5. Overview of a compliance audit

Standards on Assurance Engagements 5:2
What is a compliance audit? 5:2
Overview of ASAE 3100 5:2
Ethical requirements 5:3
Quality control 5:3
Professional scepticism 5:3
Acceptance and continuance 5:3
Overview of the audit approach under ASAE 3100 5:5
Planning 5:6
Performing 5:7
Evaluate, report and wrap-up 5:7
5. Overview of a compliance audit

This chapter provides guidance for Assurance Practitioners who are required to undertake a compliance engagement.

This chapter provides an overview of the methodology and details of the relevant standards and specific information relating to the entities covered by this guide are covered in the appropriate chapter:

- Compliance audit of an SMSF – Chapter 2;
- Audit of a real estate agent’s trust account – Chapter 6;
- Audit of client monies – Chapter 7;
- Audit of a solicitor’s trust account – Chapter 8.

Standards on Assurance Engagements

The relevant standards are the Standards on Assurance Engagements (ASAEs) which are issued by the Auditing and Assurance Standards Board (AUASB) as discussed below:

- ASAE 3000 Assurance Engagements Other than Audits or Reviews of Historical Financial Information is the over-arching standard which is for general application to assurance engagements other than audits or reviews of historical financial information covered by ASREs and ASAs.
- ASAE 3100 Compliance Engagements is the specific standard which is considered in conjunction with ASAE 3000 for the engagements covered by this guide.

Note: the term auditor has been used throughout this chapter and is interchangeable with the term ‘Assurance Practitioner’ used in the ASAEs.

What is a compliance audit?

A compliance audit is different from an external audit since the auditor is not forming an opinion on the financial report but on the client’s compliance with specified criteria.

The objective of a compliance engagement is to enable the auditor to express a conclusion on whether an entity has complied in all material respects, with requirements as measured by the suitable criteria.

The responsibility for an entity’s compliance with requirements as measured by the suitable criteria rests with the responsible party. A compliance engagement performed by an auditor does not relieve the responsible party of its obligations to ensure compliance with requirements as measured by the suitable criteria.

Overview of ASAE 3100

ASAE 3100 provides mandatory requirements and guidance for auditors engaged to provide assurance on an entity’s compliance with externally imposed requirements as measured by suitable criteria.

ASAE 3100 requires the auditor to:

- Comply with applicable ASAEs;
- Comply with the fundamental ethical principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour;
- Implement quality control procedures;
- Meet acceptance and continuance procedures;
- Agree the terms of the engagement in writing;
- Plan the compliance engagement so that it will be performed effectively;
- Consider materiality and compliance engagement risk when planning and performing the compliance engagement;
5. Overview of a compliance audit

- Obtain sufficient appropriate evidence on which to base the conclusion and evaluate the impact on the conclusion of any compliance breaches noted;
- Consider the effect of events up to the date of the compliance report;
- Prepare, on a timely basis, documentation that is sufficient and appropriate to provide a basis for the auditor’s conclusion and evidence that the engagement was performed in accordance with ASAE 3000 and ASAE 3100;
- Express a conclusion about the subject matter information.

The auditor is required to document the key elements of the compliance framework, such as procedures for identifying, assessing and reporting compliance incidents and breaches.

**Ethical requirements**

The auditor is required to comply with the fundamental ethical principles of:
- Integrity;
- Objectivity;
- Professional competence and due care;
- Confidentiality;
- Professional behaviour.

Additional guidance on these requirements can be found in Chapter 1 – Overview of Audits and Reviews.

**Quality control**

The auditor is required to implement procedures to address the following elements of a quality control system that applies to the individual engagements:
- Leadership responsibilities for quality on the assurance engagement;
- Ethical requirements;
- Acceptance and continuance of client relationships and specific assurance engagements;
- Assignment of assurance engagement teams;
- Assurance engagement performance; and
- Monitoring.

Further information on the quality control requirements can be found in Chapter 1 – Overview of Audits and Reviews.

**Professional scepticism**

A compliance audit should be planned and performed with an attitude of professional scepticism which is discussed in detail in Chapter 1.

**Documentation**

The auditor is required to prepare and maintain documentation on a timely basis that provides:
- A basis for their conclusion; and
- Evidence that the engagement was performed in accordance with ASAE 3000 and ASAE 3100.

**Acceptance and continuance**

**Tripartite relationship**

When considering whether an engagement should be accepted or continued, the auditor needs to determine who is responsible for the subject matter. This responsibility should rest with a party other than the intended users or the auditor, otherwise the engagement should not be accepted.
Whilst the responsible party may be a user of the information, they should not be the only users, i.e. there must be at least three parties involved in an assurance engagement. This should be acknowledged in the engagement letter.

For example – in a solicitor trust audit – the solicitor is the responsible party and although they are a user, the Law Society is also a user.

**Non-compliance with ethical principles**

The auditor should only accept or continue with any engagement where nothing has come to their attention to indicate the fundamental ethical principles will not be satisfied.

This means considering whether:

- Relevant ethical requirements, such as independence and professional competence will be satisfied and
- The assurance engagement exhibits the following characteristics:
  - the subject matter is appropriate;
  - the criteria to be used are suitable and are available to the intended users;
  - the auditor has access to sufficient appropriate evidence to support the assurance practitioner’s conclusion;
  - the auditor’s conclusion, in the form appropriate to either a reasonable assurance engagement or a limited assurance engagement, is to be contained in a written report; and
  - the auditor is satisfied that there is a rational purpose for the assurance engagement. If there is a significant limitation on the scope of the auditor’s work, it may be unlikely that the assurance engagement has a rational purpose. Also, an auditor may believe the engaging party intends to associate their name with the subject matter in an inappropriate manner.

Also, if the party engaging the auditor (the ‘engaging party’) is not the responsible party, the auditor ordinarily considers the effect of this on access to records, documentation and other information they may need to complete the assurance engagement.

**Competence**

The auditor considers where they or the team possess the necessary professional competencies to perform the engagement.

**Engagement letter**

The terms of the engagement are agreed in a letter prepared by the auditor and signed off by both parties, this letter should refer to applicable legislation, as necessary.

The letter includes:

- the objectives of the compliance engagement;
- the scope of the compliance engagement; and
- the suitable criteria against which compliance is measured.
Overview of the audit approach under ASAE 3100

In a compliance engagement sufficient appropriate evidence is obtained as part of an iterative, systematic engagement process involving:

a) obtaining an understanding of the entity’s business and its compliance environment which includes the key elements of the entity’s compliance framework;

b) obtaining an understanding of the requirements, the suitable criteria and other engagement circumstances which, depending on the subject matter, may include obtaining an understanding of internal controls and testing the effectiveness of these controls;

c) obtaining an understanding of the internal compliance function where appropriate and any relevant testing of compliance controls performed as part of that function during the period;

d) Evaluating the results of this testing and the level of reliance that can be placed on this work and the impact on further control and substantive procedures;

e) based on the understanding acquired under (a), (b) and (c), assessing the risks that the entity may be non compliant with requirements as measured by the suitable criteria; responding to assessed risks, including developing overall responses, and determining the nature, timing and extent of further procedures; and

f) performing further evidence-gathering procedures clearly linked to the identified compliance engagement risks, using a combination of inspection, observation, confirmation, recalculation, re-performance and enquiry. Such further evidence-gathering procedures may involve substantive procedures, including obtaining corroborating information from sources independent of the entity, and depending on the nature of the activity or subject matter, tests of the operating effectiveness of controls.
Planning

A compliance audit needs to be planned so that it will be performed effectively. The planning phase of a compliance audit involves:

- developing an overall strategy for:
  - scope;
  - emphasis;
  - timing; and
  - conduct of the engagement.
- preparing an engagement plan consisting of a detailed approach for the nature, timing and extent of evidence-gathering procedures to be performed and the reasons for selecting them.

The following items should be included within the audit plan:

- The terms of the engagement.
- The characteristics of the subject matter/requirements and the identified criteria and the appropriateness and suitability of these.
- The engagement process and possible sources of evidence.
- The understanding of the entity and its environment and the compliance framework, including the risks that the entity may not be compliant with the requirements as measured by the suitable criteria.
- Identification of intended users and their needs, and consideration of materiality and the components of assurance engagement risk.
- Personnel and expertise requirements, including the nature and extent of experts’ involvement.

The audit plan is updated throughout the engagement, as necessary.

Business understanding

The auditor needs to obtain and document their understanding of the subject matter and other considerations in relation to the engagement to allow them to:

- Identify and assess risks of the entity’s non-compliance with the requirements as measured by the suitable criteria; and
- Sufficiently design and perform appropriate evidence-gathering procedures.

Professional judgement (discussed further in Chapter 1) is used to determine the extent of the understanding needed to allow them to sufficiently assess the compliance engagement risk.

Compliance engagement risk is defined as ‘the risk that the assurance practitioner expresses an inappropriate conclusion when the entity is materially non-compliant with the requirements as measured by the suitable criteria.

Elements of a compliance framework

In order for the auditor to be able to plan appropriate audit procedures, they need to obtain an understanding of the compliance environment and document the key elements of the compliance framework, this would include:

- Procedures for identifying and updating compliance obligations.
- Staff training and awareness programs.
- Procedures for assessing the impact of compliance obligations on the entity’s key business activities.
- Controls embedded within key business processes designed to ensure compliance with obligations.
- Processes to identify and monitor the implementation of further mitigating actions required to ensure that compliance obligations are met.
- A monitoring plan to test key compliance controls on a periodic basis and report exceptions.
- Procedures for identifying, assessing, rectifying and reporting compliance incidents and breaches.
- Periodic sign off by management and/or external third party outsourced service providers as to compliance with obligations.
- A compliance governance structure that establishes responsibility for the oversight of compliance control activities with those charged with governance, typically a Board Audit, Risk Management or Compliance Committee.
5. Overview of a compliance audit

Once this understanding has been obtained then the audit can assess the appropriateness of the subject matter and the suitability of the criteria to evaluate or measure the subject matter.

**Materiality**

The auditor considers materiality when planning and performing the compliance engagement and in assessing any compliance breaches.

Materiality is applied to a compliance audit in a different way from the audit of a financial report. A compliance audit is concerned with compliance with set requirements (such as standards or laws), rather than the misstatement of the financial report. In assessing this compliance, the auditor is required to test transactions to ensure that they have been dealt with and recorded in a way that is consistent with legislation.

For example, if a transaction has been recorded incorrectly then that is a breach of the legislation and therefore the dollar value of the transaction does not matter.

ASAE 3100 defines materiality in the context of a compliance audit as:

i. in relation to potential (for risk assessment purposes) or detected (for evaluation purposes) breaches – instance(s) of non compliance that are significant, individually or collectively, in the context of the entity’s compliance with the requirements as measured by the suitable criteria, and that affect the auditor’s conclusion; and/or

ii. in relation to the compliance framework and controls – instance(s) of deficiency that are significant in the context of the entity’s control environment and that may raise the compliance engagement risk sufficiently to affect the auditor’s conclusion.

**Performing**

During this phase of the audit, the auditor performs evidence-gathering procedures that are clearly linked to the identified risks.

The procedures generally use a combination of inspection, observation, confirmation, recalciulation, re-performance, analytical procedures and enquiry.

Such further evidence-gathering procedures involve substantive procedures, including obtaining corroborating information from sources independent of the entity, and depending on the nature of the subject matter, tests of the operating effectiveness of controls.

Where there are material deficiencies in the entity’s compliance framework, the auditor assesses the impact on the risk of non-compliance and therefore amends their procedures, as appropriate.

**Evidence obtained**

The audit assesses whether the audit evidence obtained is both sufficient (in respect of the quantity of the evidence) and appropriate (the quality of the evidence).

**Use of an expert**

Where the auditor deems that the use of an expert is necessary then the auditor and expert should have the combined necessary knowledge and skill to allow them to determine that sufficient, appropriate evidence has been obtained regarding the subject matter and criteria.

**Written representations**

The auditor should consider whether it is necessary, or required by legislation, to obtain representation on certain matters from management.

**Evaluate, report and wrap-up**

**Deficiencies and compliance breaches**

When deficiencies or compliance breaches have been found during the course of the audit, the auditor needs to determine whether they are material based on the criteria.

In evaluating any deficiencies and compliance breaches the auditor generally considers materiality as specified in the terms of the engagement, any relevant legislative, regulatory or other requirement which may apply and the effect on the decisions on the intended users of the compliance report and the auditor’s conclusion.
**Communication to the responsible party**
The auditor should communicate any deficiencies or compliance breaches as soon as possible to the responsible party for the material as soon as practical.

**Subsequent events**
Where subsequent events have the potential to affect the entity’s compliance and the appropriateness of the auditor’s conclusion then they should be considered.

**Audit report**
Whilst many of the engagements covered in this guide may have specified content and format for the audit report on the compliance engagement, the auditor should ensure that the report is in accordance with the requirements of ASAE 3000 and ASAE 3100.

The audit report contains the following elements:

a) a title that clearly indicates the report is an independent assurance report;

b) an addressee;

c) an identification and description of the requirements;

d) period of compliance being reported on;

e) identification of the suitable criteria;

f) where appropriate, a description of any significant, inherent limitation associated with the evaluation of compliance with the requirements as measured by the criteria;

g) when the criteria used to evaluate the requirements are available only to specific intended users, or are relevant only to a specific purpose, a statement restricting the use of the compliance report to those intended users or that purpose;

h) a statement to identify the responsible party and to describe the responsible party’s and the auditor’s responsibilities;

i) a statement that the engagement was performed in accordance with ASAEs and the level of assurance provided;

j) a summary of the work performed;

k) the auditor’s conclusion:

   i. in a reasonable assurance engagement, the conclusion shall be expressed in the positive form;

   ii. in a limited assurance engagement, the conclusion shall be expressed in the negative form; and

   iii. where the assurance practitioner expresses a conclusion that is other than unqualified, the assurance report shall contain a clear description of all the reasons;

l) the compliance report date; and

m) the name of the firm or the auditor, and a specific location, which ordinarily is the city where the auditor maintains the office that has responsibility for the engagement.

Appendix 1 of ASAE 3100 has an example compliance report which may be used where the legislation or other requirements do not require a specific format or content for the report.