

Audit guideline for energy businesses (draft)



An appropriate citation for this paper is:

Essential Services Commission 2017, *Audit guideline for energy businesses (draft)*: November 2017.

Copyright notice

© Essential Services Commission 2017

C/17/20173



This work, *Audit guideline for energy businesses (draft)*, is licensed under a Creative Commons Attribution 4.0 licence [creativecommons.org/licenses/by/4.0/]. You are free to re-use the work under that licence, on the condition that you credit the Essential Services Commission as author, indicate if changes were made and comply with the other licence terms.

The licence does not apply to any brand logo, images or photographs within the publication.

Draft audit guideline for energy businesses

This guideline replaces:

Guideline No. 22 – Regulatory audits of energy businesses C/14/1138

Enquiries concerning the currency of this guideline should be addressed to -

The Essential Services Commission

Level 37, 2 Lonsdale Street

Melbourne 3000

Telephone (03) 9302 1300, facsimile (03) 9302 1303

Amendment record

Part	Issue no.	Date	Pages	Checked
	1	21/09/09	14 – New section 6.2.3	
	2	21/09/09	15 – Section 6.4 renumbered	
	3	22/01/14	General revision	
	4	30/11/17	General revision (draft)	

Contents

1. DEFINITIONS	1
2. INTRODUCTION	2
2.1. Purpose of the guideline	2
3. KEY REGULATORY AUDIT CONCEPTS	4
3.1. Purpose of a regulatory Audit	4
3.2. Identifying risk, and determining type, frequency and timing of an Audit	4
4. APPOINTING THE AUDITOR	6
4.1. Licence condition to appoint an Auditor	6
4.2. Empanelment of Auditors	6
4.3. Licensees to appoint an Auditor from the panel	6
4.4. The commission's approval	6
5. APPROVING THE AUDIT SCOPE	7
5.1. Type of Audit	7
5.2. Identifying regulatory obligations to be Audited	7
5.3. Specific compliance issues	8
5.4. Audit period	8
5.5. Planning	8
5.6. Briefing the Auditor	9
6. CONDUCTING THE AUDIT	10
6.1. Audit methodology	10
6.2. Reliance on other work	10
7. ASSESSING AND REPORTING ON COMPLIANCE	11
7.1. Standard compliance grades	11
7.2. Compliance performance indicators and assessments	11
7.3. Step one	13
7.4. Step two	14
7.5. Step three	16
7.6. Step four	16
7.7. Current and period compliance	16
7.8. Level of confidence	16
7.9. Continuous improvement	16

7.10. Signed statement	17
7.11. Findings register	17
7.12. Audit Report	17
7.13. Draft deliverables	17
7.14. Reporting procedures	18
7.15. Copy of final deliverables	19
8. RESPONDING TO THE AUDIT	20
9. Quality assurance framework	22
10.AMENDMENTS	25

DRAFT

1. DEFINITIONS

'Audit' means an audit conducted under a Licence or Relevant Guideline, or which is required to be conducted under a Licence or Relevant Guideline.

'Auditor' means the Audit Firm engaged by the Licensee, and approved by the commission. The Auditor will be a party to the Audit Deed.

'Audit Deed' means the standard tripartite deed as defined at 4.1.1 and signed by the commission, the Auditor and the Licensee that confirms each party's obligations arising from the Audit.

'Audit Report' means the report on the Audit prepared by the Auditor in accordance with clause 7.12.2.

'Audit Team' means, at any time, the group of persons engaged by the Auditor in accordance with this guideline to undertake the Audit.

'commission' means the Essential Services Commission.

'COSO' means the Committee of Sponsoring Organisations of the Treadway Commission.

'Information Specifications' means the commission's published requirements for Licensee reporting.

'Licence' means the Licence issued to the Licensee by the commission pursuant to either the Electricity Industry Act 2000 or the Gas Industry Act 2001.

'Licensee' means the person who holds a Licence.

'Obligation' means anything the Licensee is required to do pursuant to its Licence; in particular, complying with performance requirements and reporting regulatory information to the commission (regulatory information may include performance information for comparative reporting).

'Relevant Guideline' means a guideline or statement published by the commission (as revised or substituted prior to the relevant time) dealing with audits under the condition of the Licence and/or referred to in the Audit Deed.

'Risk Assessment' means the Risk Assessment undertaken by the commission in accordance with 3.2.1.

'Subcontractor' means any person contracted by an Auditor, other than a direct employee of the Auditor, for the purposes of conducting an Audit.

2. INTRODUCTION

2.1. Purpose of the guideline

- 2.1.1. *Audit guideline for energy businesses, February 2018 (the guideline)* sets out the requirements of the commission when requesting that energy Licensees undertake regulatory Audits. The guideline outlines how the regulatory Audit scope will be determined, how the Auditor will be approved, what governance arrangements will apply during the Audit process and the form and format of the Audit Report.
- 2.1.2. The parts of this guideline that relate to the performance by the commission of its functions and exercise of its powers are guidelines published by the commission under section 13 of the *Essential Services Commission Act 2001*.
- 2.1.3. This guideline applies to Licensees as a condition of Licence. Under the terms of a Licence, Licensees are required to:
- a) comply with the guideline and any other guideline relevant to the Audit process; and
 - b) appoint an independent Auditor to conduct an Audit of:
 1. their compliance with their Licence Obligations, including the Obligation to comply with industry codes and guidelines; and
 2. the reliability and quality of the information reported by them to the commission, and whether that information is consistent with the commission's specifications.
- 2.1.1. This guideline applies to Auditors. Under the terms of the tripartite Audit Deed, the Auditor is required to comply with this guideline as a Relevant Guideline.
- 2.1.2. The commission requires that any regulatory Audits of Licensees must be based on the general principles stated in *Standard on Assurance Engagements ASAE 3100 Compliance Engagements*. It is also expected that, where appropriate, Auditors will apply the principles and guidelines recommended by relevant standards including: *Standard on Assurance Engagements ASAE 3402 Assurance Reports on Controls at a Service Organisation*; *Standard on Related Services ASRS 4400 Agreed-Upon Procedures Engagements to Report Factual Findings*; *AS 3806-2006 Compliance programs*; *AS/NZS ISO 31000:2009 Risk management – Principles and guidelines*; and *COSO Enterprise Risk Management – Integrated Framework*
- 2.1.3. The guideline is intended to:
- a) *make sure that Audits are conducted in an independent, thorough way to aid comparison across sectors*; this will be achieved by establishing the minimum

requirements for conducting Audits, the level of independence and expertise required of Auditors, and the conduct and reporting of Audits;

- b) *encourage a culture of continuous improvement in the energy industry*; this will be achieved by minimising the likelihood that significant non-compliance will remain undetected, and providing Licensees with an opportunity to resolve non-compliance before the commission considers enforcement action; and
- c) *optimise the cost-effectiveness of Audits*; the commission will achieve this by taking a risk-based approach to defining the scope of Audits.

2.1.4. Nothing in the guideline is intended to limit the commission in the exercise of its powers. This includes, without limitation, the specification of terms of any agreement or deed to be entered into by the commission with a Licensee, or an Auditor, in relation to matters relating to an Audit

DRAFT

3. KEY REGULATORY AUDIT CONCEPTS

3.1. Purpose of a regulatory Audit

- 3.1.1. The purpose of a regulatory Audit is to provide the commission with independent assurance that Licensees are complying with their Licence Obligations.
- 3.1.2. To make sure that an Audit is independent, a three party relationship must exist between the commission, the Licensee, and the approved Auditor. This should be the case where :
- a) the commission is the intended recipient of the Audit and user of the reported information;
 - b) the audited body is responsible for reporting its compliance with its Licence Obligations; and
 - c) the Auditor is responsible for independently forming a view as to whether the Licensee has met its licensing Obligations, and the primary duty of the Auditor and any subcontractor is to the commission.
- 3.1.3. The standard for the commission's baseline and thematic regulatory Audits, *ASAE 3402 Assurance Reports on Controls at a Service Organisation* states that the Auditor is to express a conclusion on compliance with requirements, as measured by suitable criteria. The criteria for the purpose of an Audit conducted under the guideline are the following:
- a) all relevant aspects of the applicable energy Licences;
 - b) all relevant aspects of the *Electricity Industry Act 2000* and the *Gas Industry Act 2001*; and
 - c) all relevant aspects of Orders in Council, industry codes, standards, rules, guidelines and procedures applicable to the Licensee under a Licence or a relevant Act.
- 3.1.4. Regulatory Audits will generally include an assessment of a Licensee's compliance framework against *AS 3806–2006 Australian Standard Compliance Programs*.

3.2. Identifying risk, and determining type, frequency and timing of an Audit

- 3.2.1. The commission will conduct a Risk Assessment in order to determine:

- a) whether a Licensee will be the subject of an Audit;
- b) the Obligations to be included in the Audit scope;
- c) the type of Audit to be performed; and
- d) the frequency of any Audit.

3.2.2. In conducting a Risk Assessment the commission will consider the risks and consequences of non-compliance and the factors in clause 3.2.3. The commission will give priority to auditing high risk Obligations and Licensees, once identified. Obligations and Licensees identified as low or medium risk may be the subject of an Audit less frequently than high risk Obligations and Licensee.

3.2.3. In conducting a Risk Assessment, the commission will consider a range of factors relevant to the Licensee and their Obligations. Where relevant, these include:

- a) cost to customers or the public;
- b) danger to public health or safety;
- c) damage to property;
- d) loss or reduction of energy supply or customer service;
- e) environmental damage;
- f) the compliance history of the Licensee;
- g) Licensee's likely or known non-compliance with Licence conditions, including assessment of previous Audit results;
- h) information from other industry departments and agencies;
- i) adverse public reaction;
- j) threat to actual or comparative competition (e.g. making invalid comparisons between Licensees' performance); and
- k) any other matter considered relevant by the commission.

3.2.4. The frequency and timing of an Audit is at the sole discretion of the commission. The commission may require that a Licensee is subject to an Audit at least once every three years.

3.2.5. Any risks self-identified by the Licensee in addition to those considered by the commission should be communicated to both the commission and the Auditor, prior to the Audit scope being finalised. The commission will then determine whether its priorities require these obligations to be included in the scope of the Audit.

3.2.6. Further assessment of a Licensee's relevant Obligations will be used by the commission, in consultation with the Licensees, to identify the minimum set of obligations to be audited in accordance with clause 5.5.

4. APPOINTING THE AUDITOR

4.1. Licence condition to appoint an Auditor

- 4.1.1. The energy Licence conditions require a Licensee to appoint an Auditor at the commission's request. The Licensee must also comply with relevant aspects of this guideline or any other relevant guideline.
- 4.1.2. The Auditor and the Licensee must enter into a tripartite deed (**Audit Deed**) with the commission in the form of the commission's standard Audit Deed, or in such other form as the commission may require.
- 4.1.3. The primary duty of care the Auditor and any Subcontractor is to the commission, not to the Licensee.

4.2. Empanelment of Auditors

- 4.2.1. The commission may appoint or remove Auditors from the panel in accordance with '*Joining the Audit Panel*' and with clause 9.1.8 of this guideline.

4.3. Licensees to appoint an Auditor from the panel

- 4.3.1. A Licensee must select an Auditor from the panel when the commission requests a Licensee to appoint an Auditor as provided in clause 4.1.1. In exceptional circumstances, the commission may agree to the appointment of a suitably qualified non-panel Auditor.
- 4.3.2. The appointment of an Auditor is subject to a maximum term of three consecutive audits. Licensees must appoint a new Auditor once the maximum number of audits has been reached.

4.4. The commission's approval

- 4.4.1. A Licensee must obtain the commission's in-principle approval of the Auditor selected from the panel of approved Auditors for the purposes of the guideline having regard to the factors specified in clause 9.1.2.
- 4.4.2. Final approval will be conditional on satisfactory execution of the Audit Deed. If an Audit Deed is terminated, any approval of the relevant Auditor lapses.
- 4.4.3. The commission may reject the nomination, if for any reason it is dissatisfied with the nomination.

5. APPROVING THE AUDIT SCOPE

5.1. Type of Audit

- 5.1.1. In response to its risk assessment, the commission may require, in consultation with the Licensee, one or more of the following types of Audits to be performed:
- a) Baseline Audit to provide a baseline assessment of key Licence obligations. Where a Licensee has held a Licence for 12 months or less, a modified version of the Baseline Audit may be performed;
 - b) Thematic Audit to provide an extensive assessment of selected obligations applicable to industry issue(s); and
 - c) Tailored Audit to provide an extensive assessment of selected obligations applicable to a specific Licensee.
- 5.1.2. The commission may require an Audit to be conducted in accordance with one or more of the following standards:
- a) *Standard on Assurance Engagements ASAE 3402 Assurance Reports on Controls at a Service Organisation – Type 1 Report;*
 - b) *Standard on Assurance Engagements ASAE 3402 Assurance Reports on Controls at a Service Organisation – Type 2 Report;* and
 - c) *Standard on Related Services ASRS 4400 Agreed-Upon Procedures Engagements to Report Factual Findings.*
- 5.1.3. The commission may require a pulse check self-assessment to be performed. This is a light touch review used to monitor selected obligations, and to promote and encourage best practice. The review will be conducted in accordance with the terms and templates specified by the commission.

5.2. Identifying regulatory obligations to be Audited

- 5.2.1. Before each Audit, the commission, in consultation with the Licensee, will review and nominate the regulatory Obligations for the Licensee which will be included in the Audit. The commission will document this as the minimum Audit scope.
- 5.2.2. The minimum audit scope will specify the:
- a) regulatory Obligations (generally identified by clause and sub-clause number), performance indicators and specific compliance issues (see 5.3) to be the subject of the Audit;

- b) audit period (see 5.4.);
- c) type of Audit (see 5.1); and
- d) details of the expected time frame for undertaking and completing the Audit, and for providing final Audit report.

5.3. Specific compliance issues

- 5.3.1. Specific compliance issues generally take the form of questions about actions that the commission considers the Licensee would need to take, in order to demonstrate adequate compliance with regulatory Obligations identified in the scope. For instance, the commission may require the Auditor to have regard to language issues, when assessing a Licensee's compliance with complaint-handling Obligations.
- 5.3.2. Where specific compliance issues have been identified for an Obligation that is included in the Audit scope, those issues must be addressed by the Auditor in its Audit Report.

5.4. Audit period

- 5.4.1. For some Obligations, Auditors will be required to assess compliance over a period of time, as well as at the time of the Audit. This is particularly important, for example, in assessing regulatory information to be published by the commission. The reliability of the information should be assessed over the period to be covered by the commission's report.
- 5.4.2. The Audit period, or periods, to be covered will be specified by the commission in the minimum Audit scope.
- 5.4.3. The commission will advise Licensees of the minimum Audit scope, as described in sections 5.1 to 5.4.

5.5. Planning

- 5.5.1. In consultation, the Licensee and the Auditor should then review the minimum Audit scope to identify the relevant staff who will be needed for interview and the records that will be required for examination and testing, and make the necessary arrangements.
- 5.5.2. The Licensee and the Auditor should also review any other high-risk Obligations relevant to those proposed for inclusion in final Audit scope.
- 5.5.3. The Licensee should then specify any additional Obligations to form part of the Audit scope. These are Obligations that the Licensee or its Auditor has identified as high risk, and that the commission has not included in its minimum Audit scope. The Licensee should highlight any change to the time frame for completing the Audit that the

Licensee and Auditor consider necessary. The Licensee should then submit its proposed Audit scope to the commission for approval.

- 5.5.4. In cases where the Licensee or the Auditor has not identified any high risk Obligations, the commission may request a copy of the risk assessment prepared by the Licensee or the Auditor for review.
- 5.5.5. If a Licensee's Audit proposal meets the commission's minimum requirements, the commission will approve the proposal.

5.6. Briefing the Auditor

- 5.6.1. When the Auditor has been appointed and the Audit scope has been approved, the commission will brief the Audit team in the presence of the Licensee, before the Audit commencement to make sure that the commission's requirements are clearly understood.
- 5.6.2. Licensees must give the Auditor a copy of the approved audit scope at or before the briefing.
- 5.6.3. The Auditor will provide regular updates to the commission on the progress of the Audits as and when required by the commission.

6. CONDUCTING THE AUDIT

6.1. Audit methodology

- 6.1.1. The methodology employed must be based on the general principles of the *Standard on Assurance Engagements ASAE 3402 Assurance Report on Controls at a Service Organisation* and *ASRS 4400 Agreed-Upon Procedures Engagements to Report Factual Findings* as applicable, and the generic minimum requirements specified in item 1 of schedule 2 of the Audit Deed or any other requirements specified by the commission.
- 6.1.2. The commission may set out its expectations of minimum requirements for the conduct of Audits.

6.2. Reliance on other work

- 6.2.1. The commission seeks to avoid duplication of effort and repetition of audit work previously performed. Therefore the Auditor is expected to make use of other recent independent audits, where relevant to issues in the scope of the current Audit. The extent to which these independent Audit findings may be used is a matter for the Auditor's professional judgement having regard to their relevance to the Audit scope and confidence levels required for the type of Audit requested in clause 5.1.
- 6.2.2. The Auditor must notify the commission of their intent to rely on other work, the details of which, must be provided upon request
- 6.2.3. Other audit reports, if provided by the Licensee to the Auditor at the planning stage, may not eliminate Obligations from the scope of the current Audit but may reduce the extent of work needed to provide the commission with the level of assurance it requires.
- 6.2.4. The Audit Report should document the Auditor's reliance, if any, on others' work and on Licensee management's representations.

7. ASSESSING AND REPORTING ON COMPLIANCE

7.1. Standard compliance grades

- 7.1.1. It is important that compliance is rated using standard grades, thereby maximising the comparability of the results reported to the commission.
- 7.1.2. The commission uses a specific grading system in order to assess compliance. Auditors must use the prescribed standard grades for the regulatory information and compliance with Licence Obligations subject to Audit in accordance with *Standard on Assurance Engagements ASAE 3402 Assurance Report on Controls at a Service Organisation*.
- 7.1.3. Auditors must report compliance grading in the findings register template specified by the commission (see 7.11).

7.2. Compliance performance indicators and assessments

- 7.2.1. Where Audit engagements require review of compliance performance indicators, the grades used to assess regulatory information focus on the reliability of the Licensee's procedures for generating the information and the quality of the data produced by those procedures.
- 7.2.2. The Auditor must determine the data quality by having regard to:
 - a) the systems and processes used to generate the data;
 - b) the methods used, if any, to extrapolate or estimate data; and
 - c) the way in which reports are prepared and the extent to which reports are communicated, reviewed, approved, and acted upon.
- 7.2.3. The Auditor must assign a two-part grade (e.g. B2, DX) to each category of information in the Audit scope as follows:

Grade Reliability assessment

- A** All data is based on robust information systems that support the compliance program, and documented policies, practices and procedures, which are:
- updated as required and endorsed by the licensee’s management;
 - consistent with the commission’s information specifications;
 - communicated and readily available to all staff; and
 - fully understood and followed by staff to support compliance outcomes and acted upon at all levels of the organisation, including the Board and senior executive management.
- B** Most data conforms with Grade A. Data integrity is compromised due to minor compliance failures and inadequate controls over information systems. For example, a minority of data may be based on:
- information specifications that are different to those published by or reported to the commission;
 - outdated policies and procedures;
 - inconsistent compliance practices;
 - minor deviations from documented operating policies and procedures;
 - policies and procedures that are not properly communicated or that are misunderstood by staff;
 - system upgrades and changes that have resulted in loss of data; or
 - estimation or extrapolation of data that conforms with Grade A.
- C** In many cases, but not all, data does not conform with Grade A. Data integrity is significantly compromised due to compliance failures and lack of controls over information systems. For example, the majority of the data may be based on:
- information specifications that are materially different to those published by or reported to the commission;
 - policies and procedures that are not documented and endorsed by the licensee’s management;
 - documented operating policies and procedures that are significantly out of date, incomplete or not followed;
 - policies and procedures that are not communicated to staff or fully understood;
 - processes that do not retain source documentation for verification purposes;
 - processes that increase the risk of manual intervention or data that is manually managed outside a major system; or
 - estimation or extrapolation of data that conforms with Grade A or B.
- D** Data is not relevant, suitable or adequate to form an objective determination regarding its quality.

Grade	Accuracy
1	± 1% Where a performance indicator is relevant to operations in principle but no data exists and none is reported in the audit period, this should be graded 1.
2	± 5%
3	± 10%
4	± 25%
5	± 50%
6	± 100%
X	For small samples where an error would be more than 100%, or data that is not relevant, suitable or adequate.

7.2.4. Where Audit engagements do not require review of compliance performance indicators, the Auditor must assess compliance using the following grading system as outlined in 7.3.




7.3. Step one

7.3.1. To assess if compliance is reliable and demonstrable, the following control areas may be considered:




- a) Policies / procedures;
- b) Skills / training;
- c) Systems / maintenance;
- d) Monitoring / feedback;
- e) Culture / practices.

7.3.2. A traffic light grading system must be used to indicate the adequacy and effectiveness of each control relating to each compliance Obligation. The adequacy of control grading will require professional judgment while the effectiveness of control grading will follow, at a minimum, the sampling methodology specified in Audit scope. The Auditor should consider the definitions outlined below when grading.

Grading adequacy of process and control

Grade	Description	Adequacy definition
	Inadequate	Significant to full revision or development of processes and controls is required for the control objective and ultimately the compliance Obligation to be met.
	Partially Adequate / Requires Improvement	Revision of some key processes and controls is required for the control objective and ultimately the compliance obligation / Improvement opportunities exist in some key processes and controls for the control objective and ultimately the compliance Obligation to be met.
	Adequate	Minimal or no action is required for the control objective and ultimately the compliance Obligation to be met.

Grading effectiveness of process and control

Grade	Description	Effectiveness definition
	Ineffective	The requirements of the control objective have not been met, or adequate, relevant and suitable information to form an objective determination on effectiveness was not available to demonstrate compliance. Findings noted are considered material in nature and require urgent remedial action.
	Partially effective / requires improvement	Key requirements of the control objective have been met but only minor achievements in compliance have been demonstrated. Findings noted are considered significant and require substantial effort to correct.
	Effective	Most requirements of the control objective have been met with some minor failures or breaches. Findings noted are considered minor and require routine efforts to correct in the normal course of business.




7.4. Step two

- 7.4.1. A two dimensional compliance matrix must be used to indicate overall compliance with an Obligation. The overall compliance grading will combine the two control grades as determined in clause 7.1 to give a resulting compliance grade as outlined below.

Compliance Matrix

		Adequacy of Control		
		<i>Inadequate</i>	<i>Partially Adequate / Requires Improvement</i>	<i>Adequate</i>
Effectiveness of Control	<i>Ineffective</i>			
	<i>Partially Effective / Requires Improvement</i>			
	<i>Effective</i>			

Overall compliance grade

Grade	Description
	Non-Compliant
	Partially Compliant
	Compliant

7.5. Step three

7.5.1. The Auditor must use the following criteria to classify each overall compliance grade:

- a) Where the traffic light grading combination for adequacy and effectiveness contains at least one red, the overall compliance grade is non-compliant.
- b) Where the traffic light grading combination for adequacy and effectiveness is green and yellow, the overall compliance grade is partially compliant.
- c) Where the Licensee's controls are effective and adequate, the overall compliance grade is compliant.

7.6. Step four

7.6.1. Auditors must use their professional judgment to arrive at a conclusion for all compliance grades.

7.7. Current and period compliance

7.7.1. Unless otherwise stated in the scope, the Auditor is required to assign grades:

- a) for all Obligations, current compliance at the time of the Audit; and
- b) for specified Obligations, compliance over the Audit period.

The grade for current compliance and compliance over the period can be taken as being the same if the Auditor has identified no significant changes to procedures or systems over the Audit period. If significant change has been identified, however, the Auditor must also assign a grade to represent compliance over the Audit period.

7.7.2. For example, if a particular data set was of poor quality for half the Audit period and, following procedure and system changes, was more reliable and accurate for the remainder of the period, compliance over the period should be assessed as lower than current compliance.

7.8. Level of confidence

7.8.1. Compliance grades should be assessed by the Auditor to the level of confidence required for the type of Audit requested in clause 5.1, based on statistical methods where possible and judgement in other cases.

7.9. Continuous improvement

7.9.1. The Auditor is required to review the Licensee's Audit response, with regards to the adequacy and effectiveness of action plans and the schedule for their completion to address compliance issues. This review will also include an assessment of the Licensee's continuous improvement activities to ensure the sustainability of its compliance program

7.10. Signed statement

7.7.2. The Audit Report must include a statement signed by the Auditor which states:

- a) that the Auditor has complied with the guideline and the Audit Deed in conducting the Audit, making Audit findings and preparing the Audit Report;
- b) that the Auditor was responsible for seeking and assessing information, and the Licensee for providing the information and related assurances of its reliability;
- c) that the Audit findings reflect the Audit level of assurance required for the type of Audit requested in clause 5.1.; and
- d) the Auditor's professional opinion on overall assessment of compliance. for reports required to be prepared in accordance with *Standard on Assurance Engagements ASAE 3402 Assurance Reports on Controls at a Service Organisation*.

7.11. Findings register

7.11.1. Detailed information on findings beyond those required in Audit Reports of the *Standard on Assurance Engagements ASAE 3402 Assurance Report on Controls at a Service Organisation* must be reported separately to the commission in the findings register template specified by the commission. The purpose of the findings register is to provide details on findings, including compliance grading, compliance classifications and where applicable, recommendations and management comments.

7.12. Audit Report

7.12.1. The purpose of the Audit Report is to provide a context and conclusion for the Audit. The Audit Report should comply with the Audit Report template specified by the commission and meet the standard level of Audit Report requirements in clause 9.1.3 d).

7.12.2. The Auditor must prepare the audit report to meet the requirements of the guideline and with reference to the reporting standards set by *Standard on Assurance Engagements ASAE 3100 Compliance Engagements*, *Standard on Assurance Engagements ASAE 3402 Assurance Reports on Controls at a Service Organisation* and *Standard on Related Services ASRS 4400 Agreed-Upon Procedures Engagements to Report Factual Findings*.

7.13. Draft deliverables

7.13.1. From time to time and with prior written notice to the Auditor and the Licensee, the commission may require draft findings registers (see 7.11), Audit Reports or briefings to be provided.

7.13.2. The Auditor must provide to the commission an electronic copy of the draft findings register (see 7.11) and Audit Report on the same day that it is provided to the

Licensee, and at least 15 business days before the closing meeting with the commission, if requested to do so by the commission . This allows the commission an opportunity to consider the significance of the Audit Report in a timely way.

- 7.13.3. The commission does not intend to publish the draft deliverables but may publish any information it deems appropriate if the Auditor fails to provide a final findings register (see 7.11) and Audit Report within the required timeframe.

7.14. Reporting procedures

- 7.14.1. The Licensee must make sure that its CEO or a delegated officer authorises the management comments in the Audit Report (as required for reports prepared in accordance with *Standard on Assurance Engagements ISAE 3402 Assurance Reports on Controls at a Service Organisation*) or in the Licensee's letter of response to breaches identified (for Audits prepared in accordance with *Standard on Related Services ASRS 4400 Agreed-Upon Procedures Engagements to Report Factual Findings*) and forwards it to the commission at least five days before the closing meeting with the commission. This allows the Licensee an opportunity to:

- e) assess whether the Audit Report accurately reflects the Licensee's performance; and
- f) begin taking corrective action if non-compliance has been identified. Management comments on corrective action should address all aspects of the non-compliance identified including:
 - (a) Whether management agree or disagree with the non-compliance identified;
 - (b) Where management agrees with the non-compliance identified, describe the correction action(s) that will be taken in response to the non-compliance to mitigate the risk identified;
 - (c) Where management disagrees with the non-compliance identified, explain why and describe the alternate corrective action(s) that will be taken in response to mitigate the risk identified; and
 - (d) For all corrective actions described, indicate the targeted completion date and the title of the accountable individual.

- 7.14.2. The Licensee must not, however:

- a) require or seek changes to be made to the Audit Report that conflict with the Auditor's professional judgement and its primary responsibility to the commission; this includes requiring a change to be made that would, in effect, remove or obscure any adverse finding of the Auditor;
- b) unreasonably withhold payment or terminate the Audit contract over a disputed Audit finding; or
- c) significantly delay the forwarding of the Audit Report to the commission.

7.14.3. A request for extension must be made in writing by the licensee to the commission and is subject to the commission's approval.

7.15. Copy of final deliverables

7.14.4. The Licensee must provide to the commission:

- a) As specified by the commission, either a hard copy and/or an electronic copy (in PDF form to allow publication on the commission's website) of the findings register (see 7.11), Audit Report and letter of response to any breaches identified at least five business days before the closing meeting with the commission; and
- b) a copy of each publicly available report, record or document on which the auditor has relied upon in arriving at a finding in the audit report promptly after being requested by the commission to do so.

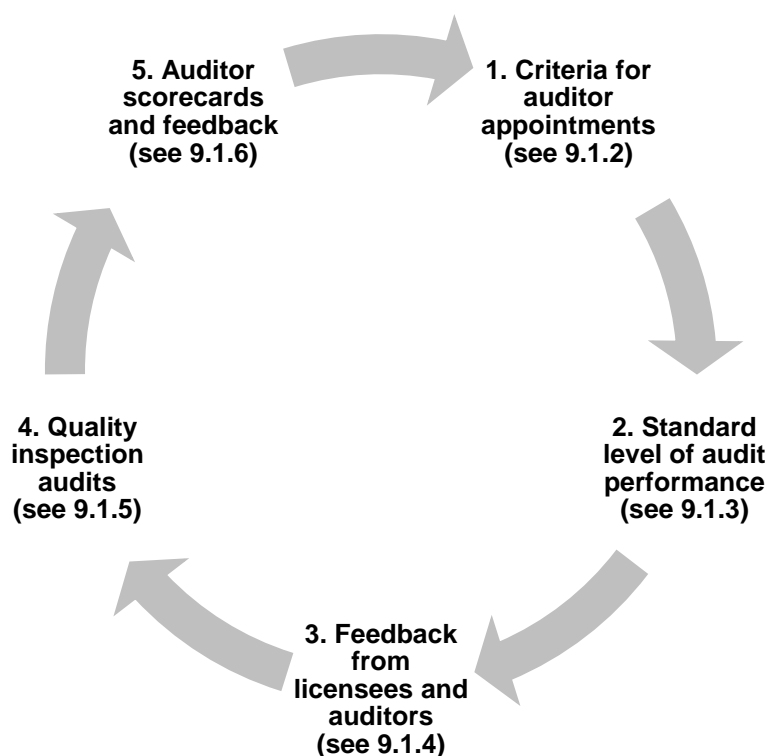
8. RESPONDING TO THE AUDIT

- 8.1.1. The Licensee must make sure that its Board or a delegated officer considers the Audit Report as soon as possible after it is received.
- 8.1.2. In addition to its obligation under clause 8.1.1 of the guideline, within 30 business days of receiving the final Audit Report, the Licensee must provide to the commission a written statement from management as specified in clause 7.14.1.
- 8.1.3. In response to an Audit Report, the commission may (without limiting its powers and rights):
- a) obtain and analyse the Auditor's record of its contacts with the Licensee. For example, to obtain more details of reported non-compliance, or to investigate whether significant changes have been made to drafts of the Audit Report;
 - b) require further Auditing or re-performance to be undertaken as specified in clause 9.1.3 e).
 - c) arrange a quality inspection audit to be conducted as specified in clause 9.1.5.
 - d) require termination of any contract by which the Auditor was engaged to conduct the relevant Audit;
- 8.1.4. Where the Audit identifies non-compliance, the commission may (without limiting its powers and rights):
- a) require action to be taken by a Licensee to address any non-compliance, or to mitigate the risk or consequences of future non-compliance upon review of provisions of regulatory instruments that appear to be unclear, inadequate, excessive or trivial; or
 - b) exercise the enforcement powers available to it under relevant legislation
- 8.1.5. The commission will report publicly and comment on the results of any Audit undertaken (and the steps, if any, required to achieve compliance). This may include reporting the results of the Audit as part of its performance reporting function. A summary of communication procedures is outlined below. The commission reserves the right to re-consider the time frame. This may be extended if the complexity or the difficulty of an Audit so requires, or relevant functions have been outsourced, at the commission's discretion and in consultation with the Auditor and the Licensee subject to Audit.

Communication procedures	Primary participants	Time frame
Planning		No more than 30 days between issue of indicative scope to engagement of Auditor and issue of final Audit scope
Engagement of auditor	Licensee Auditor	Within 15 business days after the indicative Audit scope is issued
Scope preparation session	commission, Licensee Auditor	Within 25 business days of when the commission issues the indicative scope
Finalisation of scope	commission, Licensee Auditor	No more than 30 days after the indicative Audit scope is issued
Fieldwork and Reporting		No more than 90 days between start of Audit fieldwork to issue of final Audit Report
Start of audit fieldwork	Licensee Auditor	The date when the Auditor commences its review on the Licensee's premises, or on a date agreed with the commission
Frequency of status updates to the commission	Auditor, commission	Based on the nature or complexity of the Audit, as specified by the commission
Audit de-briefing	Auditor, commission	May be required by the commission depending on the status updates and nature or complexity of the Audit
Submission of draft deliverables	Auditor	At least 15 business days before the closing meeting with the commission, on a date specified in the Audit scope
Submission of final deliverables	Auditor	At least five business days before the closing meeting with the commission, on a date specified in the Audit scope
Closing meeting	commission, Licensee Auditor	No more than 90 days from the start of the Audit fieldwork, or on a date agreed with the commission
Responding to audits	Licensee	Within 30 business days after the final deliverables are issued

9. Quality assurance framework

9.1.1. To ensure the quality of Audits performed by Auditors, the commission has a quality assurance framework incorporating the following elements:



9.1.2 The commission will review and approve Audit nominations for an engagement having regard to:

- the maximum term of three consecutive audits for an Audit relationship;
- work that the firm has performed for the Licensee in the previous two years, and work that the firm is currently doing for the Licensee or has bid for;
- Auditor's past performance on Audits with other Licensees as applicable;
- Auditor's scorecard results (see 9.1.6.);
- number of Audits the Auditor has concurrently with other Licensees;
- advice of any potential conflict of interest and, if so, the way in which the potential conflict of interest is proposed to be managed; and
- any other information on the Auditor's appointment.

9.1.3. The commission will monitor, assess and uphold the quality performance of an Audit by ensuring:

- key performance indicators in Audit Deeds are met;

- b) weekly status updates are provided by Auditors, including all requested details in a format specified by the commission;
- c) a completed quality and assurance checklist is submitted by the Auditor in the format specified by the commission; and
- d) only Audit Reports that comply with the standard specified by the commission are accepted. Auditors must ensure Audit Reports meet the following standard requirements of the commission:
 - 1. prepared with professional rigour and in accordance with professional Audit standards;
 - 2. concise and clear in its findings, addressing the Audit scope;
 - 3. written in plain English, avoiding industry jargon;
 - 4. evidence based, substantiating findings; and
 - 5. free from errors.
- e) further Audit or re-performance is undertaken (whether by the relevant Auditor or another) where the commission considers the Audit Report is or may be unsatisfactory in a material respect. For example, where the commission:
 - 1. has independent information contradicting an assessment made by the Auditor.
 - 2. is not satisfied that the individual Audit provide adequate assurance that the Audits of the Licensee produce results that are validly comparable; or
 - 3. requires better information on which to assess whether compliance or other action should be taken.

The commission may require that the licensee arrange for another Auditor approved by the commission to undertake any such further Audit.

- 9.1.4. The commission will assess the feedback obtained from Licensees on Auditors and vice versa.
- 9.1.5. The commission may engage a provider independent of the Audit panel to conduct quality inspection Audits on a sample of active Auditors of preceding years. This may escalate to a deep dive review, including re-performance of the Audit if the quality inspection Audit indicates quality issues.
- 9.1.6. The commission will use its discretion to rate the performance of Auditors using score cards and provide Auditors with feedback on the result. A poor score card result may preclude an Auditor from certain types of Audits, and/or removal from the Audit panel.
- 9.1.7. The commission will assess Auditor performance through data sources available to them in addition to the quality assurance framework above.

- 9.1.8. In accordance with 'Joining the Audit Panel', any failure by the Auditor to follow this Guideline or comply with any obligation owed to the Commission under the Audit Deed when performing an audit may result in removal from the Audit panel.

10. AMENDMENTS

- 10.1.1. The commission may amend or revoke the guideline.
- 10.1.2. The commission will not make material amendments to the guideline until Licensees and other stakeholders have had an opportunity to comment on the nature of any proposal to amend or revoke the guideline and those comments have been considered, in accordance with the commission's Charter of Consultation and Regulatory Practice.