Auditor Protocol

Guidelines

25 October 2016

Version control

Version	Date amended	Comments
1	25 October 2016	Draft for consultation

Foreword

This document sets out the auditor protocol that Authority-approved auditors need to follow when carrying out audits under the participant audit regime (audit regime).

This document should be read in conjunction with the *Risk and Materiality Guidelines* that set out procedures that auditors must follow when planning an audit and classifying audit findings according to materiality and risk.

Contents

Tables

Figures

1 Introduction

1.1 This document sets out the auditor protocol that Authority-approved auditors must follow when carrying out audits under the audit regime.

1.2 This protocol is based on relevant requirements set out in the ISAE 3000 (NZ)[1] and is divided into two sections as follows:

(a) Section 2 covers how to conduct an audit, including:

(i) rules auditors must follow when deciding to accept or continue with an audit engagement

(ii) rules and guidelines auditors must follow when planning and performing an audit

(iii) audit reporting requirements

(iv) audit administration.

(b) Section 3 prescribes professional and ethical requirements:

(i) to identify and address threats to objectivity (including conflicts of interest)

(ii) for professional competence and due diligence requirements.

2 Audit conduct

Introduction

2.1 Audit conduct refers to the rules and framework under which the auditor approaches and carries out an audit.

2.2 The Authority may remove an auditor's approval if the auditor is materially non-compliant with any of the provisions set out in this protocol.

2.3 The Authority may require auditors to provide recommendations to mitigate participant compliance risk.

Acceptance and continuance of an audit engagement

2.4 An auditor must not accept or continue an audit engagement if any of the ethical and professional requirements set out in Section 3 are not met.

2.5 An auditor must only accept or continue an engagement if they have sufficient resources to carry out the audit.

2.6 At the time of approval and prior to the start of any audit, the auditor must declare any:

[1] The ISAE (NZ) 3000 standard for Assurance Engagements Other than Audits or Reviews of Historical Financial Information includes requirements for assurance practitioners to comply with:

(a) professional and ethical standards as prescribed by IFAC Code of Ethics for Professional Accountants or, in New Zealand, Professional and Ethical Standards: Code of Ethics for Assurance Practitioners (PES1)

(b) International Standards on Quality Control for Firms that Perform Audits and Reviews of Financial Statements, and Other Assurance Engagements (ISQC3), or in New Zealand, Professional and Ethical Standards 3: Quality Control for Firms that Perform Audits and Reviews of Financial Statements (PES3).

(a) threats to the five fundamental principles of audit best practice (see Section 3, items 3.1 and 3.2)

(b) conflicts of interest (see the section titled Identifying and addressing threats and conflicts of interest).

Audit planning

2.7 The Authority applies the *Risk and Materiality Guidelines*[2] to specify:

(a) the scope for audits[3]

(b) audit priority areas[4]

(c) materiality ratings to be used to categorise instances of non-compliance and general audit findings.

2.8 When planning an audit, the auditor must:

(a) follow the guidance set out in the Audit performance section of this document

(b) follow any relevant requirements in the *Risk and Materiality Guidelines*

(c) prior to commencing the audit, create an Audit Planning Report that sets out:

(i) the areas/obligations that the auditor intends to review/audit

(ii) the software/tools/information systems the auditor intends to review (where applicable)

(iii) the procedures the auditor intends to employ to scrutinise the above areas

(iv) the timing for undertaking audit procedures and producing audit reports

(v) a list of the auditors involved in the audit.

2.9 When planning the audit under this section (Audit planning) and carrying out the audit under the section below (Audit performance), the auditor must consider:

(a) any comments the Authority has provided on the Audit Planning Report submitted under item 2.8(c)

(b) any self-reported instances of non-compliance and relevant internal audit findings (and modify any audit procedures accordingly)

(c) any follow-up actions the auditor must undertake for any previous audit findings. For example, if the previous audit findings indicate the need for preventive, corrective, or improvement actions, the auditor must follow up to:

(i) check whether the preventive, corrective, or improvement actions have been implemented

(ii) verify the completion and effectiveness of those actions.

---

2 Refer to the *Risk and Materiality Guidelines*.

3 Scope can include operational compliance, software and IT systems review. Scope will vary depending on the risk profile of the participant being audited.

4 Focus areas relate to business processes and systems used to implement specific Code obligations. Areas can also be defined as clusters of obligations or individual obligations.

Audit performance

Audit procedures

2.10 Audit procedures refer to activities undertaken by the auditor to:

(a) assess compliance and/or detect non-compliance with the audited entity's obligations under the Code and any other relevant criteria

(b) assess and evaluate compliance risk.

2.11 Audit procedures can include, but are not limited to:

(a) sample testing of compliance and controls

(b) document reviews

(c) interviews

(d) business process walkthroughs.

2.12 The auditor must perform audit procedures in accordance with the following requirements (taking into account the *Risk and Materiality Guidelines*):

(a) Functional areas with Residual Risk Rating of **High**:

(i) undertake thorough compliance testing (ie, moderate-high sample sizes, test all obligations)

(ii) undertake business process walkthroughs (ie, shadowing personnel on tasks)

(iii) examine effectiveness and verify application of controls

(iv) undertake document reviews and interviews as required.

(b) Functional areas with Residual Risk Rating of **Medium**:

(i) undertake moderate compliance testing (moderate-low sample sizes, test selected obligations)

(ii) undertake business process walkthroughs for selected business processes

(iii) examine effectiveness and verify application of controls (for selected processes)

(iv) undertake document reviews and interviews as required.

(c) Functional areas with Residual Risk Rating of **Low**:

(i) undertake light compliance testing (low sample sizes, test a small number of obligations)

(ii) review controls for a small sample of selected business processes.

(iii) undertake document reviews and interviews as required.

2.13 An auditor must modify their procedures if their assessment of risk changes during the course of the audit. For example, if a particular area appears to have weaker controls than previously assumed or if material instances of non-compliance are discovered, the auditor must either increase the level of scrutiny applied in that area or provide a qualified conclusion (see paragraph 2.31 below for guidance on qualified conclusions).

Document reviews

2.14 The auditor must consider the following when conducting document reviews (eg, reviews of business process documentation/procedures, reports, electronic communications, etc):

(a) whether the information in the documents provided is:

(i) complete

(ii) correct, eg, a review of a business process document or procedure should include an assessment of compliance with the Code or other relevant criteria (eg, if the procedure is followed will it result in an outcome compliant with the Code?)

(iii) consistent (ie, the document is consistent in itself and with any related documents)

(iv) current.

(b) whether the documents being reviewed cover the audit scope and provide sufficient information to support the audit objectives.

Sampling

2.15 The auditor should conduct sample testing when it is not practical or cost effective to examine all available information in an audit.

2.16 Auditors may use either judgement-sampling or statistical sampling.

Judgement-based sampling

2.17 Judgement-based sampling relies on the knowledge, skills, and experience of the auditor.

2.18 For judgement-based sampling, the auditor should consider the following:

(a) previous audit experience

(b) previously identified key risk areas and areas for improvement

(c) representativeness of sample (ie, the extent to which the sample provides breadth and coverage of all types of items or (if relevant) material items in the population)

(d) degree of change in technology, business processes, human resources or other systems.

Statistical sampling

2.19 If statistical sampling is selected, the sampling plan should be based on the audit objectives and the known characteristics of the population from which the sample will be drawn.

2.20 Statistical sampling uses a sample selection process (based on probability theory) to:

(a) determine the sample size

(b) project sample results to the population or stratum sampled

(c) measure sampling risk: the level of sampling risk is an important consideration and represents the tolerable error level (eg, a sampling risk of 5% means the auditor is willing to accept the risk that 5 out every 100 samples examined will not reflect the actual values that would be seen if the entire population was examined).

2.21 Methods of selecting samples include use of:

(a) random selection (applied through random number generators)

(b) systematic selection in which the number of sampling units in the population is divided by the sample size to give a sampling interval (eg, 25), and having determined a starting point within the first 25, each 25th sampling unit thereafter is selected

(c) haphazard selection, in which the auditor selects the sample without following a structured technique (so as to eliminate bias).

2.22 When statistical sampling is used, an auditor must appropriately document the work performed including the description of the population sampled, sampling criteria, statistical parameters used (eg, sampling risk), sampling selection methods used, sample sizes used, and the results obtained.

2.23 Further audit sampling guidelines and information is provided in Appendix A.

Obtaining evidence

2.24 The auditor must consider whether they have requested adequate information as evidence. Particularly, the auditor must consider whether the evidence is:

(a) Relevant: Does it enable them to form an unqualified conclusion with respect to the participant's compliance?

(b) Reliable: Is the evidence accurate, true and untampered with?

(c) Sufficient: Does the evidence provide adequate assurance (ie, has enough evidence been requested and/or is additional information or data required)?.

2.25 If the auditor notes any inconsistencies in the evidence requested, or doubts the reliability of the evidence requested, the auditor must modify his or her procedures accordingly (eg, by requesting different information, increasing the sample size, or interviewing relevant personnel to understand how the evidence has been produced, etc).

Evaluating instances of non-compliance

2.26 If the auditor suspects instances of non-compliance, the auditor must investigate further to determine whether it is a genuine non-compliance.

2.27 For all confirmed instances of non-compliance (including self-reported) the auditor must:

(a) investigate the circumstances and cause of the non-compliance and any remedial measures (existing or planned) to mitigate the risk of the non-compliance recurring

(b) evaluate the non-compliance with respect to the materiality levels prescribed by the Authority under the Audit planning, section of this document, item 2.7(c).

Forming an audit conclusion

2.28 The auditor must form a conclusion or view about:

(a) the extent to which the participant (being audited) is compliant with its Code obligations

(b) the adequacy of the participant's business processes, procedures, systems, and controls to manage its compliance risk.

2.29 When forming a conclusion with respect to paragraph 2.28(a) and 2.28(b) above, the auditor must evaluate the appropriateness and sufficiency of evidence requested and, if necessary, request further information.

2.30 The auditor must provide an unqualified conclusion if they are satisfied that the participant being audited has complied with its obligations.

2.31 The auditor must provide a qualified conclusion if:

(a) there are instances of non-compliance; or

(b) a scope limitation exists, so that the auditor is unable to form a view about the level of compliance as a result of (but not limited to) the following:

(i) the participant is unable or unwilling to provide the evidence (data, information, or access to business processes/systems)

(ii) the participant or other relevant party has placed a limitation on the scope of audit activities to be performed

(iii) the nature of the evidence is such that it does not enable the auditor to fully assess the level of compliance

(iv) the auditor is unable to evaluate an instance of non-compliance or other audit finding with respect to the materiality ratings prescribed by the Authority under the Audit planning, section of this document, paragraph 2.7(c).

Reporting of audit findings

2.32 The auditor must submit to the Authority an audit report that meets the requirements set out in this section.

2.33 The audit report must include a clear expression of the auditor's conclusion as formed in the Audit performance, section of this document, paragraph 2.28. The auditor must follow the language guidelines prescribed by the Authority with respect to unqualified[5] and qualified[6] conclusions/opinions.

2.34 Audit reports must contain the following information:

(a) The name of the participant being audited.

(b) The lead auditor and all persons used to perform the audit.

(c) An informative summary of audit procedures performed: The summary does not need to be overly detailed, but should not be ambiguous. Specifically, it must contain enough information to clearly convey the following information:

[5] For example, an unqualified conclusion or opinion could be stated as, "We have not noted any incidents or issues that suggest [participant X] has not complied with their obligations under the Electricity Industry Participation Code." This language is consistent with a negative assurance opinion.

[6] For example, a qualified conclusion or opinion could be stated as:

i. Where instances of non-compliance have been noted: "With the exception of the incidents noted in Section [X], we have not noted any incidents or issues that suggest [participant X] has not complied with their obligations under the Electricity Industry Participation Code." This language is consistent with a negative assurance opinion.

ii. Where the auditor has been unable to obtain sufficient or reliable evidence: "Note further that due to the issues stated in Section [X], we are not able to form a view with respect to [participant X's] compliance with obligation A, B, and C."

(i) obligations that have been tested/reviewed

(ii) business processes/procedures and systems that have been reviewed

(iii) nature of audit procedures performed in the areas above (eg, compliance testing, business process walkthroughs, and documentation reviews, etc)

(iv) timing of the audit procedures

(v) extent to which information was made available to the auditor.

(d) A summary of findings that, subject to paragraph 2.31(b)(iv), must be presented as follows:

(i) Instances of non-compliance must be categorised in accordance with the materiality ratings prescribed by the Authority under the Audit planning, section of this document, paragraph 2.7(c). For further details on how instances of non-compliance should be reported, refer to Appendix B.

(ii) General audit findings (or recommendations) must also be categorised in accordance with the materiality ratings prescribed by the Authority under the Audit planning, section in this document, paragraph 2.7(c).

(iii) If the Authority has requested proposed measures to address audit findings, a summary of recommended measures.

2.35 The Code sets out the process that must be followed for each audit. Specifically, the Code requires:

(a) the auditor to provide the participant with a draft audit report detailing the provisional findings of the audit

(b) the auditor to give the participant a reasonable opportunity to comment on the draft audit report

(c) the auditor to consider any comments it receives from the participant about the draft audit report

(d) the auditor to include the following in the final audit report:

(i) any conditions the auditor considers the participant must satisfy for the participant to comply with the Code, and any action the participant has taken in respect of those conditions

(ii) a list of all agents the participant has delegated its Code obligations to (if any)

(iii) the participant’s comments (if any) on the draft audit report

(iv) a summary that specifies:

- the date of the audit report
- the name of the audited participant or agent
- the scope of the audit
- whether the audit established that the processes and procedures comply with the Code
- the auditor's name.

(e) if the Authority certifies a participant under the Code, the participant must provide the finalised audit report to the Authority as part of its application for certification at least two months prior to certification being required or the expiry of certification.

2.36 The Authority will publicise:

(a) a copy of the audit report

(b) the participant's compliance plan (if any)

(c) the date of the next audit.

Audit administration

2.37 For each audit engagement, the auditor shall maintain an audit trail thorough enough to understand the nature, timing, and extent of procedures performed and significant matters raised.

2.38 This must include (but is not limited to):

(a) minutes of all meetings and interviews

(b) written representations, eg, if a participant makes an assertion with respect to their compliance, use of controls, business processes/systems used to implement obligations, etc, the auditor must ensure that assertion is confirmed in writing

(c) files, documents, and data that contain proof of audit procedures performed

(d) electronic communications between the auditor, the Authority, and the participant being audited.

2.39 The auditor must retain the above documentation for a period of no less than three years.

3 Professional and ethical requirements

Fundamental principles of audit best practice

3.1 Auditors must comply with the following five fundamental principles of audit best practice:

(a) integrity: to be straightforward and honest

(b) objectivity: to not allow bias, conflict of interest, or undue influence override professional judgement

(c) professional competence and due care: to maintain knowledge and skill at a level necessary to competently undertake the relevant audit

(d) confidentiality: to respect confidentiality of information acquired in the course of audits and not disclose such information to third parties without proper authority (unless there is a legal/regulatory reason to do so)

(e) professional behaviour: to be compliant with relevant laws and regulations and not act in a manner that discredits the auditor’s profession.

Identifying and addressing threats and conflicts of interest

3.2 Auditors must maintain appropriate policies and procedures to enable them to identify and mitigate the following threats and conflicts:

(a) self-interest threats, eg:

(i) if an auditor has financial interest in the audited participant's organisation

(ii) if an auditor has a relationship with a person of influence in the audited participant's organisation

(b) if the audited participant's business comprises a large proportion of the auditor's revenue.

(c) self-review threats, eg, if an auditor has to review or audit a process/document/system of controls or other system that they have been involved in designing and/or implementing

(d) advocacy threats, eg, if an auditor promotes the audited participant's position to the point that the auditor's objectivity is compromised

(e) familiarity threats, eg, if a long-standing or close relationship with a client causes an auditor to be overly sympathetic so that their objectivity is compromised.

(f) intimidation threats, eg:

(i) if an auditor is deterred from acting objectively because of actual or perceived pressures, including attempts by the audited participant to exercise undue influence over the auditor

(ii) if the audited participant's business comprises a large proportion of the auditor's revenue.

(g) Conflicts of interest: This can arise where the auditor undertakes an engagement for two or more parties who interests with respect to the relevant matter are in conflict (eg, if the auditor is auditing two market participants, and providing an adverse opinion for one of the entities is aligned with the interests of the second audited party; this scenario can arise where the compliance risks of two organisations are related or dependent).

3.3 If an auditor identifies a threat or conflict (as described in paragraph 3.2 above), the auditor must immediately:

(a) declare that threat or conflict to the Authority

(b) specify mitigation measures that the auditor intends to employ to eliminate or reduce (to acceptable levels) the threat or conflict.

3.4 If an auditor is unsure whether a specific situation is a threat or conflict of interest, the auditor should discuss the situation with the Authority.

3.5 Subject to the information provided in paragraph 3.3 above, the Authority may remove the auditor from an audit engagement or remove the auditor's Authority approval.

3.6 On the Authority's request at the time of auditor appointment, and any time after that, the auditor must disclose the policies, procedures and systems used to identify and address the threats and conflicts described in paragraph 3.2 above.

Professional competence and due diligence requirements

Knowledge and skills of auditors

3.7 Auditors must ensure they maintain their skills and knowledge at a level that enables them to conduct audits diligently, robustly, and in accordance with this protocol.

3.8 Auditors must ensure all personnel on audit teams possess the requisite skills, knowledge, and practical experience to conduct audits diligently, robustly, and in accordance with this protocol.

3.9 Auditors are required to have knowledge and skills in the following areas:

(a) audit principles, procedures, and methods that enable the auditor to:

(i) apply audit procedures

(ii) plan and organise their work effectively and efficiently

(iii) prioritise and focus audit effort, and categorise audit findings based on risk and materiality taking into the account the *Risk and Materiality Guidelines*

(iv) collect information via effective interviewing, listening, and observing and via reviewing documents, records, and data

(v) understand the appropriateness and implications of using sampling techniques for auditing

(vi) verifying the relevance, reliability, completeness, and sufficiency of information collected

(vii) assess factors that may affect the reliability of audit findings and conclusions

(viii) maintain confidentiality and security of information

(ix) communicate effectively (verbally and in writing)

(x) document audit findings and prepare appropriate audit reports.

(b) risk management principles so that the auditor can apply the *Risk and Materiality Guidelines*.

(c) organisational context (with respect to the organisation of the audited entity), including:

(i) governance, size, and structure

(ii) general business and management concepts and processes

(iii) cultural and social aspects of the audited entity.

(d) Code and other regulatory obligations relevant to the audited entity (in particular, auditors should possess a good understanding of Parts 1, 10, 11, 15 and 16A of the Code).

(e) systems (including back-office systems), processes, and procedures used by the audited entity to implement its Code obligations.

Relying on the work of others

3.10 An auditor may use suitably qualified employees or subcontractors to assist them in carrying out an audit task. However, the auditor is responsible for the accuracy and quality of the final audit.

3.11 If the lead auditor relies on the work of another auditor, the lead auditor must review the other auditor's work and assess the compliance of the participant. If the lead auditor considers that further information is required, the lead auditor must seek clarification from the relevant participant. The lead auditor's assessment should assess:

(a) the competence and experience of the auditor

(b) the independence of the auditor from the organisation and are being audited[7]

(c) whether the audit is complete and has assessed the auditable areas in sufficient detail

(d) whether the audit is accurate and represents the likely compliance status of the participant.

3.12 If the lead auditor is relying on the information contained in an audit of an agent used by the participant, the auditor needs to review the agent audit thoroughly to ensure the audit is relative to the participant and audit period. This review should include verifying that the agent audit report:

(a) applies to the period being audited (ie, it was finalised no more than seven months prior)

(b) covers functions provided by the agent that are within scope in the participant audit

3.13 In addition to reviewing the agent audit, the lead auditor should perform appropriate spot checks of outcomes to verify that the participant under audit is compliant with regards to functions performed by the agent.[8]

Auditor training and development

3.14 Auditor knowledge and skills can be acquired by, but not limited to:

(a) formal education/training and experience that contribute to the development of knowledge and skills in the businesses the auditor intends to audit

(b) training programmes that cover generic auditor knowledge and skills

(c) audit experience acquired under the supervision of an auditor in the same discipline

(d) experience in a relevant technical, managerial, or professional position

(e) other relevant training that the Authority may require auditors to undergo in accordance with paragraph 3.15.

3.15 The Authority may require auditors to arrange and undergo relevant training.

Engagement Quality Control Reviews

3.16 The Authority may require an auditor to undergo an Engagement Quality Control Review in respect of a particular audit.[9]

---

[7] See section 3.2 for list of threats and conflicts all auditors, including subcontractors will need be aware of and manage.

[8] For example, where the agent is providing a service that checks for registry discrepancies, the lead auditor should perform its own check to verify that the agent is picking up and addressing all registry discrepancies.

[9] An Engagement Quality Control Review is conducted by the Authority on the audit to form a view of the auditor's compliance with this *Auditor Protocol* and the *Risk and Materiality Guidelines*.

3.17 If the Authority subjects an audit to an Engagement Quality Control Review, the auditor must make available to the Engagement Quality Control Reviewer:

(a) all relevant audit documentation (as collated under the Audit administration, section of this document, paragraph 2.37)

(b) any other information reasonably required by the Engagement Quality Control Reviewer that is required to form a view about the auditor's compliance with this protocol.

3.18 If the Authority subjects an audit to an Engagement Quality Control Review, the Authority may seek and evaluate feedback from audited participants.

Appendix A Audit Sampling

A.1 Sampling is the detailed investigation of less than 100% of the population under audit. Sampling should be used when it is not practical to audit 100% of the population.

A.2 The quality of the conclusions the auditor makes as a result of sampling depends on the design and size of the audit sample.

Sample design and stratification

A.3 Auditors are expected to use 'judgement-based sampling'.

A.4 Judgment-based sampling is a type of non-random sample where selections are based on the opinion of an expert.

A.5 Judgement-based sampling is useful in the context of the audit regime as it allows the auditor to focus on areas of greater risk and greater impact.

A.6 It is expected the auditor will use a range of different populations (stratification) to comment on outcomes both in terms of general compliance and cases that may diverge from the normal process.

Table 1: Types of judgement-based sampling

Method of sampling	Description
Typical case	Looks at the typical examples of the population. For example: Sampling a number of new connections for the participant.
Extreme case	Looks at extreme examples from the population. For example: Instances where the participant took more than 30 days to update the registry.
Critical case	Focuses on individual cases that were dramatic or important. For example: Instances where the participant took more than 300 days to update the registry.
Diverse characteristics	Selecting a sample with a diverse range for characteristics. For example: Sampling metering installations by choosing a combination of different meter type, meter manufacturer, installer, and year of install.

Method of sampling	Description
Homogeneous	Focusses on a subgroup where the population has similar characteristics: For example: Reconciliation submissions created by new staff members or metering installations of a single meter type.

A.7 Auditors should ensure it is clear in the audit report and audit notes what types of sampling have been used as well as the details and outcome of the sampling. The results of the sampling should provide the basis for the auditor's conclusions for the participant's:

(a) compliance with the Code

(b) non-compliance and potential materiality of the breach (if any).

Sampling of controls

A.8 In the context of the audit regime, controls are the processes put in place to ensure compliance with the Code.

A.9 When auditing, the auditor needs to identify the controls that are in place and discuss the likely effectiveness of these controls in the audit report.

A.10 When sampling, the auditor should review the controls in place and determine whether:

(a) processes were followed

(b) the controls were effective in ensuring the participant complied with the Code.

Appendix B Non-compliance reporting

B.1 Auditors must record any instances of non-compliance with a provision of the Code by a participant in the audit report in the form set out in the table below.

Figure 1: Format for compliance plan

Auditor completes sections in blue. Participant completes sections in yellow.

Non-compliance	Description		
With: <CLAUSE BREACHED> From/to:<DATES BREACH OCCURED>	< DESCRIPTION OF THE NON-COMPLIANCE> Potential impact: <AUDITOR TO COMPLETE> Actual impact: <AUDITOR TO COMPLETE> Audit history: <AUDITOR TO COMPLETE> Controls: <AUDITOR TO COMPLETE> Breach risk rating: <AUDITOR TO COMPLETE>		
Audit Risk Rating	Rationale for audit risk rating		
<Audit Risk Rating>	<AUDITOR TO COMPLETE>		
Actions taken to resolve the issue		Completion date	Remedial action Status
[1. Participant comments]		[2. proposed or actual completion date]	<AUDITOR TO COMPLETE>
Preventative actions taken to ensure no further issues will occur		Completion date	
[3. Participant comments]		[4. proposed or actual completion date]	

B.2 The detail required under the column headings are described further in the table below.

(a) **Non-compliance**: There are two parts to this section:

(i) **Clause breached:** The Code obligation that has not been complied with

(ii) **Dates breach occurred:** The date(s) of the non-compliance.

(b) **Description**: The description includes the following elements:

(i) **Description of the non-compliance:** The description should not seek to explain everything about the non-compliance; the body of the audit report should contain that detail. If the auditor is confident the non-compliance was deliberate, it should be noted in this field. It is not necessary to specifically investigate the intent of an audited party.

(ii) The materiality ratings, both in terms of **actual impact** and **potential impact** of the non-compliance. This reflects the Residual Risk rating of the issue underlying the finding as described in the *Risk and Materiality Guidelines* and reiterated in the table below.

- Please refer to the *Risk and Materiality Guidelines* for further detail and examples of how these ratings should be applied in practice.

- The auditor must articulate the basis for their categorisation (which should be compliant with the principles set out in the *Risk and Materiality Guidelines*).

Table 2: Audit risk ratings

Risk rating	Description
High	The issue may have major impact on settlement outcomes, on market participants and/or end-consumer if not addressed immediately. These findings require executive attention.
Medium	The issue may have a moderate impact on settlement outcomes, on market participants, and/or end-consumer if not addressed within the next six–12 months. These findings require management level attention.
Low	Issue may have a minor impact on settlement outcomes, on market participants and/or end-consumer if not addressed within 12–24 months. These findings require team management level attention.

(iii) **Audit History:** A history of previous non-compliance with the clause identified in the audit. Audit history denotes how many times this non-compliance has been identified as a non-compliance in previous:

- none
- once previously
- twice previously
- three or more times previously
- unknown.

(iv) **Controls:** Procedures the audited party has in place to remedy the situation. The auditor should comment on any controls and procedures the audited party has in place.

Table 3: Assessment of controls

Control assessment	Description
In place	Controls are in place and are effective.
Needs improvement	Controls are in place, but are not always effective in assuring compliance.

Control assessment	Description
None	There are no controls in place to ensure compliance.
Unknown	The auditor is aware that there are controls in place, but has not been able to audit them.[10]

(v) **Breach risk rating:** This is an assessment of the risk of the breach to the market, based on the Audit risk rating (Table 1) and the Level of Control.[11]

Table 4: Breach risk ratings

		Adequacy of control		
		Weak	**Moderate**	**Strong**
Audit risk rating	**High**	**9**	**6**	**3**
	Medium	**6**	**4**	**2**
	Low	**3**	**2**	**1**

(c) **Remedial action:** Comment on what, if any, remedial action has been taken by the audited party.

Table 5: Remedial action

Remedial action status	Description
Disputed	The audited participant does not believe any remedial action is required.
Investigating	The audited party is in the process of identifying the remedial actions required to address the breach.
Identified	The audited party has identified the remedial actions required to address the breach and is in the process of implementing them.[12]

[10] It is expected that an assessment of "unknown" will be used very rarely. This assessment indicates that the auditor has not been able to complete the audit. Any assessment of 'unknown' should include a clear description of why this assessment has been made and why none of the other available options are suitable.

[11] See risk and materiality guidelines for more information on assessing risk, including the audit risk rating and adequacy of control.

[12] In some instances there may be action required by other parties, such as the Authority. In these cases the remedial action may be for the participant to propose a Code amendment.

Remedial action status	Description
Cleared	The audited party has already implemented the corrective actions required to address the breach. No further action is required and the issue is fully resolved.

(d) **Actions taken to resolve the issue** (filled in by participant)**:** This is free-form text where the participant can describe the actions they have taken to resolve the identified issue. This should include a description of any action taken to ensure corrected data is provided to affected parties.

(e) **Preventative actions taken to ensure no further issues will occur** (filled in by participant)**:** This is free-form text where the participant can describe any additional controls put in place to prevent further recurrence of the issue.

(f) **Completion date:** The proposed or actual completion date for the actions taken to resolve the issue and preventative actions taken to ensure no further issues will occur.

Sample compliance plan

Figure 2: Example of completed compliance plan

Non-compliance	Description		
With: Clause 5 of Schedule 11.3 and clause 10(1)(a)(ii) of Schedule 11.3 From/to: 1 April 2016–31 March 2017	Trader did not provide final information to the losing trader within 5 business days for 15 ICPs. Five related to the standard switch process (clause 5 of Schedule 11.3) and 10 related to the switch move process (clause 10(1)(a)(ii) of Schedule 11.3). Potential impact: Medium Actual impact: Medium Audit history: Once previously Controls: Needs improvement		
Audit risk rating	Rationale for audit risk rating		
High	Has a major impact on one new retailer and timely and error free customer switching.		
Actions taken to resolve the issue		Completion date	Remedial action Status
Switch requests were from a new retailer that had not been created in our systems. As a result switch requests were not picked up. These switch requests were processed manually. Have added new retailer to system so future switch requests will be processed automatically.		16/05/2017	Investigating
Preventative actions taken to ensure no further issues will occur		Completion date	

Investigating a system change that would enable new retailer codes to be loaded automatically. Expected delivery date December 2017.	31/12/2017	
Registry exception reporting in place to identify and alert team as soon as a switch request is received from a participant code not in our system.	23/05/2017	

Appendix C Audit frequency calculation

C.1 Clause 16A.12(1)(e)(iv) requires audits to include the auditor's recommended next audit date.

C.2 The recommended next audit date is one piece of information the Authority will consider when determining the participant's next audit date. The Authority's final decision may differ from the auditor's recommendation.

C.3 While auditors are expected to apply their professional judgement when determining the recommended next audit date, the audit frequency calculation should be used as a starting point for the recommended audit frequency.

C.4 This section describes the calculation of the future risk rating for an audit. Applying the future risk rating to the indicative audit frequency table will allow auditors to calculate the indicative audit frequency.[13]

C.5 In order to calculate the future risk rating, sum the breach risk rating for each breach.

C.6 For example, if an audit identifies three breaches:

- Breach one has a 'high' audit risk rating and 'moderate' controls; Breach risk rating = 6
- Breach two has a 'medium' audit risk rating and 'strong' controls; Breach risk rating = 2
- Breach three has a 'low' audit risk rating and 'weak' controls; Breach risk rating = 3.

C.7 The future risk rating is calculated as: 6 + 2 + 3 = 9.

C.8 The future risk rating is applied to the indicative audit frequency table (found in the relevant audit guideline) to determine the *indicative audit frequency*.

C.9 Auditors can determine a *recommended next audit date*. This is the auditor's professional opinion taking into consideration the:

- the *indicative audit frequency*
- the participant's proposed resolution of breaches (including breaches that have been cleared during the audit)
- breaches that are outside of the participant's control (either due to needing improvements in the wording of the Code, or are due to the actions of another participant)
- any instances where there is a risk of future breaches, but this risk did not result in an alleged breach during the audit period.

[13] The indicative audit frequency table is different for each participant type, and is part of each participant's audit guidelines.

References

Risk and Materiality Guidelines
ISAE (NZ) 3000, Assurance Engagements Other than Audits or Reviews of Historical Financial Information (July 2014)
International Standards on Auditing (ISA) Implementation in New Zealand (2010)
Practice Advisory 1210.A1-1: Obtaining External Service Provider to Support or Complement the Internal Audit Activity

Glossary of abbreviations and terms

Audit risk rating	The risk rating applied to audit findings to reflect the level of risk associated with the issue underlying the finding.
Authority	Electricity Authority.
Code	Electricity Industry Participation Code (2010).
Engagement Quality Control Review	A review conducted under paragraph 3.16 to assess an auditor's compliance with this *Auditor Protocol* and the *Risk and Materiality Guidelines*.
Future risk rating	Rating of future risk of breaches based on the number and severity of Code breaches identified in current audit.
Lead auditor	The auditor responsible for the production of the participant audit report.
Recommended next audit date	Auditors opinion of when the participant should next be audited.
Residual risk	The level of risk that remains once all efforts have been made to reduce the risk to tolerable levels. The concept of residual risk is used to focus audit effort in the planning stage and to categorise audit findings. See the Risk and Materiality Guidelines for more details.