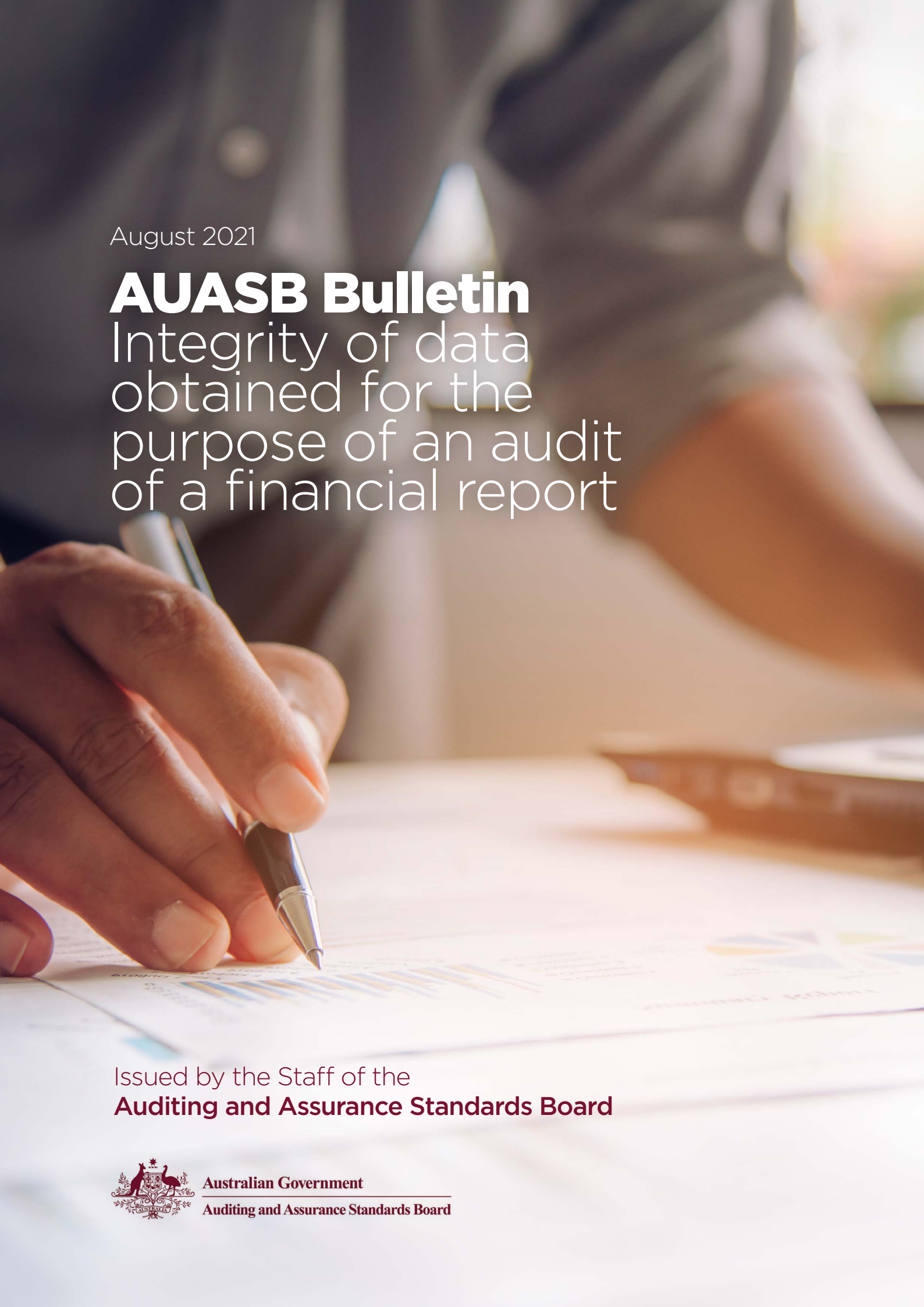


August 2021

AUASB Bulletin

Integrity of data obtained for the purpose of an audit of a financial report

Issued by the Staff of the
Auditing and Assurance Standards Board

Australian Government
Auditing and Assurance Standards Board

About the AUASB

The Auditing and Assurance Standards Board (AUASB) is an independent, non-corporate Commonwealth entity of the Australian Government, responsible for developing, issuing and maintaining auditing and assurance standards.

Sound public interest-oriented auditing and assurance standards are necessary to reinforce the credibility of the auditing and assurance processes for those who use financial and other information. The AUASB standards are legally enforceable for audits or reviews of financial reports required under the *Corporations Act 2001.* For more information about the AUASB see the AUASB Website.

Acknowledgement

The Staff of the Office of the Auditing and Assurance Standards Board express special thanks to the AUASB Technology Project Advisory Group for their contributions to this publication.

Disclaimer

This publication has been prepared by the Staff of the Office of the Auditing and Assurance Standards Board.

The views expressed in this publication are those of the author(s) and those views do not necessarily coincide with the views of the Auditing and Assurance Standards Board. Any errors or omissions remain the responsibility of the principal authors.

Enquiries

Auditing and Assurance Standards Board
PO Box 204
Collins Street West,
Victoria, 8007
Australia

Tel: +61 3 8080 7400

Email: enquiries@auasb.gov.au

Website: www.auasb.gov.au

Copyright

© Commonwealth of Australia 2021

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968,* no part may be reproduced by any process without prior written permission. Requests and enquiries concerning reproduction and rights should be addressed to the Managing Director, Auditing and Assurance Standards Board, PO Box 204, Collins Street West, Victoria 8007

Table of contents

Purpose of this publication

In the audit of a financial report, the relevance and reliability of the information to be used as audit evidence is fundamental to the auditor being able to obtain sufficient and appropriate audit evidence to support the auditor's conclusion[1].

Being able to access and utilise client data, in some instances, is becoming fundamental to executing a quality audit and is being facilitated by technology which allows auditors to capture, store and analyse data in a more effective way. Where previously the process to collect the underlying accounting and other relevant client information for the audit was often very manual with information collected in paper form or packs provided via email or USB, the nature of how client data is being accessed by auditors has expanded well beyond what was initially envisioned in the auditing standards.

The AUASB is aware that the process to collect data[2], transform[3] it into a useable format, determine its integrity, and assess its reliability, can be challenging for auditors, especially the documentation of this process which is having greater regulator focus.

In response to these challenges, the AUASB is releasing two publications. This first publication is focussed on data integrity, addressing matters related to the collection and transformation of data by the auditor. The second publication is focussed on determining the reliability of data collected by the auditor in accordance with the auditing standards. (See figure 1 below).

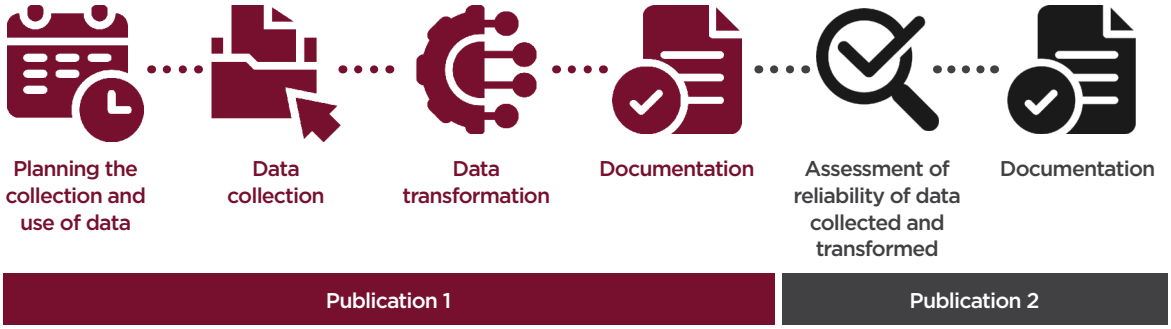


Figure 1 - Data flow

Whilst the terms integrity and reliability are often used interchangeably, for the purposes of these publications they have been split into two separate but interlinked concepts.

- Integrity in the context of this AUASB publication refers to the accuracy with which data has been extracted from the identified source, transferred to the auditor and transformed into an appropriate format for the auditor to use.
- Reliability in the context of this AUASB publication links with reliability in ASA 500 *Audit Evidence.* In order for the auditor to obtain reliable audit evidence, ASA 500 requires auditors to obtain audit evidence about the accuracy and completeness of information to be used as audit evidence.

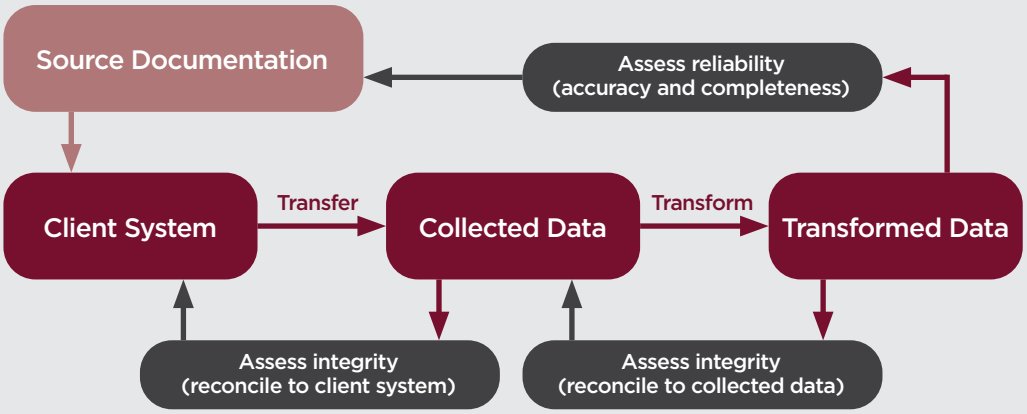
[1] See ASA 500 *Audit Evidence* paragraph 7.

[2] Throughout this publication, the term "collection" is used to describe the extraction of data and transfer of the data to the auditor. Where relevant extraction or transfer is used rather than collection.

[3] Throughout this publication the term "transformation" is used to describe the process through which raw data collected from the client is turned into a format which is useable by the auditor (including to be loaded into the auditor's data analytic solutions).

This distinction has been made as data can have integrity (it reconciles with where it was collected from) but not reliability (insufficient evidence has been obtained over the accuracy and completeness of information).

Example: Integrity vs Reliability



An auditor has extracted data from their client's inventory system to perform procedures related to the accuracy, valuation and allocation of the inventory account balance and related disclosures. The data extracted, transferred and stored by the auditor has been reconciled to the client's system with no errors. The auditor concludes that the information collected has maintained its **integrity** from the client's system.

The auditor intends to perform procedures to assess the obsolescence of inventory using the aging of inventory. To determine the reliability of the data to be used as audit evidence, the auditor selects a sample and tests the accuracy and completeness of the purchase date column of the extracted data set. The auditor identifies from the sample tested that X number do not agree with the source documentation. Therefore, there are questions about the **reliability** of the data for the auditor's purposes.

This publication is not a substitute for reading the auditing standards and is not intended to provide a template for complying with the requirements of the auditing standards. Auditors are required to use their professional judgement to determine the appropriate procedures relevant to their circumstances to be able to comply with the auditing standards.

The IAASB is in the process of revising ISA 500 *Audit Evidence* to modernise the standard and respond to challenges created through the use of technology by auditors and clients. This publication may be updated when the standard has been approved and issued by the AUASB.

Planning the extraction, transfer, transformation and use of data in an audit of a financial report

Introduction

The collection and transformation of data is a fundamental part of an audit when using technology. Whilst the collection and transformation may appear to be a straightforward step, there are a number of ways in which this process can go wrong which can have a significant impact on the auditor's ability to achieve the overall objective of the audit. Where this process is not executed effectively, the problems can significantly compound in terms of additional time spent by the audit engagement team re-performing, adjusting or performing additional procedures or at the extreme end, the auditor's opinion being based on inappropriate evidence.

To mitigate the risks of errors in the collection and transformation process, it is important at the beginning of the engagement to consider and plan the overall approach to data for the audit.

Whilst the focus of this publication is on meeting the requirements of the auditing standards, there are a number of commercial considerations addressed in this publication which are outside of the auditing standards but are nonetheless important in the context of collecting, transforming and using data in an audit of a financial report.

Developing a 'Data Strategy'

Under *ASA 300 Planning an Audit of a Financial Report*, auditors are required to establish an overall audit strategy that sets the scope, timing and direction of the audit and guides the development of an audit plan[4] which is more detailed than the overall strategy.

The auditor's approach to the use of data should follow a similar approach and be appropriately planned to achieve the overall objective of the audit. In the context of this publication the term "data strategy" is used to describe the overall strategy and planned approach to data. Having a stand-alone data strategy is not a requirement of the auditing standards but has been included as a way to manage the collection, transformation and use of data in an audit of a financial report in a consistent manner.

The matters outlined in the data strategy provide a basic framework which can be applied to the use of data in an audit of a financial report to assist auditors in meeting the requirements of the auditing standards regarding the collection, transformation and determination of the integrity of data in particular, documentation requirements of the auditing standards.

[4] See ASA 300, paragraph 7.

In this publication, a data strategy consists of establishing:

Objective (Page 8)

What is the objective of the data collection (e.g. risk assessment or response)?

What is the risk of material misstatement and the specific classes of transactions and account balances data is required for?

Data (Page 9)

What data is needed to meet the objective, where is the data located and can it be extracted in a useable and timely format?

How will the data be extracted and transferred to the auditor?

Storage (Page 10)

Once extracted, where will the data be stored and how will the integrity be maintained?

Who (Page 11)

Who will undertake the collection and transformation of data?

What tools will be used?

Are specialist skills needed to collect and transform data? Do the skills exist within the audit team or firm?

Objective

Before commencing any collection and transformation of data, it is important for auditors to determine the objective of the use of the data in the audit, this determination may include:

- Identifying the specific procedure the data is intended to be used for. (For example, is the data to be used for risk assessment, audit response or both?)
- Where applicable, the specific classes of transactions and balances data will be required for. Not all data will relate to a specific class of transaction or balance, for example, data may be collected as part of the auditor's understanding of general IT controls.
- The timing of procedures that require data. (For example, substantive procedures may be performed at both interim and year-end, so data that may usually be collected at year-end is required to be collected at both).
- How does this collection fit in with the overall approach to the audit? Are there other procedures that will benefit from the data collection?

What data is available and where is it located?

After establishing a clear objective for the use of data, it is important to determine whether the data needed to meet the objective is actually available, where the data is located and whether it can be extracted in a useable and timely manner. This deeper understanding of the client's data can increase the efficiency and effectiveness of the audit through, for example:

- enabling selection of primary data sources, such as the underlying Enterprise Resource Planning system (ERP), rather than client-generated and maintained reports; and
- testing a data set once which is used in multiple procedures throughout an audit and can be efficiently re-performed in subsequent years.

In establishing what data is available and where it is located, auditors may consider[5]:

- Whether the data needed to meet the objective is available and accessible by the auditor. This includes identifying whether the data is from an internal or external information source as this may impact on the availability and timeliness.
- The volume of the data expected to be extracted and transferred.
- The nature of the data (for example, whether it is financial, non-financial, master data, system configuration data or reports) and whether there are any specific confidentiality and privacy requirements that should be considered as part of the collection and storage.
- Where the data is from an internal source, identifying the specific system or systems the data is to be obtained from and understanding the system in sufficient detail to determine whether there are any inherent limitations or challenges in the system. This may involve understanding:
    - The complexity of the system(s) which may affect the understandability of any outputs.
    - The level of customisation of the system by or for the client, for example, are systems off the shelf or have they been customised by the client or specifically developed for the client? (Customisation may present problems such as X indicates a manual journal in an off the shelf system but means something different in a customised system).
    - Connectivity and reliance on other systems and the level of automation involved (for example, are there manual or automated transfers between systems).
    - Controls over the preparation and maintenance of data.
- Will the data be available when it is needed in the audit plan? (For example, understanding the cut-off date for processing all transactions in the GL for year-end. Where data is collected before this date, there is a risk that the data will be incomplete or inaccurate).

[5] In some instances, data may remain in the client's environment and be accessed in situ for the purposes of performing audit procedures. Whilst this publication does not specifically cover matters related to in situ data access and usage, it is likely that many of the risks outlined in the publication may also be relevant for the auditor to consider where data remains in the client's environment.

Where will collected data be stored and how will its integrity be maintained?

After establishing what data is needed and where that data is located, it is important to establish where the data will be stored once extracted and how will the integrity of the data be maintained once it is in the auditor's control. The method of collection will be covered in the next section on "Who will collect and transform the data".

The collection and storage of client data is not a new process for auditors. The AUASB Standards[6] and ethical requirements of the APESB[7] already require firms to establish policies and procedures to maintain the confidentiality, safe custody and integrity of engagement documentation as well have appropriate retention policies for that documentation.

Whilst the AUASB Standards and relevant ethical requirements address engagement documentation, it is important for auditors to consider their approach to retaining data which does not form part of engagement documentation. Where data is retained for analytics and benchmarking or other purposes, the retention should be discussed with the client and a policy for retention and destruction of data implemented[8].

Another matter to consider regarding the storage of client data is the potential for data breaches. Auditors should be aware of obligations, if any, under the Privacy Act 1988 of holding client data and where firms operate across jurisdictions, legislation in other jurisdictions such as the EU and UK General Data Protection Regulation (GDPR). Like other organisations, the loss of personal information stored by the firm, including client data can pose a significant commercial risk.

When considering the storage of data auditors may consider matters such as:

- Does the firm have permission from the client to collect and store the data?
- Does the firm have appropriate infrastructure to store the data?
    - Where is the firm's infrastructure located? Where infrastructure crosses borders, certain data may not be able to be stored there.
    - How will the firm maintain security over the data?
- Will a third-party be used to store data?
    - Where a third-party is used, what are the agreements around access, backups and retention with the third party?
    - How does the third-party maintain security over the data?
    - Where will the data be stored by the third party? Will the data cross-borders?
- Are appropriate retention and destruction policies in place for data collected which does not form part of the engagement documentation?
- Does the firm have a plan in place in the event of a data breach?
- Does the firm have appropriate data handling training in place for staff to communicate the importance of safe handling of client data?

[6] See ASQC 1 *Quality Control for Firms that Perform Audits and Reviews of Financial Reports and Other Financial Information, Other Assurance Engagements and Related Services Engagements* paragraphs 46 and 47.

[7] See APES 110 *Code of Ethics for Professional Accountants (including Independence Standards)* paragraphs R114.1, 114.1 A1 and R360.26.

[8] There are a number of matters (legal and ethical) not addressed as part of this publication that auditors/firms should consider as part of the retention of data which does not form part of the audit file.

Who will collect and transform the data?

An important part of the process of using data in an audit is being able to document and explain the process to extract, transfer, transform (including loading into any tools) and determine the integrity of information to be used as audit evidence.

A key part of this process is determining, and documenting, who is involved in this process and how the requirements of ASA 220 have been met, in particular requirements relating to engagement performance (direction, supervision and review)[9].

When considering who will be involved in the extraction, transfer and transformation auditors may consider matters such as:

- Will the extraction of data be performed by the client, the auditor or an expert?
- Where the client will perform the extraction:
    - Does the client have sufficient understanding of the systems to be able to extract the data needed by the auditor?
    - Can the collection be done by the client in a timely manner?
    - What procedures will need to be performed by the auditor to determine that the client has not manipulated the data during the extraction or transfer?
- Where the extraction is to be performed by the auditor:
    - What tools will be used to perform the extraction?
    - What are the processes to determine the reliability of any tools used during the extraction?
    - Where relevant, does the engagement team member have expertise to be able to use the necessary tools to collect and prepare large volumes of data (for example, where large volumes of transactions are collected can they use SQL or another database tool)?
- Where an expert is required, is the expert an internal or external auditor's expert?
    - Understand requirements around the use of internal and external auditor's experts as part of ASA 220 and ASA 620 *Using the Work of an Auditor's Expert.*
- Do engagement team members have sufficient understanding of the extraction, transfer and transformation process to be able to identify errors in the process?

Where the data has been produced by a management's expert, GS 005[10] provides guidance around the use of the work of a management's expert including the determining whether an auditor's expert is needed to assess the work of the management's expert.

[9] See ASA 220 *Quality Control for an Audit of a Financial Report and Other Historical Financial Information.*

[10] GS 005 *Evaluating the Appropriateness of a Management's Expert's Work.*

Collecting data

Overview

Maintaining the integrity of data collected by the auditor is fundamental to the auditor's use of data. Errors in the extraction and transfer process which are not identified may impact on the auditor being able to obtain sufficient and appropriate audit evidence to support the auditor's conclusion.

The process to collect data for use in an audit can vary significantly based on the nature and source of the data but also from entity to entity where systems have been configured in different ways. It is important that a robust process covering both the extraction and transfer data is established to mitigate some of the risks to integrity. This process can be established at a firm level and may include consideration of when experts need to be used or specific data where expertise is required.

Regardless of the process to collect data and who undertakes the collection, it is important that auditors (engagement team members) establish a strong understanding of what can go wrong during the collection process to be able to execute the collection process appropriately and ensure that the integrity of data is maintained.

What can go wrong?

Area of collection	What can go wrong?	Possible mitigation
Data specific issues	· Issues with integrity of data before any collection has occurred. · Data transferred from the client becomes corrupted during the transfer. · Issues with integrity of data held by a third-party.	· Reconciliation of data post extraction and transfer. · Auditors being given direct access to collect data rather than relying on the client. This is noted as contingent on the client and the client's systems.
System issues	· Inability to extract data in a useable format (for example, reports can only be extracted in PDF). · Extraction being incomplete or failing to run. · Extracting large volumes of data causes system crashes. · Limitations around availability of data (point in time only data or specific identifiers are not retained by system).	· Understanding limitations of systems early and working with clients to identify alternatives. · Ensuring client has sufficient understanding of their own systems which may include discussions with software vendors. · Contacting software vendors directly to understand how to extract data needed.
Who is undertaking the extraction	· Lack of client knowledge of their system results in incorrect data being extracted (e.g., incorrect parameters in a report). · Lack of auditor knowledge of the system results in incorrect data being extracted. · Lack of auditor understanding of how tools operate. · Technical errors occurring when data is loaded into auditor's systems. · Manipulation of data during extraction and transfer process.	· Assessing the reliability of any underlying data extraction tools being used by the client. · Assessing the skills and competence of the team and having clear policies on who can perform tasks and when experts are required. · Having a process to identify any manipulation during the extraction and transfer process where this has not been undertaken by the auditor.

Transforming data

Overview

In this context of this publication, transformation is used to describe the way the raw data collected by the auditor is processed for use by the auditor (including for loading into the auditor's data analytic solutions).

The process to transform data into a useable format and load that transformed data into tools to be used by the auditor creates a number of opportunities for errors to occur. If this step is done incorrectly, the use of the data and any conclusions made based on the transformed data can be incorrect and impact on the auditor's opinion.

It is important as part of this step that once the data is transformed it is reconciled to the collection to ensure its integrity. The risk of something going wrong during the transformation phase is increased where a large amount of data cleansing is required to be done manually by the auditor.

Area of transformation	What can go wrong?	Possible mitigation
Transformation	· Incorrect mapping of data and other basic errors being made during the cleansing of data for use in auditor systems such as deleting or incorrectly interpreting key information (for example, deleting unique identifiers for transactions or US date formats incorrectly converted to Aus. date). · Errors in the tools and environments used by the auditor either from the tool not working as intended or errors from the auditor loading the data into auditor tools such as column shifting or special characters creating issues. Different tools will have different needs which may be outside of the expertise of auditors performing the loading.	· Having clear documentation of the mapping of data. For example in SAP document type "SA" can be an indicator of manual journals. · Performing procedures to identify mapping and other basic errors once it is loaded into the auditor's tools and environments. · Having appropriate skills and competence in the team to be able to understand the transformation and review it appropriately.
Storage of transformed data	· Data once transformed is altered.	· Having clear procedures on how to manage data once it leaves the client's system to maintain integrity such as restricting access only to authorised staff.

Audit documentation and data retention

It is important that a consistent approach to documentation be developed by auditors/firms which follows the process and outcomes of the collection, transformation and use data.

Documentation should address matters such as the technology deployed by the auditor/firm to undertake the collection and transformation, how that technology was deemed suitable for use as well as how the engagement partner has understood the process and outcomes to be able to discharge their oversight responsibility, especially requirements related to direction, supervision and review.

Documentation of the collection and transformation process may include:

- The nature and source of the data, including identifying characteristics which may include:
    - The type of data.
    - The system the data was collected from.
    - The specific data tables or reports used to collect the data.
- How the data was extracted, including:
    - The date the extraction occurred.
    - Who undertook the extraction?
        - Why they are appropriately skilled to undertake the extraction.
        - Where an auditor's expert is used, determination of whether the expert is an internal or external expert. Where an internal expert is used, documentation in line with applicable requirements of ASA 620 *Using the Work of an Auditor's Expert* and ASA 220.
    - The method of extraction including any tools used.
        - How were the tools deployed determined to be working appropriately?
    - The method of transferring the data to the auditor, including any tools used.
        - How has the auditor ensured that the data has not been manipulated during the process of transferring the data to the auditor.
    - Assessment of the accuracy and completeness of the data extracted to the source to conclude on the integrity of the data obtained.
- How the data was transformed, including:
    - Who undertook the transformation?
        - Why they are appropriately skilled to undertake the transformation.
        - Where an auditor's expert is used, determination of whether the expert is an internal or external expert. Where an internal expert is used, documentation in line with applicable requirements of ASA 620 *Using the Work of an Auditor's Expert* and ASA 220.
    - The method of transformation including any tools used.
        - How were the tools deployed determined to be working appropriately?
    - Assessment that the integrity of the data has been maintained throughout the transformation process.

- Direction, supervision and review of engagement team members.
- How the auditor maintained the integrity of the data after the collection and transformation process (through retention and storage).

The IAASB's Audit Documentation When Using Automated Tools and Techniques provides guidance and examples which auditors may find helpful when determining the appropriate form, content and extent of audit documentation when data has been obtained and automated tools and techniques used.

The auditing standards are technology neutral and require sufficient documentation to be prepared so that an experienced auditor having no previous connection with the audit can understand what has occurred and how conclusions were reached[11]. The extent of documentation and retention of data in the engagement file is a matter of professional judgement in accordance with the requirements of ASA 230. ASA 230 is principles based, and therefore remains applicable regardless of the nature of the tool or technique that the auditor applies, and the data used.

Whilst there can be challenges in determining how to document the collection (extraction and transfer) and transformation of data, it is important for auditors to keep in mind that whilst the volume of data collected by auditors has changed, the documentation expectation has not. Entire populations of data are not required to be included as part of the audit documentation and auditors should approach documentation the same way that they approach the documentation of something like general journal testing.

Any data sets collected, and which do not form part of the audit documentation, should be appropriately secured and have appropriate retention and deletion policies established for them. Whilst these full data sets may not form part of the audit documentation, documentation of their collection and transformation should form part of the audit documentation.

[11] See ASA 230 *Audit Documentation* paragraph 8.

Australian Government

Auditing and Assurance Standards Board

Podium Level 14, 530 Collins Street, Melbourne VIC 3000 | www.aasb.gov.au