Risk and Materiality Guidelines

Guidelines

2 May 2017

Version control

Version	Date amended	Comments
1	25 October 2016	Draft for consultation
1.1	2 May 2017	Finalise following consultation

Foreword

These guidelines must be followed by the Authority and Authority-approved auditors when:

- determining focus areas and level of effort in carrying out audits under the participant audit regime
- classifying instances of non-compliance (breaches) and other audit findings related to audits carried out under the participant audit regime.

Read these guidelines in conjunction with the *Auditor Protocol* and the *Inherent Risk Register*.

Commonly used terms

Audit risk rating	The risk rating to be applied in accordance with Table 10 to audit findings to reflect the level of risk associated with the issue underlying the finding.
Compliance rating	The rating to be applied in accordance with Table 9 to indicate whether an audit finding is a breach or a recommendation.
Control	A system, process, or procedure that, when applied, mitigates against breaches of the Electricity Industry Participation Code 2010 and/or adverse settlement outcomes and/or inefficient market operations/outcomes.
Engagement Quality Control Review	A review to be undertaken in accordance with the *Auditor Protocol* to assess an auditor's compliance with the *auditor protocol* and these *Risk and Materiality Guidelines*.
Inherent risk	The level of risk as measured by likelihood and consequence before control strength is taken into account. Inherent risk is determined by applying the risk matrix in Table 4. The categories of inherent risk are defined in Table 5.
Inherent risk register	The register maintained by the Authority that contains an up-to-date list of all identified risks along with their likelihood and consequence ratings and inherent risk ratings.
Residual risk	The level of risk that remains once all efforts have been made to reduce the risk to tolerable levels. Residual risk is determined by combining inherent risk and control strength using Table 7
Risk	The effect of uncertainty on the objectives of an organisation or institution.

Contents

Tables

Figures

1 Introduction

The participant audit regime

1.1 The participant audit regime (audit regime) is the participant audit, approval, and certification process contained in Parts 1, 10, 11, 15, and 16A of the Electricity Industry Participation Code 2010 (Code).

1.2 The purpose of the audit regime is to:

- evaluate participants' compliance with the Code provisions that are audited under the regime
- enable the Authority to make informed decisions regarding the certification, approval, and audit frequency of participants
- support the efficient operation of the electricity industry.

1.3 The key goals of the audit regime, (the things that the Authority wants to achieve with the audit regime), are:

- the timely and accurate settlement of the wholesale electricity market
- timely and error-free ICP switching
- for participants to provide accurate and complete information to others in a timely manner.

Risk

1.4 In general, risk is the *effect of uncertainty on achieving objectives.*[1]

1.5 In the context of the audit regime:

- *uncertainty* is an unpredictable outcome as a result of the manner in which each participant implements, systems, and processes
- *objectives* are the key goals listed in paragraph 1.3.

1.6 The key goals of the audit regime are met through compliance with the Code.

Risk assessment and the audit regime

1.7 In the context of the audit regime, risk can be defined as:

The possibility that an event occurs, which leads to an outcome that adversely impacts the goals of the audit regime.

1.8 Risk assessment is used to:

(a) set audit scope and focus

(b) report on audit findings

(c) prioritise remedial actions to address audit findings.

1.9 Examples of risks under the audit regime include:

[1] https://en.wikipedia.org/wiki/Risk#International_Organization_for_Standardization

(a) the risk that an ATH[2] incorrectly certifies an inaccurate meter, which leads to inaccurate meter data being used for settlement (and for calculating distribution charges and billing customers)[3]

(b) the risk that a distributor provides an incorrect 'effective date' for a loss factor, which leads to inaccurate data being used for settlement (and for calculating lines charges and billing customers)

(c) the risk that a trader incorrectly applies the seasonally adjusted profile shape to non-half hour (NHH) volumes, resulting in incorrect allocation of volumes between NHH meter reads

(d) the risk that a metering equipment provider (MEP) does not update metering details in the registry within the Code-specified timeframes, leading to inefficient operation of the customer switching process.

Materiality and the audit regime

1.10 Within the context of the audit regime, materiality refers to the measurement of the actual and potential impact that the participants' actions have on the goals of the audit regime.

1.11 Materiality is used by:

- auditors when classifying audit findings in audit reports
- the Authority as part of determining the participant's next audit date
- the Compliance Committee when making decisions on alleged breaches of the Code.[4]

Purpose of these guidelines

1.12 The purpose of these guidelines is to:

- provide context for the use of risk and the use of materiality within the audit regime
- set out the process for using inherent risk and residual risk to determine audit focus and effort
- set out the process for auditors to assess materiality.

1.13 This will support more efficient audits by ensuring audit focus and effort is assigned to the areas of greatest risk.

Structure of these guidelines

1.14 These guidelines are structured as follows:

---

[2] "ATH" is defined in the Code to mean, "a person who is approved under Schedule 10.3 to operate an approved test house".

[3] Although not part of the purpose of the audit regime, the data used for settlement is often used for distributor charging and customer billing, so the realisation of a risk to the wholesale electricity market is likely to also affect distributor charging and customer billing.

[4] The Authority's Compliance Committee (comprising of three Authority Board members) carries out most of the Authority's compliance functions. See more information at http://www.ea.govt.nz/code-and-compliance/compliance/about-compliance/.

(a) Section 1 (this section) provides an overview of the audit regime and the context of risk and materiality within the audit regime

(b) Section 2 sets out the approach to risk-based planning

(c) Section 3 sets out the process for assessing risk

(d) Section 4 sets out the process for assessing materiality.

2 Approach to risk-based planning

2.1 Risk assessment is used to set an audit's scope and effort.

2.1 Using a risk-based approach to plan audits helps ensure that:

(a) audits are conducted more efficiently

(b) audit outputs are of more use to the Authority and participants

(c) remedial measures (to address compliance risk) can be prioritised in a practical manner in accordance with the level of risk posed by the relevant finding.

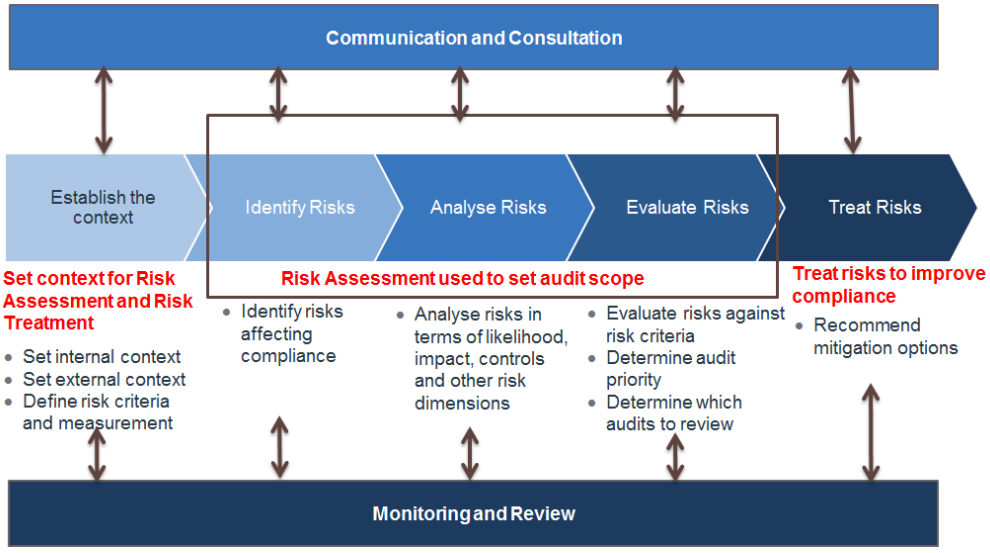
Overview of the framework

2.2 These guidelines are based on the risk management framework for the ISO 31000:2009 standard (*Risk management – Principles and guidelines*).

2.3 The framework contains high level principles and guidelines to provide organisations with a structured approach to identifying, measuring, and mitigating risks. It can be used across a wide variety of applications.

2.4 In the context of audits, the framework is used to identify and quantify compliance risks to focus audit effort, classify audit findings (based on materiality), and prioritise remedial measures.

Figure 1: Overview of ISO 31000:2009 risk management framework



Source: ISO 31000:2009

Overview of risk-based planning procedure

2.5 The ISO 31000:2009 framework can be applied during the audit planning phase to:

(a) define materiality levels and risk measurement criteria

(b) set audit scope based on participant type risk

(c) set tailored focus areas for audits (or audit priority areas) based on individual participant risk

(d) determine whether audits should be subject to engagement quality control reviews.

2.6 The audit regime uses three core documents as part of the risk-based planning process:

- **Risk and materiality guidelines**: Set out how to assess risk, the process for applying risk to focus audit effort, and how to assess materiality.
- **Auditor protocol**: Sets the standards for auditing and expectation of auditors when performing audits.
- **Inherent risk register**: Sets out the inherent risks, which are used by the auditor as a starting point to determine the audited participant's residual risk.

2.7 At a high level the risk-based planning process involves:

Table 1: Risk-based planning process

Step	Description	Document
1	Establish the objectives of the audit regime.[5]	*Risk and Materiality Guidelines*
2	Define the risk measurement criteria.[6]	*Risk and Materiality Guidelines*
3	Define materiality criteria.[7]	*Risk and Materiality Guidelines*
4	Identify industry level risks by participant class.	*Inherent Risk Register*
5	Analyse and evaluate industry level risks with respect to likelihood and consequence to determine an 'inherent risk rating' (low / med / high) for use by the auditors.	*Inherent Risk Register*
6	Review the controls in place to manage the inherent risks to determine 'residual risk' and therefore the 'audit priority'. The audit priority determines the minimum approach required by the auditor.	*Auditor Protocol*
7	Report on: (i) instances of non-compliance classified by the materiality definition developed above. (ii) areas of potential future non-compliance classified by the materiality definition developed above.	*Auditor Protocol*
8	Monitor and review of risks to ensure risks used for audit planning are kept current and updated.	*Inherent Risk Register*

Relationship between inherent risks, residual risks, and audit

2.8 Inherent risks are predetermined for each class of participant and available to auditors via the inherent risk register.

[5] See para 1.2.

[6] See section 3.

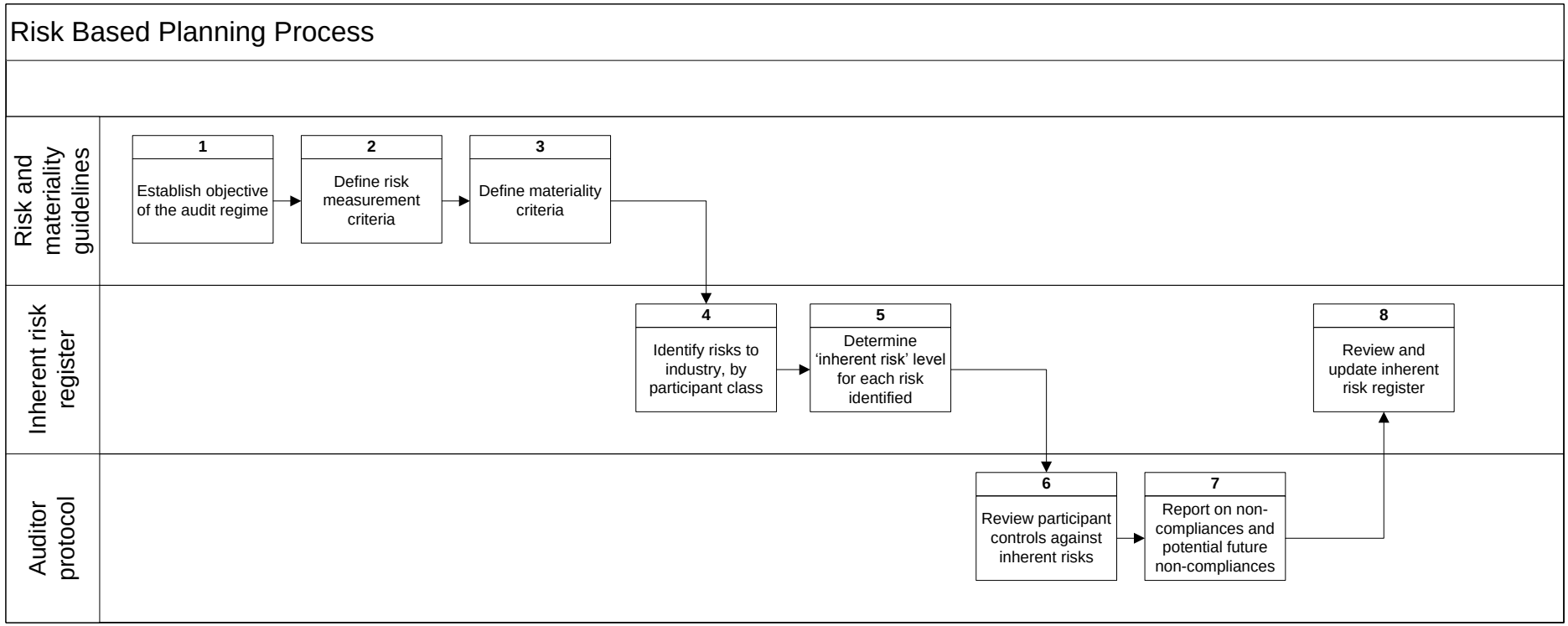
[7] See section 4

2.9 Auditors assess the effectiveness of the participant's controls against each inherent risk to determine the residual risk specific to that audited participant.

2.10 Auditors use the residual risk of the participant to determine the level of effort required to audit each area.

2.11 Auditors then audit the participant applying the level of effort assessed to each auditable area.

Figure 2: Overview of the risk-based planning process



3 Risk measurement criteria

3.1 There are two types of risk that need to be measured in the context of the audit regime:

(a) **Inherent risk**: Inherent risk represents risk in the absence of any controls. Inherent risks are assessed by the Authority, in consultation with industry and are used as the basis for determining residual risk. Inherent risks are specific to a class of participant, not to individual participants.

(b) **Residual risk**: Residual risk represents the risk once the effectiveness of controls has been assessed by the Auditor. Residual risk is used by the auditors to determine audit priority and effort. Residual risks are specific to each participant.

3.2 Risk is measured with respect to the following criteria:

(a) **Likelihood**: How likely is it that the risk will manifest itself in the absence of any controls?

(b) **Consequence**: What is the impact (financial, reputational, etc) to the market and participants if the risk manifests?

(c) **Strength of controls**: What controls/mitigation measures does the audited entity have in place to manage the risk?

Inherent risk assessed

3.3 The Authority assesses and communicates inherent risk through the *Inherent Risk Register*. The *Inherent Risk Register* is developed in consultation with industry to identify the risks inherent with operating in the electricity market.

3.4 Inherent risk is determined through a four step process:

(a) identify the risk

(b) assess the likelihood of risk (in the absence of any controls)

(c) assess the consequence should the risk eventuate

(d) combine the likelihood and consequence to determine the inherent risk rating.

Identify the risk

3.5 Risks are identified through industry consultation and the following process:

(a) for each class of participant, identify the general risks the audit regime is concerned with[8]

(b) for each risk, identify the undesirable outcome that would manifest if the risk occurred[9]

(c) for each auditable clause, identify the key risk(s) associated with the clause.

[8] Examples of key risks may include inaccurate submission information or inaccurate registry records.

[9] For example inaccurate submission information may lead to inaccurate invoices for reconciliation participants. Inaccurate registry records may lead to delayed customer switching. This in turn may lead to inaccurate submission information over the period of the switch.

Likelihood

3.6 The likelihood of each inherent risk identified is measured as follows:

Table 2: Likelihood of risk

Likelihood	**Descriptor**
Almost certain	Risk will occur in most circumstances
Likely	Would probably occur in most circumstances
Possibly	Could occur at some time
Unlikely	Not expected to occur in most circumstances
Rare	May occur in exceptional circumstances

3.7 Examples of the application of likelihood can be found in Appendix A.

3.8 The factors that must be taken into account to determine likelihood of risk include, but are not limited to, the following:

(a) Opportunities for errors/failures/non-compliance to occur: The greater the volume and frequency of process events which contribute to the risk, the greater an opportunity for an error to arise.

(b) Complexity of the business processes that might contribute to the risk: For example, a complex multi-step process involving multiple staff may be subject to more errors than a simple one-step process undertaken by a single staff member.

(c) Level of manual intervention in the process: A high level of manual intervention within a business process increases the scope for and likelihood of errors occurring.

(d) Incentives surrounding the process: Where adverse incentives exist, there may be a greater likelihood that the process is completed with errors (eg, if performance is measured based on number of transactions completed, there may be incentives to complete tasks at greater speed compromising accuracy).

(e) History of past performance of business processes that contribute to the risk: For example, past instances of non-compliance.

Consequence

3.9 The consequence of risks is classified as follows:

Table 3: Consequence of risk manifestation

Consequence	Examples
Major	The risk has the potential to lead to major settlement errors that affect consumers and/or significantly impact on multiple market participants and consumers (that may not be reversed or could be reversed but with difficulty).

Consequence	Examples
Moderate	The risk has the potential to impact on a particular area of settlement and/or one or more market participants with potentially minor impacts on consumers (that could be reversed easily).
Minor	The risk is not severe enough to adversely impact on other market participants or on consumers, but is significant enough for the Authority/the industry to consider remediating (ie, benefit of remediation outweighs cost).
Immaterial	The risk is not severe enough to adversely impact on other market participants or on consumers and could be dealt with using normal business procedures (eg, workarounds) and/or the cost of addressing the risk outweighs the benefit.

3.10 Examples of the application of consequence can be found in Appendix A.

Inherent risk rating

3.11 Inherent risk represents the risk in the absence of any controls.

3.12 The likelihood (Table 2) and consequence (Table 3) ratings are combined using the matrix (Table 4) to determine the inherent risk.

Table 4: Inherent risk rating matrix

		Consequence			
		Immaterial	**Minor**	**Moderate**	**Major**
Likelihood	**Almost certain**	**Medium**	**Medium**	**High**	**High**
	Likely	**Low**	**Medium**	**High**	**High**
	Possibly	**Low**	**Medium**	**High**	**High**
	Unlikely	**Low**	**Medium**	**Medium**	**Medium**
	Rare	**Low**	**Low**	**Medium**	**Medium**

Table 5: Inherent risk score

Inherent risk score	Description
High	High risk area with reasonable likelihood of manifestation and potentially severe/major adverse outcomes on market and end-consumer.
Medium	Medium risk area with low to reasonable likelihood of manifestation and moderate adverse outcomes on market and end-consumer.
Low	Low risk area with low likelihood of manifestation and low/negligible impacts on market and end-consumer.

3.13 Examples of the application of inherent risk can be found in Appendix A.

Residual risk

3.14 Residual risk is the risk that remains after the audited participant's measures to reduce and manage risk (known as controls) have been taken into account.

3.15 Residual risk is determined by the auditor and is used to set a priority level.

3.16 The residual risk rating is calculated by combining the inherent risk with control strength (ie, the level of risk after measures have been taken to reduce the risk).

Strength of controls

3.17 A control is a system, process, or procedure that is applied to mitigate against Code breaches and/or adverse settlement outcomes and/or inefficient market operations/outcomes.

3.18 Examples of controls include:

(a) error monitoring (eg, validation procedures, exception reporting, etc)

(b) business process documentation

(c) automated systems, tools, and alerts (to mitigate against manual errors).

3.19 Control strength must be measured as follows:

Table 6: Adequacy of controls

Control strength	Criteria
Strong	Control will mitigate risk to an acceptable level (ie, errors will be rare and/or impact of error will be reduced) or eliminate risk.
Moderate	Controls will mitigate risk most of the time, but there is room for errors to occur.
Weak	Controls are weak and are unlikely to mitigate risk and remove errors.
No control	Controls are non-existent, do not mitigate risk or remove errors

3.20 Determination of control strength must, where possible, take into account the following types of controls:

(a) **Preventative control**: Controls that ensure an issue or error does not arise in relation to a risk. The existence of preventative controls may be seen to be strong controls.[10]

(b) **Detective controls**: Controls that identify where an issue or error has arisen and require corrective controls to address the issue. Depending on the nature of the control, this may be seen to be an effective control provided there are associated corrective controls in place.[11]

(c) **Corrective controls**: Controls that ensure that an issue or error that has occurred is addressed. Corrective controls may be deemed effective, albeit lower in strength

[10] For example, system validation that prevents an incorrect ICP number from being entered into the system.

[11] For example, system checks that identify where a duplicate address exists.

than preventive controls, as the impact of the issue/error may have already manifested.[12]

3.21 In assessing overall control strength, auditors need to consider how individual controls work together to mitigate a particular risk.

3.22 Guidance on assessing control strength can be found in Appendix A.

Residual risk rating

3.23 The adequacy of controls (Table 6) is combined with the inherent risk ratings (Table 5) to determine a residual risk rating (Table 7). The residual risk rating determines the audit priority and the level of examination that is required for each risk (Table 8).

Table 7: Residual risk rating matrix

		Adequacy of control			
		No Control	**Weak**	**Moderate**	**Strong**
Inherent risk	**High**	**High**	**High**	**High**	**Medium**
	Medium	**Medium**	**Medium**	**Medium**	**Low**
	Low	**Low**	**Low**	**Low**	**Low**

Table 8: Level of examination required

Residual risk rating	Level of effort to be dedicated to risk area
High	Examine all risks in this area. Undertake thorough compliance testing and review effectiveness of controls to manage risk.
Medium	Examine at least 60 % of risks in this area. Undertake moderate compliance testing and review effectiveness of controls to manage risk.
Low	Examine at least 25 % of risks in this area. Undertake light compliance testing and select a small sample of business processes to review controls.

Calculating inherent risk if controls are not known

3.24 Auditors should assess controls and determine the levels of residual risk when preparing for an audit. An auditor should apply an assumed adequacy of 'weak' if they are unable to determine the adequacy of the audited participant's controls.

Measuring residual risks and setting audit priority areas

Auditors to assess inherent risk rating for any identified risks not on the inherent risk register

3.25 The auditor must assess the inherent risk of any identified risks that are not on the *Inherent Risk Register*. The auditor should follow the assessment process set out in paragraphs 3.4 to 3.12.

[12] For example, controls that check the accuracy of submission information after the initial wash-up has occurred.

3.26 For each risk for each audited participant or group of participants (as relevant and efficient), an auditor must determine control strength using the guidelines and procedures set out in paragraphs 3.17 to 3.22.

3.27 Auditors must determine a residual risk rating for each risk by applying the matrix set out in Table 7. The residual risk rating should also be used to determine the risk rating of audit findings as set out in paragraphs 4.2 to 4.6.

3.28 The auditor must use the finalised residual risk ratings to do the following for each audit (or group of audits if relevant and efficient) they undertake:

(a) Shortlist risks to examine, using Table 8 as a guide.

(b) Shortlist Code obligations, business processes, and functional areas that map to the shortlisted risks in item (a) above which will form part of the audit scope.

(c) Determine whether to include any software programs, tools, or IT systems in scope. For example, if a participant uses an in-house spreadsheet program to regularly implement a high risk function, then the auditor may want to include it in scope for testing.

3.29 Auditors must clearly document in their audit reports their rationale for selecting the risks, business function areas, and scope planned for their audits.

3.30 Auditors must ensure risk areas are rotated over consecutive audits to ensure all risk areas are covered over time.

4 Materiality measurement criteria

4.1 Materiality is used by auditors to classify auditing findings in audit reports.

4.2 Audit findings are classified using a two dimensional scale that takes into account the:

(a) compliance rating of the finding

(b) audit risk rating of the finding.

4.3 The compliance rating of an audit finding is categorised as follows:

Table 9: Compliance rating

Rating	Description
Breach	Evidence of non-compliance with the Code has been found.
Recommendation	Issues that could potentially lead to non-compliance with the Code, but where no evidence of breaches has been found. This relates to audit findings where the auditor has uncovered evidence of ineffective controls, or of controls that are not being applied.

4.4 The audit risk rating of an audit finding is categorised in accordance with the residual risk rating scale in Table 10 (these are based on the inherent risk/control strength matrix provided in Table 7).

Table 10: Audit risk ratings

Risk Rating	Description
High	The issue may have major impact on settlement outcomes, on market participants and/or end-consumers if not addressed immediately
Medium	The issue may have a moderate impact on settlement outcomes, on market participants and/or end-consumers if not addressed within the next 6–12 months
Low	The issue may have a minor impact on settlement outcomes, on market participants, and/or end-consumers if not addressed within 12–24 months.

4.5 Examples of how to rate an audit finding can be found in Appendix B.

4.6 In determining the audit risk rating, the auditor must form a view about the risk posed by the underlying issue, considering:

(a) the residual risk rating associated with the issue, taking into account the:

(i) inherent risk rating associated with the issue as provided in the *Inherent Risk Register*

(ii) control strength rating determined using the guidelines and procedures set out in paragraphs 3.17 to 3.22

(iii) rating matrix set out in Table 7

(b) any other participant-specific characteristics the auditor deems appropriate.

4.7 If the issue or risk is not included in the *Inherent Risk Register*, an auditor must:

(a) use the guidelines set out in:

(i) paragraphs 3.6 to 3.8 to assess likelihood

(ii) paragraph 3.9 to assess consequence

(iii) paragraphs 3.17 to 3.22 to assess control strength

(b) consider any other participant-specific characteristics the auditor deems appropriate

(c) articulate in the audit report the new risk and the rationale for determining the risk rating of the finding.

Appendix A Risk assessment examples

Examples of risks categorised by likelihood

A.1 To assist auditors understanding of how likelihood ratings should be applied in practice, examples of risks categorised by likelihood are set out below.

A.2 Note these examples are indicative only, and in some cases hypothetical breach histories are used to illustrate how auditors should take a participant's past performance into account to determine likelihood.

A.3 These risks do not identifying the root cause of the manifestation. It will be up to the auditor to identify the causer and the effectiveness of the controls to prevent future non-compliance. For example many categories of risk can manifest as a result of poor staff training or an absence of cover for key personnel.

Table 11: Examples of risks categorised by likelihood (in the absence of controls)

Likelihood criteria	Example of risk	Rationale for categorisation
Almost certain	The risk that a reconciliation participant submitting inaccurate volume submissions to the reconciliation manager leads to inaccurate data being used for settlement. Or The risk that a reconciliation participant's raw meter data validation process does not identify missing intervals, leading to submissions containing missing intervals being submitted for settlement. Or The risk that inaccurate ICP connection data is	Volume submissions involve large quantities of metered data being processed six times a month with potential manual intervention and some level of complexity which provides multiple opportunities for failure. Electricity meters, including HHR AMI metering installations, can be read on a daily basis. The volumes of information processes and complexity of participant systems involved in the process provides multiple opportunities for failure. New connections occur multiple times on a daily basis and involve

Likelihood criteria	Example of risk	Rationale for categorisation
	recorded in the registry (as part of a new connection process) resulting in inaccurate data being used for settlement.	multiple participants and manual processes.
Likely	The risk that a losing trader entering incorrect effective dates in the registry during a switch leads to inaccurate data being used for settlement and residential customer billing. Or The risk that a faulty meter is installed as a result of an MEP failing to follow Code installation requirements, which leads to inaccurate data being used for settlement. Or The risk that the registry is updated outside of the timeframes specified by the Code, leading to inaccurate data being used for settlement.	The total amount of switches processed by reconciliation participants may vary but on average occur tens of thousands of times per month across the industry. Although there is manual intervention, the switching task itself is quite simple. This is a moderate-low frequency event that has some complexity (in terms of the number of procedures and requirements that need to be met) and high levels of manual intervention. Multiple registry updates are made each day. Registry updates are simple to implement, but some registry updates involve manual processes.
Possibly	The risk that a metering installation not being maintained properly (as a result of a losing MEP providing metering records for the wrong installation to the gaining MEP) leads to inaccurate data being used for settlement. Or	This is a fairly simple task, which may not occur too frequently. The transmittal of records would involve manual tasks (eg, retrieval, transmittal) and there is scope for human error.

Likelihood criteria	Example of risk	Rationale for categorisation
	The risk that a distributor's failure to notify relevant traders of changes to shared unmetered load leads to inaccurate data being used for settlement.	This is a one-off event that is not complex in nature but is prone to human error (eg, failure to notify, incorrect information provided).
Unlikely	The risk that a trader entering an incorrect profile code in the registry leads to inaccurate data being used for settlement. Or The risk that not all ICPs are notified to the Market Administrator when requesting an ICP transfer leading to inaccurate allocation of volumes at the affected NSPs.	Profile codes for a particular ICP change infrequently so this is a low-frequency event and relatively simple to enter. Most participants use automated systems, however, there is scope for manual error. Transfer of ICPs can occur monthly. The process affects multiple ICPs, is low complexity, and involves manual intervention.
Rare	The risk that a distributor entering an incorrect POC Code leads to inaccurate data being used for settlement and/or to bill residential customers Or The risk that a distributor makes an error when updating loss factors in the registry leading to inaccurate data being used in settlement.	The POC code changes rarely and changing it in the registry is a simple task. However, as there is manual intervention there is some risk of failure. Process for updating loss factors occurs yearly. Affects a single loss factor. Is low complexity and involves manual intervention.

Examples of risks categorised by consequence

A.4 To assist auditors understand how consequence ratings should be assessed, examples of risks categorised by consequence are set out below.

A.5 Note that **these examples are indicative only**, and in some cases hypothetical breach histories are used to illustrate how auditors should take participant past performance into account to determine consequence.

Table 12: Examples of consequence ratings of risks

Result type[13]	Consequence rating	Examples	Rationale
Multiple or extensive use of inaccurate data or extended instances of missing or outdated data	Major	Inaccurate meter data submitted to the reconciliation manager for multiple intervals and multiple ICPs due to systemic errors in a trader's systems. Trader uses inadequate/unreasonable historical meter data to estimate actual usage at most ICPs for consecutive months (eg, estimating usage for a mild winter using meter data from a previously colder winter or recycling old estimates).	Systemic application of inaccurate, missing data, or outdated/historical data can have major financial and reputational impacts.
Inaccurate data is used	Moderate-major	Data submitted to the reconciliation manager is inaccurate (eg, due to faulty or tampered meter, incorrect meter multiplier used by trader or sourced from an inaccurate distributed unmetered load (DUML) database).	Inaccurate volumes will feed into reconciliation submissions and customer billing. This can result in either under or over submission and under or over billing of customers. Inaccurate submission volumes will affect the amount of unaccounted for energy (UFE) allocated to participants trading on the same balancing area and if within the wash-up cycle can be corrected through the wash-up process.

[13] That is, the adverse **result** that arises as a result of a risk **event** occurring.

Result type[13]	Consequence rating	Examples	Rationale
			The impact of the error is not necessarily constrained by the magnitude or the nature of the error. For example, if meter data errors occur only in a small number of intervals, but the errors deviate significantly from the actual usage, then the overall impact of the error can be moderate/major.
Data is not updated	Minor-moderate	Site is upgraded from an unmetered supply to a metered supply but the registry is not updated to reflect that there is no unmetered load (UML) onsite. Leads to inaccurate volumes submitted for reconciliation and inaccurate billing of consumers.	Updating of unmetered load details is an infrequent, commonly manual process. The volumes and number of ICPs affected are generally low.
Outdated or approximated data is used	Immaterial-minor	Loss factors are not adjusted on time leading to outdated loss factors being used Price category code is backdated in the registry by more than 3 business days but still prior to settlement and customer invoicing.	Outdated data may not be the best representation of real true losses on the network resulting in inaccurate UFE. However, there will be limited impact on market settlement due to the self-balancing allocation of UFE and ability to correct volumes via the wash-up process. The information is made available prior to settlement / customer billing, so no incorrect information flows to the market. The classification will be context dependent. For example, if the outdated loss factors are only minimally different to the updated loss factors, have only been applied for one period (and can be reversed), or are not associated with large submission volumes then the consequence is immaterial.

Result type[13]	Consequence rating	Examples	Rationale
Efficiency of market operations compromised	Immaterial-minor	Losing trader fails to update registry on time leading to a residential consumer not being switched in a timely fashion.	There is likely to be minimal impact on the residential consumer as a result of a minor delay in a switch (eg, 1 or 2 days). However, this does have a reputational impact on market integrity.

Examples of inherent risk

A.6 To assist auditors understand inherent risks, examples of potential inherent risks are set out below.

A.7 Note that **these examples are indicative only**, the actual inherent risks will be consulted on as part of the inherent risk register.

Table 13: Examples of inherent risk

Risk	Impact	Causer
Inaccurate volume information submitted for reconciliation	Inaccurate invoicing of trader. Inaccurate UFE and invoicing of other traders. May impact customer and distributor invoicing.	Historical estimate process does not correctly apply seasonally adjusted profile shape.
Inaccurate information populated on registry	Inaccurate information submitted for reconciliation. Delays to customer switching.	Trader not updating status of ICP on the registry to 'active' once ICP is energised.
Registry information not corrected in a timely manner	Inaccurate information submitted for reconciliation. Business decisions made on information that is out of date. Delays to customer switching.	MEP not updating metering information on the registry once metering is certified.

Guide for determining control strength

4.8 Auditors can use the following guidelines to determine control strength.

Control strength	Examples
Strong	Routinely applied automated processes that have been thoroughly tested/audited. For example, a tested/audited software program that validates meter data on a regular basis is a strong preventative and detective measure.
Moderate	Automated processes that occur infrequently may be good controls but may lead to errors if the process is not updated to take into account Code or business changes. However, if such a control exists in conjunction with clear process documentation and robust change governance the overall effect of the control may be strong. Semi-automated tools or systems with scope for manual error. For example, well-tested macros with scope for user input error; or automated calendar/system alerts with scope for dismissal by the user. Manual processes with process documentation (which include detective and corrective controls, as relevant) is also a good control. However, as the risk of human error cannot be eliminated, such a process may be prone to error.
Weak	Manual processes with poor quality or no business process documentation. Note the existence of high quality process documentation for one-off manual processes that may occur infrequently (eg, de-commissioning of an ICP) is important as there is more scope for error in a process that is not regularly applied. Therefore, the criteria for assessing the strength of a control/procedure would vary for a regular manual process compared with an infrequent one.
No control	Manual processes with no business process documentation and minimal operator training. Processes may have a high risk of human error due to poor training, poor documentation, and infrequent use.

Appendix B Application of materiality for audit findings

B.1 Note that the examples in Table 14 and Table 15 are indicative only, and in practice each audit finding will be context-dependent and should be scrutinised on a case by case basis.

Table 14: Materiality rating application guidelines

Compliance rating	Risk Rating		
	High	**Medium**	**Low**
Breach	Code breach where the underlying issue is considered a high risk. For example: • Reconciliation participant fails to submit some HH volume information leading to other participants being invoiced incorrectly (in categorising the breach as High the auditor may take into account the size of the participant and their potential impact on settlement outcomes). • Reconciliation participant's submission is missing volume information. Although the participant is a medium-sized trader, the auditor notes their submissions are often incomplete leading to an overall risk rating of high. • Distributor fails to create ICP identifier within 3 business days of a request; no financial impact (as ICP identifier created before end of month). Auditor notes	Code breach where the underlying issue is considered a moderate risk. For example: • Distributor provides incorrect address information relating to a metering point. Although there is nil impact, the auditor notes past breaches and the potential financial impact in the event that the meter needs to be deregistered (in assigning the medium rating the auditor takes into account the likelihood of the potential result manifesting, as well as its consequence). • Reconciliation participant does not have a complete audit trail for all data gathering, validation, and processing functions. In this case the issue is that the lack of an audit trail may make retracing errors problematic, leading to potential inaccuracies in settlement. Although errors	Code breach where the underlying issue is considered a low risk. For example: • Reconciliation participant enters incorrect ICP identifier in the registry. However, this is corrected later, and no switches occur leading to no impact. Auditor notes that this is a one-off error and therefore deems the issue to be low risk. • A losing MEP does not provide a gaining MEP with requested information within the 10 business day deadline. Although a breach, this does not have any impact on settlement outcomes. The auditor notes this is a one-off breach with limited likelihood of recurrence.

Compliance rating	Risk Rating		
	High	Medium	Low
	recurrence of delay creating ICP identifier with previous breaches that had a financial impact; therefore auditor deems the risk rating to be high. • Reconciliation participant enters incorrect ICP identifier in the registry. Although there is no impact due to the customer not switching (before the error is corrected), auditor notes multiple such instances of incorrect ICP identifiers and notes this breach has occurred in previous audits. Therefore, the auditor deems this a high risk breach as there is an increased likelihood error will continue to occur and result in financial or other impacts (ie, a switch occurs before the error is rectified). • MEP is not inspecting metering installations within the timeframe specified by the Code. While the registry has been updated and in most cases the recertification activities demonstrated that the installations remained accurate; the MEP has been aware of the issue for the past 9 months and	are "likely" and the participant only has "moderate" controls, the reconciliation participant is a small trader. Therefore errors are likely to have only minor impacts on settlement. Therefore, the auditor deems this finding a "medium" risk. • MEP is not updating metering details on the registry within 10 business days of re-certifying metering installations. The MEP has been aware of the issue for the past 15 months but has not taken action to address the non-compliance. The auditor deems this finding a "medium" risk due to lack of controls and increased likelihood of ongoing non-compliance.	

Compliance rating	Risk Rating		
	High	**Medium**	**Low**
	has not taken action to address the non-compliance. The auditor deems this finding a “high” risk due to lack of controls and increased likelihood of ongoing non-compliance.		
Recommendation	Non-breach related issue where the underlying issue is considered a high risk. For example: • Auditor finds that a reconciliation participant's tools to validate volume information have a very high scope for error. However, no breaches have occurred to date. The risk is deemed high due to the high likelihood of potential breach and major/moderate consequence of such a breach. • Reconciliation participant provides estimates instead of meter readings. Although this is not a Code breach, the auditor notes this is a recurring issue. Although not in breach, the auditor deems the use of estimates (in lieu of actual meter readings) to have a major/moderate impact on settlement outputs.	Non-breach related issue where the underlying issue is considered a moderate risk. For example: • Auditor notes distributor has limited or poor quality business process documentation to support one-off manual tasks such as meter point deregistration or to support regular manual tasks for which breaches have been noted previously. • Auditor notes that although dispatchable load purchaser’s compensation factors have been calculated correctly, the tool for calculating compensation factors has some risk for input data error. Auditor considers likely risk of error occurring in the future with minor to moderate impacts on settlement outcomes. Therefore,	Non-breach related issue where the underlying issue is considered a low risk. For example: • Auditor notes minor errors in participant’s business process documentation. However, auditor notes that these errors are not implemented in practice as the documentation is seldom referred to by experienced staff. In the event new staff implement the process, there is a minor risk that the errors may affect operational practice and lead to a breach with minor/moderate impact. Therefore, the auditor deems this to be a low risk audit finding. • Auditor notes scope for improving governance around business process documentation to ensure Code changes are captured appropriately.

Compliance rating	Risk Rating		
	High	Medium	Low
		the auditor deems this a medium risk finding.	

Table 15: Examples of application of materiality ratings

Breach description	Rating	Reason for rating
Provision of incorrect submission information and failure to conduct revisions for five distributed unmetered load ICPs, leading to under submission of 500,000 kWh per annum.	High	Major impact on settlement and risk that submission information may not be corrected within the 14-month window.
Provision of incorrect submission information and failure to conduct revisions for ten shared unmetered load ICPs, leading to under submission of 1,095 kWh per annum.	Medium	Moderate impact on settlement. Would become High if not resolved within specified timeframe.
Corrections for stopped meters made from the date found and revisions not conducted. 15,000 kWh under submission.	Medium	Moderate impact on settlement. Would become High if not resolved within specified timeframe.
Corrections not conducted for 300 bridged meters: 100,000 kWh under submission.	High	Major impact on settlement and risk that submission information may not be corrected within the 14-month window.
Three late switch files out of 15,000 total files.	Low	Minor impact on other participants. Small percentage of overall files.
Ten late switch files out of 150 total files.	Medium	Moderate impact on other participants. Moderate percentage of overall files.
1,000 late switch files out of 5,000 total files.	High	High impact on many participants. High percentage of files.

Breach description	Rating	Reason for rating
Active status not updated within 5 business days for 5 out of 100 total ICPs. All updates within 30 business days.	Low	Minor impact on settlement outcomes and other participants. No outliers.
Active status not updated within 5 business days for 35 % of ICPs. 10 % of updates over 30 days with the longest being 250 days.	High	Major impact on settlement outcomes and other participants. Some outliers.
MEP updates metering details later than 10 business days for 50% of ICPs. Average days is 16.	High	Major impact on settlement and other participants because it can hold up switching and submission and can lead to incorrect tariffs or profiles.
MEP updates metering details later than 10 business days for 7 out of 2,500 ICPs. Non-standard circumstances exist in all cases. Average days for the 2,500 ICPs is 6.5 days.	Low	Minor impact on settlement and other participants.
ATH does not conduct error and uncertainty calculations in accordance with the Code for any metering installations: 7,000 metering installations have been done in total.	High	There is no evidence of inaccuracy, but there is potential for inaccuracy so this matter may have a major impact on settlement outcomes.

References

Auditor Protocol
AS/NZS ISO 31000:2009 *Risk Management – Principles and guidelines* (extracts from ISO31000:2009 used with permission)

Inherent Risk Register

Glossary of abbreviations and terms

Authority	Electricity Authority
Audit risk rating	The risk rating to be applied in accordance with Table 10 to audit findings to reflect the level of risk associated with the issue underlying the finding
Code	Electricity Industry Participation Code 2010
Compliance rating	The rating to be applied in accordance with Table 9 to indicate if an audit finding is a breach or a recommendation
Control	A system, process, or procedure which is applied to mitigate against Code breaches, and/or adverse settlement outcomes, and/or inefficient market operations/outcomes
Engagement Quality Control Review	A review to be undertaken in accordance with the *auditor protocol* to assess an auditor's compliance with the *auditor protocol* and these *risk and materiality guidelines*
Inherent risk	The level of risk as measured by likelihood and consequence before control strength is taken into account. Inherent risk is determined by applying the risk matrix in Table 4 and the categories of inherent risk are defined in Table 5
Inherent Risk Register	The register maintained by the Authority that contains an up to date list of all identified risks along with their likelihood and consequence ratings and inherent risk ratings
MEP	Metering equipment provider
Residual risk	The level of risk that remains once all efforts have been made to reduce the risk to tolerable levels. Residual risk is determined by combining inherent risk and control strength using Table 7
Risk	The effect of uncertainty on the objectives of an organisation or institution
UFE	Unaccounted for energy.