Testing methodology for audit testing is to be determined by the auditor undertaking the audit (depending on size and value of transactions.

Fieldwork Steps:

2.01	Opening Meetings (if required)– to obtain better understanding of systems and controls in place. Meeting notes to be made and saved on SharePoint folder.
2.02	Create a Risk Matrix working paper for each audit objective within SAM. Populate objectives, risks, controls, tests fields. This forms the test programme.
2.03	Review of test programme (by Chief Internal Auditor/ Audit Manager – for Senior or Associate Auditor as necessary)
2.04	Commence testing and input SAM progress control date ('**Fieldwork Started**' date)

[6] PSIAS ref 2240 Engagement Work Programme

2.05	On completion of fieldwork, input SAM progress control date (‘**Fieldwork Completed**’ date) and ensure that all relevant support working papers are attached on SAM and cross referenced to working papers.
2.06	Arrange an exit meeting with the auditee to discuss findings/ issues found and initial proposed recommendations. Notify the auditee that the findings will be subject to a quality review and recommendations may change.
2.07	Use SAM report screen to create report. Generate Word Document (see below 5.3.2) The details on report from SAM is used to populate the New Template Report within Standard Docs.
2.08	Working papers and draft audit report will be reviewed by Audit Manager[7] using SAM review function or Review Sheet on Sharepoint
2.09	Input ‘**Manager Review**’ progress date on SAM and clear all review points.
2.10	Input SAM progress control date (‘**Clearance/Review Meeting Held**’)
2.11	Email the agreed draft audit report to Chief Internal Auditor for review (there is no provision in progress dates for this stage to be input).
2.13	Discuss any report amendments if necessary
2.14	Issue draft report to auditee as per the distribution list – Draft Reports to be issued to Heads of Service and above
2.15	Input SAM ‘**Final Draft Report issued**’ date on SAM

Fieldwork Outputs:

A	Meeting notes
B	Completed control matrix and working paper reviews (Audit Manager)
C	Cross referenced working papers (incl tests spreadsheet)
D	SAM generated report
E	Clearance/Review meeting notes (if undertaken)
E	Fully reviewed audit report (by both Audit Manager and Chief Internal Auditor)
F	Email issuing draft report to auditees (file in Correspondence folder)

Further Guidance:

This section will include the bulk of the working papers and will be prepared while the test programme is being executed. The contents of this section will vary greatly from one audit to another; however, in general terms it should record the full detailed results of the audit.

Auditors must ensure this aspect of the work is fully documented and saved. This is a KEY stage of work to demonstrate PSAIS compliance[8] and specifically the important principle of professional competency and quality assurance processes. SAM has been designed to save all working papers within each audit / assignment and it is vital (to demonstrate PSIAS required quality assurance and consistency) that this used fully.

[7] PSIAS ref 2340 Engagement Supervision

[8] PSIAs ref 2300 Performing the Engagement

It is also ESSENTIAL that Auditors communicate regularly and effectively with the auditee to minimise the possibility of "surprises" at the end of the audit. This may be done informally (for example by emails, discussions) or via formal meetings but must be evidenced and proactive.

5.3 Outcome Reporting

5.3.1 Final Audit Reports

Internal Audit is, by its nature a logical, evidential profession which requires clear and concise reports that contain evidenced and objective findings to support an independent audit opinion[9]. The Audit Opinion within every report must provide service management with a view regarding the adequacy of assurance in relation to:

- Control systems
- Compliance
- Organisational Impact

To achieve the above objective audits must consider (and maintain the evidence that supports) an opinion on the:

- adherence to external regulations, legislation, internal policies and procedures, for each area audited / examined;
- financial and operating information, quality of performance management, safeguarding of assets, and the economic, effective and efficient use of resources;
- the effective identification and management of significant risks.

The service has a standard, consistent report template to be used across all services, that provides the basis to demonstrate PSIAS compliance. The template should only be varied in exceptional circumstances and in agreement with the Chief Internal Auditor. It is not for auditees to change audit reports unless there are factual inaccuracies.

At the exit meeting, auditors should ensure that auditees accept the issues raised and either agree the improvement actions suggested by Audit or provide alternative actions that will address the issue raised. Alternative management actions should be noted as such within the "recommendations box" in the report template. No target date or follow up will be needed except where an alternative action is proposed.

Audit Report Steps:

3.01	Agree any changes in report due to factual inaccuracies. Consider reporting changes back to the Audit Manager and/or Chief Internal Auditor unless these are minor. Where necessary, update SAM ensuring all actions (recommendations) are accurately entered.
3.02	Issue audit report to auditees (as per Terms of Reference) and send a copy to Audit Manager to request a customer satisfaction survey is issued.
3.03	Input SAM progress date ('**Final Report Issued**' date)
3.04	Ensure the 'actions' accurately reflect the recommendations in your report.

[9] PSIAs ref 2400 Communicating Results

3.05	Ensure 'Final issued' dates are entered in the 'Progress' tab on SAM for each action (this enables management reporting on the implementation of actions) Ensure management actions on SAM are updated after issue of final report
3.06	Copy of Final Report to be placed in Reports folder within Sharepoint and copy to be uploaded to SAM (Attachments tab, found alongside Progress Control tab).
3.07	Email issuing report to be attached to SAM audit activity ('Attachments' tab alongside 'Progress' dates tab) and to be filed in Correspondence tab on Sharepoint.
3.08	'Survey Issued' date is entered on SAM

Audit Report Outcomes:

A	Final reports should be copied into relevant folders
B	Customer Survey issued (file and record for performance management purposes)
C	Completed Customer Satisfaction Survey.

Timelines:

Report Stage	Timescale
Draft findings – send to exit meeting attendees	2 days prior to meeting
Draft report – send to auditees (management) to gain final agreement	2 days post exit meeting
Final draft report – for review/comment by auditees	5 working days
Final report (taking any further final comments into account)	2 working days

Further Guidance:

Audit Reports:

Timing: Audit reports should be issued at the time stated within the Terms of Reference. Any delays should be reported promptly to the Chief Internal Auditor/ Audit Manager.

Audit Report Opinion: There are no hard and fast rules for determining the Audit Report Opinion, however, the risk rating of the audit findings will naturally help determine the final outcome e.g. the presence of one or two 'essential' risks may be sufficient to grade an audit 'Limited'.

Recipients: All final Reports should be sent to the Director as audit sponsor. Please see Final Reports Process guide.

Target Implementation Dates: Target dates should where possible not exceed 6months from date of issue of the Report, unless the action is strategic and is obviously longer term.

‘**Limited’ and ‘Weak’ assurance opinions**: Please notify Chief Internal Auditor/Audit Manager at draft stage so they can feed concerns upwards. Directors should always be copied into the email issuing the draft report.

Management Reporting: The status of each report is summarised in reports to management and Audit Committee. Report findings are not included unless the opinion is Limited in which case the essential/important recs are summarised in the Progress update to management and Audit Committee.

Audit Reports are NOT exempt under Freedom of Information. Discussions must take place in a timely manner regarding wording that should be redacted (the service must be involved in this discussion).

5.4 Follow up

Follow ups are an important step that provides assurance to management that the agreed actions have been completed and thus the control environment has been improved as agreed[10].

It is essential that recommendations / actions are followed up for implementation and reported. The Audit Service is required to monitor (via a quarterly Action Tracker process) audit recommendations and report that information to senior management and the Audit Committee.

It is the responsibility of the Chief Internal Auditor/ Audit Manager to ensure all audits are followed up as necessary usually within 3-6 months after the issue of the final report.

A follow up process has been agreed with CLT, for the Senior Executive Assistants(SEA) to follow up implementation of Audit Recs as part of the corporate action tracker process.

All SEA have access via a SharePoint link to an audit “Composite Tracker”, which is maintained by the Counter Fraud Analyst. They are required to request progress updates from managers within their respective directorate.

A copy of all final reports should be sent to the CF Analyst, to enable update of the composite tracker.

On a monthly basis, the Chief Internal Auditor (CIA) will review the Composite Tracker for any recommendations noted as implemented. The CIA will forward all implemented recs to the relevant auditor, to obtain evidence.

Evidence must be obtained for ‘essential’ actions that are reported by auditees as implemented. For ‘important’ actions this is preferable, but not a must. Where possible, evidence of implementation should be obtained independently.

There is no need to request evidence of ‘standard’ actions.

SAM will be updated with implemented recs closed, by the CF analyst based on the Composite Tracker. Where the Auditor confirms that there is no evidence of implementation, SAM will be amended as well as the Tracker, with a new progress update.

[10] PSIAS ref 2500 Monitoring Progress

Follow-up Steps:

4.01	Counter Fraud Analyst is sent a copy of the final Report and Essential (E) and Important (I) issues and recommendations are entered on the composite Tracker.
4.02	Counter Fraud Analyst enters 'Progress' dates ('Action Completed') on SAM for each Action. Or revise target dates ('Action Summary' – 'Revised Target Date') where necessary.
4.03	On a monthly basis, the Chief Internal Auditor reviews Tracker and notifies relevant auditor of any recs that are noted as completed, by the Senior Executive Assistant (SEA)
4.04	For essential and Important recs, the auditor should obtain evidence of implementation. Where possible evidence should be obtained independent of the relevant Manager. Evidence gathering should be a quick process, not a second audit.
4.05	Update Risk Assessment

Follow-up Outcomes:

The Chief Internal Auditor/ Audit Manager will monitor 'not implemented' actions on an ongoing basis. However, where the Auditor feels that progress is not as expected, or that the risks warrant it, the Chief Internal Auditor/ Audit Manager should be advised.

Unacceptable risks such as those risks accepted by management but the auditor feels this a threat to the service/organisation must be reported to the Chief Internal Auditor/ Audit Manager who will escalate the issue(s).[11]

Other Audit Work

Internal Audit on occasion may deliver other work for its clients. Compliant with PSIAS this section outlines how the independence of IA is protected.

Grant Certification

Government Grants may require Internal Audit certification that monies have been spent on approved purposes and grant conditions fully met. A schedule of known grants is maintained and diarised within the Annual Audit Plan.

As with audits, this area of work will be allocated at the appropriate times by Chief Internal Auditor/Audit Manager.

Where Internal Audit is advised of a grant received, the grant manager will be advised of the need to ensure that relevant proof of spend and adherence to grant conditions is collated ready for audit. Internal Audit will contact the grant manager to obtain the evidence, with the aim of completing the audit in advance of the deadlines per the grant conditions.

[11] PSIAS ref 2600 Communicating the Acceptance of Risks

Upon completion a certification or declaration letter will be prepared by the auditor, a briefing note or audit report and key supporting evidence shall be provided to the Chief Internal Auditor for quality assurance and signature.

Where the Chief Executive is required to sign the grant declaration letter, a verification pack containing:

- the declaration letter signed by the Chief Internal Auditor,
- the Report summarising verification work done and
- the grant letter from the Government Department detailing the grant condition

will be forwarded to the Chief Executive's SEA.

The signed letter should be emailed to the relevant recipient per the grant letter and a request made for confirmation of receipt by return email, as evidence of submission. This should be filed on the grants folder.

Operational / Adhoc roles:

This will rarely be ongoing service delivery but where such work is delivered via IA

- The Chief Internal Auditor/ Audit Manager shall approve such work if they are assured it has no impact on the completion of the approved Audit Plan. The Audit Manager shall advise the Chief Internal Auditor of all such work approved.
- Chief Internal Auditor shall be the only person authorised to agree such work if it is considered it may impact on completion of approved Audit Plan.
- Any audit of that area will require auditing by a sufficiently independent person[12].

IA may undertake other, non-Audit assignments such as participation in (but not a member of) Project teams eg IT systems.

Currently two operational matters are delivered via Internal Audit

(1) Risk Management
Internal Audit facilitates MKCC management of risk, which is led by the director of Finance and Resources. This is done through six monthly workshops where risks owners are challenged as to the contents of the registers. Risk registers are reviewed on a quarterly basis by Internal audit, to assess adequacy of mitigating controls and progress on implementation of mitigating actions noted on the registers. Findings from these reviews are reported to Audit committee. Steps are taken to ensure that Internal Audit Independence is not compromised as much as possible.

(2) Counter Fraud
Although managed by the CIA and Audit Manager, the Counter Fraud service is delivered by a team that is not involved with delivery of internal audits. This minimises the possibility of conflict of interest to IA independence. This is therefore recognised and managed in agreement with the S151 Officer.

Consultancy:

Before undertaking work you will need to agree:

- Chief Internal Auditor approval including detailed Scope of Assignment
- Timing & Key Deliverables
- How potential independence issues will be managed / highlighted

[12] PSIAS ref 1100 Independence and Objectivity

The scope of such assignments must document any potential implications to the IA services' independence. Consultancy assignments must be created as an Audit within SAM and managed consistent with those PSIAS processes structured through SAM.

It is essential that the outcome (ie a formal report, advisory note or other) and its circulation is agreed in advance with the senior client.

Auditors must ensure they have due regard to any conflict of interest (either personal or for the service) and highlight these at the earliest opportunity.

Non-Fraud Investigations

- Periodically the Chief Internal Auditor will receive referrals for non-fraud related investigations from management, Councillors or via the Whistle-Blowing Policy.

- Auditors will draft the agreed Assessment Terms of Reference, which shall then be submitted to the Chief Internal Auditor for approval, including whether the referral warrants an internal investigation and if it does whether that shall be progressed by Internal Audit or Counter-Fraud staff or referred to another appropriate internal / external party.

- The investigation should be set up as an activity on SAM and time charged to it in the normal way. Draft/Final Reports and working papers can be attached to the activity within SAM.

Fraud Investigations:

- The Internal Audit Service maintains a professional counter-fraud service and operates within the Anti-Fraud and Corruption Policy and response Plan.

- The SAM system is used as the fraud case management system. Every investigation will be created as a specific job within the relevant Client (business unit) and files are limited to Counter-Fraud staff access and Chief Internal Auditor.

Auditors must ensure they have due regard to the potential for fraud within every audit including designing tests that address that risk within systems (e.g. duplicate payment data matching in creditors). Auditors must highlight any suspected fraud promptly to the Chief Internal Auditor.

Periodic reports on caseloads and key cases are reported to Leadership Team and Audit Committee.

Cases are usually investigated by the Senior Counter Fraud Officer, to ensure that appropriate investigative action is taken AND control implications fully understood.

Auditors supporting / undertaking any investigative work must have due regard to their audit independence at all times.

Counter-Fraud itself is not audited on the basis that its work is subject to

- Managerial oversight on every case
- HR oversight on all cases involving staff
- Senior Service Management oversight on key cases
- Corporate leadership Team oversight on key cases
- Statutory Officer oversight on key cases
- Audit Committee oversight on both caseloads *and* key cases