2.7.1 Retention of audit evidence and finalisation of audit files

Introduction

This section provides policies and guidance to help Audit Office (the Office) teams retain audit evidence in accordance with professional standards and NSW legislative requirements.

Auditing Standards ASQM 1 'Quality Management for Firms that Perform Audits or Reviews of Financial Reports and Other Financial Information, or Other Assurance or Related Services Engagements', APES 320 'Quality Control for Firms', ASA 230 'Audit Documentation' and ASA 500 'Audit Evidence' require:

- established policies and procedures for engagement teams relating to audit documentation (referenced as audit evidence throughout this policy) for audit and assurance engagements
- the assembly of the final audit file to be completed on a timely basis.

For the Office context, the legislative requirement to retain audit evidence is contained within the State Records Authority NSW (State Records NSW) Functional Retention and Disposal Authority: FA353 (FA353).

Policies and guidance – retention of audit evidence in an audit file

Audit evidence within an audit file

1. The Office's methodology, contained in the:

   - Financial Audit Methodology (for financial audit) and
   - Performance Audit Guide (for performance audit)

   defines audit evidence as 'sufficient and appropriate documentation to support an opinion, conclusion or report'. Sufficiency is the measure of the quantity of evidence and appropriateness is the measure of the quality of evidence.

2. The engagement controller (EC) is responsible for ensuring the audit file is assembled, completed, and supports the audit or assurance report with sufficient and appropriate audit evidence.

3. The audit file will consist of one or a combination of the following approved locations:

   - TeamMate audit file
   - secondary cloud storage (currently the Hub)
   - data analytics software application.

4. The TeamMate audit file may be supplemented by:
   - the secondary cloud storage in instances where individual pieces of evidence exceed 200MB. The location for files greater than 200MB is the 'Audit Evidence' folder within the relevant engagement folder in the Hub.
   - a data analytics software application in instances where a large dataset has been tested via the software.

5. Where audit evidence is filed in the secondary cloud storage and/or data analytics software application, the TeamMate file must include a reference (and link where possible) in the relevant section of the audit file to the location of that evidence retained outside of TeamMate.

6. For audits conducted by an audit service provider (ASP), the audit file will consist of the TeamMate audit file and the ASP audit file stored in the Hub.

7. The audit file (for audits conducted in-house or through an ASP) is required to be retained for a minimum of seven years after the date of the audit or assurance report (or 7 years after the consolidated audit report date if part of a group audit) in accordance with the State Records NSW FA353. To comply with this requirement, the Office has determined that records will be retained for a period of ten years. The exception is statutory audit reports from audits of NSW Government agencies which are required as a State archive and must therefore be retained forever in the Office's records management system.

Extraneous information

8. Audit teams may receive information from auditees through the Offices' Audit Collaboration Portal (ACP), emails, hard copies etc. Information not determined to be audit evidence is therefore extraneous to the audit. Information may be assessed as extraneous if it has:

   a) not been tested based on a decision by the audit team that it is not required for the audit

   or

   b) been tested and the audit team has determined that the information does not influence or support the audit conclusion.

9. Extraneous information should be retained in:

   - the ACP for information received through the ACP
   - the relevant engagement folder in the Hub or moved to the ACP workspace for information received via email
   - an alternative approved secondary storage location (this does not include One Drive).

10. For scenario a), extraneous information should be retained in the ACP or the Hub for up to 12 months after the audit file has been finalised before being assessed for destruction by the branch head.

11. For scenario b), information should be retained in the ACP, the Hub or an approved secondary storage location for up to seven years after the audit file has been finalised, before being assessed for destruction by the branch head.

Retention decision tree

12. To help ECs comply with these requirements, a decision tree has been developed (Appendix A) to provide further guidance on what is:

    - evidence and where to retain
    - extraneous information, where to retain and for how long.

Policies and guidance – finalising an audit file

13. Audit files and ACP sites for all audit and assurance engagements must be finalised within 30 calendar days of:

    - issuing the audit report for financial audit
    - tabling the report in Parliament for performance audit.

14. ACP sites are finalised by changing the phase of the audit in the ACP to the last phase ('Finalised' for FAB, and 'Tabled' for PAB). This is can only be done by the Audit Leader once the audit file in TeamMate is finalised.

    Finalisation of ACP sites will automatically trigger the start of the relevant retention period (as outlined above). At the end of the retention period, a notification will automatically be sent to the relevant branch head to review/approve the destruction of data within those ACP sites. In the event the data is not approved for destruction, a new retention period will be applied.

Finalisation

15. As part of the finalisation process, ECs must ensure:

    - both the TeamMate audit file and ACP sites are finalised
    - audit evidence and extraneous information is retained in the appropriate locations as outlined above
    - financial audit statutory audit reports are saved in The Hub.

16. For financial audit only, the following requirements apply:

    - where the General Purpose Financial Statement (GPFS) audit and special purpose financial statement or subsidiary GPFS audits are included in the same TeamMate file, the file should be finalised based on the GPFS audit report date. Where this is not practical, teams should consider whether it is more appropriate to file the different audits in separate files
    - where an ASP has been engaged, the EC must obtain and file an electronic copy of the completed ASP's audit file within the above timeframe of signing the audit report in the Hub. It may not be possible to restore or read the file without the ASP's proprietary software. However, it is important the original, unaltered audit file can be retrieved and accessed, if required. Where possible, the audit team should check the audit file is accessible and complete before accepting the backup.

Approval for an exemption to policy and modification to a file

17. The EC must ensure the **'**Approval of File Modifications After Completion and Late File Finalisations**'** form (the form) is completed where the audit team**:**

    - is not able to finalise the file in accordance with the above timeframes
    - needs to modify a file after the date of the audit report / tabled report or finalisation.

18. If the EC is not able to finalise the file in accordance with the above timeframes, the approval must be obtained before the timeframe for finalisation lapses i.e. before the 30 days passes after the issuance of the audit report or tabling the report. Once approved, a copy of the form must be filed in the Hub**.**

19. Where the file needs to be modified, the EC must:

    - obtain approval for the modification and file this in the Hub
    - instruct a team member to re-open the file, if the file has already been finalised
    - ensure the modification made is in line with the approval
    - finalise the file.

Effective date

Issued October 2023 and effective October 2023.

Appendix A - decision tree for retention of audit evidence