MKI User Policy

AUDIT SCOTLAND

Prepared for MKI Users

Reviewed and updated October 2019

Audit Scotland is a statutory body set up in April 2000 under the Public Finance and Accountability (Scotland) Act 2000. We help the Auditor General for Scotland and the Accounts Commission check that organisations spending public money use it properly, efficiently and effectively**.**

Contents

Introduction

1. MKInsight (MKI) is Audit Scotland's electronic working paper audit management system, also referred to as EWP (electronic working papers). While MKI does not replace performing detailed audit work or diminish the need to for us to demonstrate our professional judgment, it does provide a consistent platform for documenting, reviewing, sharing and reporting our work. To ensure we continue to achieve the improvements and efficiencies in delivering our audits this user policy sets out the expected standards that are to be followed by all staff when using MKI. This document sits alongside the MKI user guides available on SharePoint and within the Document Library on MKI. Compliance with the user policy is mandatory and forms a key element of our professional auditing framework.

Installation and software updates

2. MKI is installed both on citrix profiles and directly onto laptops. There will be periodic updates to MKI software, including full releases of new versions and patches (service packs) to fix small bugs, incorporating improvements to the system. As such, users' MKI profiles will require to be updated to incorporate the latest version of the software. An email will be issued to inform MKI users when the MKI software is to be updated. All MKI users must ensure that they back up all work centrally before the specified software update time. Failure to do so **will lead to the loss of work with no option for recovery.**

3. Updates to MKI citrix profiles will occur automatically and the latest version of the software will be available the next time the user opens the program through citrix. Upgrades to laptops require users to connect to the network in either a fixed audit location or main office following an upgrade - **i.e. users need to connect directly to the Audit Scotland network to ensure the upgrade is working properly on the laptop** (any issues should be reported to DSG). Appropriate arrangements should be made to do this before commencing any further work on MKI.

Audit universe maintenance

4. The audit universe (how MKI is arranged) supports consistency of our audit approach and it has been set up at four levels:
    - Level 1 - audit year
    - Level 2 - client
    - Level 3 - audit activity (risk assessment, grants, financial statements etc.)
    - Level 4 - audit programmes

5. Business Support Services (BSS) are responsible for the maintenance of the structure. No other users have the permission to amend the audit universe.

Role permissions and team membership

6. The EWP team is responsible for the maintenance of the role and team memberships as set out in the user guides and only they have the ability to amend these. Any requests for specific changes can be made by submitting an email request to ewp@audit-scotland.gov.uk.

Documenting audit work

Standard audit programmes

7. The professional support group has developed a range of standard audit programmes covering the work usually undertaken as part of an audit in compliance with our Audit Guide. It is emphasised that these programmes are generic and should be reviewed and tailored to adequately address any risk identified in a particular audited body. The MKI user guides provides details on how to set up and tailor audit programmes.

8. Some clients have unusual account areas / systems not covered by the standard audit programmes. If an audit team feel that the standard programmes cannot reasonably be adapted for their purposes, they should submit an email request to ewp@audit-scotland.gov.uk stating clearly what additional programmes they require. This will be referred to the professional support group for approval prior to inclusion in MKI.

Documentation

9. The Audit Guide sets out the key requirements for documentation of our audits, based on the requirements of ISA 230. This section provides further clarification on the requirements of auditors in terms of evidence maintained on MKI.

10. The audit work module within MKI is where auditors record their audit procedures, audit evidence obtained, and results and conclusions in compliance with the audit guide. Auditors are also able to attach documents (word, excel, PDF, etc) as audit evidence to support the results and conclusions.

11. In documenting and recording audit work within MKI, auditors are required to prepare audit documentation that is sufficient to enable an experienced auditor, having no previous connection with the audit to understand the:
    - nature, timing and extent of audit procedures performed;
    - results of the audit procedures performed, and the audit evidence obtained;
    - significant matters arising during the audit, the conclusions reached, and any significant professional judgments made in reaching those conclusions.

12. Auditors are required to document details of the audit evidence obtained, results, conclusions and any matters arising from their work directly into the appropriate fields within the MKI audit work module. Matters arising should be recorded in a manner that enables them to be fully understood without returning to the detailed work and directly extracted into an audit report without the need for significant editing.

13. The MKI user guides provides further details of how auditors are expected to document audit evidence obtained, results, conclusions and matters arising in MKI. **All final audit evidence must be recorded within MKI.**

14. With respect to attaching documents within MKI as supporting evidence; it is generally sufficient for the details of the work performed and results to record appropriate references / details of the supporting evidence or documentation (and source) to enable another auditor, wishing to re-create or re-perform the audit work, to obtain the same evidence or documentation from the original source. This means that supporting evidence or documentation does not necessarily require to be attached to the audit findings, as long as the details of the work performed and results are sufficiently documented to facilitate re-performance.

15. This is particularly important in respect of scanned documents which require significantly more hard disk space than word and excel documents and will significantly increase the file size and potentially impact on the speed of the system. Only documents essential for the audit should be scanned e.g. documentation when it directly supports a matters arising and is required to provide additional audit evidence.

Example 1

An auditor is substantively testing non-pay expenditure items. To confirm the accuracy of the amounts the auditor prepares an excel spreadsheet of the sample and documents the findings for each sample on the spreadsheet. Evidence reviewed included invoices, orders and contracts. There were two samples items where there were discrepancies between the invoiced amounts and amounts paid.

The overall findings and conclusions are documented in MKI and the excel spreadsheet is attached which includes sufficient details of the samples selected to enable another auditor to obtain the source documentation from the client if so desired, or, reperform the test. None of the supporting documentation such as invoices etc. is scanned and attached to the audit file apart from the two invoices with errors. These should be scanned and recorded as attachments as they provide audit evidence.

16. Auditors are required to consider when attaching documents into MKI whether it is necessary and consider:
    - Is a reference to the document and its source sufficient?
    - Does the document add value to the audit evidence?
    - If the document is required can it be obtained in an electronic format i.e. word, excel or PDF?
    - If planning to scan a document does it directly support a matter arising and is it required to provide additional audit evidence?

17. Auditors need to ensure there is an adequate audit trail to support all audit conclusions so that work can be easily re-performed through the review process.

Scanning

18. MKI can incorporate scanned images into the audit file and scanned documents are one form of evidence the auditor can record in the system. Due to the amount of space scanned documents take up, scanning should be used prudently. **Only documents that are essential**

audit evidence should be scanned. **Documents should be scanned in black and white**, with coloured scanning only used when necessary.

19. Auditors should exercise professional judgement when scanning documents as audit evidence. In order to assist auditors the following scanning guidelines **will** be followed:
    - Whenever possible auditors should ask the audited body to provide audit information in an electronic format (e.g. as a word document).
    - It is not necessary to copy all documents examined during the audit. It is generally sufficient for a clear unambiguous reference to the document and its source to be included when recording audit findings.
    - Any documents in the form of hand written notes i.e. interview notes should be of a good readable standard before being scanned into the system.
    - Auditors should attempt to limit scanning documents to when they directly support a matter arising and are required to provide additional audit evidence.

Backing up audit work

20. When working in MKI and connected to the Audit Scotland network, you are required at the end of each day to back up all audit programmes onto the server. This is very important as it reduces the risk of potentially losing audit work should staff go on long term leave or should the network fail. This will also allow other members of staff to view and access audit work.

21. Staff working in offices with limited internet connectivity will sometimes need to work offline. When working offline, backing up our work is very important to minimise the risk of losing any audit work. All staff working offline are required to back up their work on a daily basis and back up their work to the server at the first available opportunity. To back up when offline staff should use the audit programme import / export wizard as documented in the offline working section of the user guide.

Review

22. The Audit Guide sets out the key requirements for quality control of our audits, based on the requirements of ISQC1 and ISA 220. This section details the standards that auditors are required to meet when documenting engagement, management or supervisory reviews and responding to them, within MKI.

23. Detailed procedural guidance on how to carry out engagement, management or supervisory reviews, and how to respond to them, within MKI are contained in the "reviewing audit work" section in the MKI user guides.

24. In line with the Audit Guide the work of less experienced staff must be reviewed by more experienced team members. The permissions attached to each role help support this. First stage review within MKI requires the reviewer to review all audit procedures and associated attachments. Any further review (second stage review) requires the confirmation that sufficient audit evidence has been obtained, audit judgements are clearly documented and conclusions

have been correctly reached. When documenting review points and responding to them, auditors should ensure that appropriate professional language is used at all times.

Personal data / information

25. The Data Protection Act 1998 places a duty on Audit Scotland to protect the personal information they hold and provide individuals with access to personal information held about them. Audit Scotland's policies in respect of personal data are available on SharePoint and provide guidance on what is classified as personal data.

26. In carrying out our audit work we use and collect information that may contain some personal data. For example, personal data may be collected when testing payroll or housing benefit systems. As a minimum any personal information about individuals from audited bodies which is required as evidence for audit findings and conclusions must be stored within MKI and not in any other electronic or hard copy format. If working papers containing personal data are received in hard copy or electronically, auditors are required to return them to the audited body or securely dispose of them once the relevant information has been recorded in MKI.

27. Auditors are expected to exercise judgement when deciding which personal information should be retained as audit evidence on MKI. However, it is recommended that auditors avoid wherever possible recording information in our audit findings, conclusions and documentation which allows individuals to be identified i.e. name or bank details. It is expected, for the purposes of our audit trail, that we record for example the payroll reference number of an individual rather than their name. Exceptions to this would be areas such as senior staff remuneration which are disclosed in a body's financial statements.

Example 2

An auditor is substantively testing a sample of pension payments to individuals from the Teacher's Superannuation Scheme. A random sample is selected of payments. Details are obtained from the pension system. Details recorded on MKI should include the pension reference of the individual, the amount paid and whether it had been paid correctly. No other personal details are required.

Freedom of information (FOI)

28. This act increases the amount of information that the general public can request from all the public bodies we audit as well as Audit Scotland, the Auditor General and the Accounts Commission. Under the Act we have a duty to reply to FOI requests within 20 days of receiving the request for information. In order to comply with the requirements of any potential FOI request, auditors should ensure that all audit documentation saved on MKI is complete and any attachments are named so they can be easily accessed. Recording audit work on MKI will support FOI as the system will be the main repository for working papers for ASG.

MKI management

Naming conventions

29. To assist in improving the consistency in our approach auditors are required to follow the following naming conventions when carrying out work in MKI:
    - **Audit Name** – the auditor will complete the audit name under audit management > audit creation and review (**e.g. 19/20 – Payroll**)
    - **Audit Reference** - abbreviated entity name, year and file area (e.g. Transport Scotland payroll controls file is TS 19/20 B02)
    - **Matters Arising Title** – will consist of year, file name and a concise description of the matter arising (e.g. 19/20 - F02 - Audit Fee - Incorrect disclosure).

Completing and closing an audit file

30. An audit file **can only be completed and closed by managers** once they are satisfied that all work is completed and that sufficient evidence has been obtained. Once an audit file is closed the details and audit programme(s) can only be viewed, no items can be edited. Procedural guidance on completing and closing an audit is contained within the MKI user guides.

31. The naming convention (e.g. 19/20 Payroll) is clearly visible on the audit universe tree structure and various filter functions within MKI. If applied correctly staff will easily be able to view prior year audit files.

Business continuity

32. As part of Audit Scotland's business continuity planning process a business continuity plan has been prepared for MKI, detailing the actions that are required in certain circumstances including:
    - failure of application servers due to network infrastructure failure
    - failure in network connectivity at local site
    - failure with the MKI software
    - Morgan Kai ceases trading and can no longer support MKI.

33. All teams working from a networked local client office are required to put in place a local business continuity plan, detailing the arrangements in place to manage local outages. The local plan will be owned by the relevant manager and a copy logged with the BSS team. The plan owner is responsible for preparing the plan, updating it when new staff arrive and ensuring all staff are aware of arrangements. The manager is also responsible for reviewing the plan annually and updating their Audit Director of recurring problems. The template for local plans is at Appendix A. Tests of the plan will occur from time to time.

MKI support

Arrangements

34. With the introduction of MKI, on-going support is required to deal with issues or problems that arise with the software, our technology, and the application of our audit approach. It is therefore important that auditors are aware of the levels of support that are in place and who should be contacted when help is needed.

35. If you have a problem with a process or an action within MKI, you should consider the following options in this order of preference:

    - Ask your fellow team members
    - Consult the MKI user guides
    - Contact the EWP team - ewp@audit-scotland.gov.uk

36. Digital Support Group (DSG) are the main point of contact for all IT issues related to MKI. Auditors should raise any IT issues with DSG by either calling on 0131 625 1999 or emailing digitalsupport@audit-scotland.gov.uk. In the first instance, DSG will check the equipment, performance, software, client, server and logs. If the issue cannot be resolved by DSG then the issue will be escalated to software suppliers, Morgan Kai. The EWP team will maintain regular contact with DSG to ensure both parties are aware of and understand all outstanding IT issues.

37. Morgan Kai will provide support to Audit Scotland for all issues that cannot be resolved by the EWP team or DSG.

Appendix A: Local BCP Plan

Audit Services Group - Business Continuity Plan for fixed audit location	
Audit team	
Team location	
Plan owner	
Reviewed and approved by manager	
Team members and telephone contact details	
Arrangements for audit team when fixed audit location unavailable	

The plan owner is responsible for preparing the plan, updating it when new staff arrive and ensuring all staff are aware of arrangements. The manager is responsible for reviewing the plan annually, for approving revised plans and updating assistant director of recurring problems. It should be saved in an area staff can access - Audit WIP would be a good place.

If DSG advise of a planned outage teams can work off-line on work or excel or checked-out work from MKI. However for unplanned outages teams should consider working:

- from their base location or another local Audit Scotland office
- from another fixed audit location
- from home using Citrix Access Gateway tokens and home computer

All completed forms are to be kept at the local fixed audit location and copied to the EWP team.

Arrangements for audit team when fixed audit location unavailable	Team will work from: