Draft risk-based planning principles

Overview of the risk management standard

1. The ISO 31000:2009 standard (Risk management – Principles and guidelines) is an internationally recognised framework used by organisations to manage risk.

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

3. In the context of audits, the framework is used to identify and quantify compliance risks to:

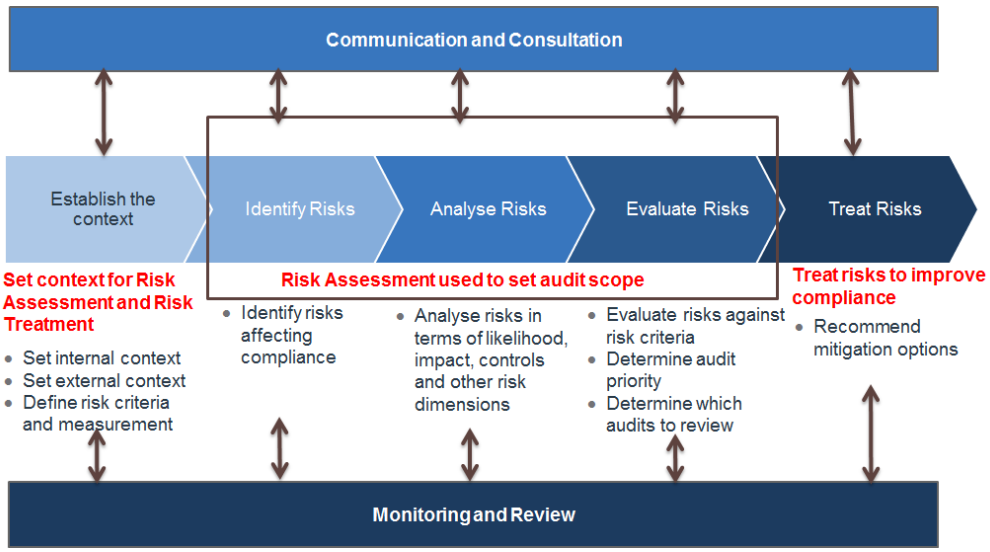
   (a) define materiality levels and risk measurement criteria

   (b) identify and quantify risks based on the risk measurement criteria

   (c) set the scope of audit activities and focus areas

   (d) recommend measures to treat (or mitigate) compliance risks.

Figure 1 Overview of ISO 31000:2009 risk management framework



Source: The diagram above is based on AS/NZS ISO 31000:2009, Risk Management – Principles and guidelines.

Risk management framework as it applies to the participant audit regime

4. 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 risk

(c) set focus areas for audits (or audit priority areas) based on participant risk[1]

(d) determine whether audits should be subject to engagement quality control reviews.[2]

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

(a) Identifying 'industry' level risks and consequences by participant class (annually or as needed). This information creates an 'inherent risk score' (low / med / high) for use by the auditors.

(b) Reviewing the controls in place to manage each of the inherent risks to determine the 'audit priority'. The audit priority determines the minimum approach required by the auditor.

(c) Following the audit, reporting on:

(i) areas of non-compliance, including materiality

(ii) areas of potential future non-compliance, including materiality and likelihood of the non-compliance in the future.

Draft risk-based planning principles

6. This section describes the principles that will be used to develop a process and guidelines for planning audit scope. Focused on specifying materiality levels, it will be divided into three sections as follows:

(a) definition of risk measurement and materiality criteria

(b) risk assessment procedures

(c) audit scope and focus setting procedures.

Definition of risk measurement and materiality criteria

Overview

7. This section describes:

(a) the risk measurement criteria for evaluating risks and setting audit focus areas under the Evaluating risks section

(b) the materiality levels are used when categorising instances of non-compliance and general audit findings.

8. The manner in which risks are identified and analysed (so that they can be evaluated/quantified with respect to the criteria set out in this section) is covered in Risk assessment procedures section.

---

[1] The level of effort dedicated to these Audit Priority areas are dependent on the level of risk in each area and is set out in the proposed auditor requirements.

[2] An Engagement Quality Control Review is conducted by the Authority on the audit to form a view of the auditor's compliance with the auditor requirements and auditing standards.

Risk measurement

9. The following criteria need to be considered when evaluating risks under the Evaluating risks section:

   (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 manifested itself?

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

10. The likelihood of a risk can be measured by:

Table 1: Likelihood of risk

Likelihood	Examples
Almost certain	Risk likely to manifest multiple times annually
Likely	Risk likely to manifest at least once or twice a year
Probably	Risk likely to manifest once every two years
Unlikely	Risk likely to manifest once every five years or less
Rare	Risk likely to manifest once every ten years or less

11. The consequence of risk manifestation can be classified by:

Table 2: Consequence of risk manifestation

Consequence	Examples
Immaterial	Risk would have nil or negligible impact on market outcomes. Examples include technical breaches where wording of the rule was breached, but intent was complied with.
Minor	Risk would have minor impact on decisions made by market participants or consumers, but not enough to cause a financial or reputational impact. Examples include delays in publication of non-critical market information.
Moderate	Risk would have minor financial or reputational impact. Examples include risks which may lead to minor settlement errors which may also cause minor/negligible financial impact on the end-consumer (minor errors in meter data submission or estimation, minor errors in

Consequence	Examples
	loss factor calculations, etc).
Major	Risk would have major financial or reputational impact. Examples include risks which may lead to major settlement errors that may also financially impact on the end-consumer (major errors in meter data submission or estimation, major errors in loss factor calculations, etc).

12. The strength of controls can be measured by:

Table 3: Adequacy of controls

Adequacy of Controls	Criteria
Strong	Control will mitigate risk to acceptable level
Moderate	Controls will mitigate risk most of the time, but room for improvement
Weak	Controls are weak or non-existent and have minimal impact on risks.

13. The strength of controls will vary with time and by participant (they can be evaluated prior to the audit to help determine the level of effort required to audit each area sufficiently):

    (a) an inherent risk rating can be determined by combining the likelihood and consequence criteria corresponding to a particular.

    (b) an audit priority rating can be determined by combining the inherent risk rating.

Table 4: Inherent risk rating matrix

		Consequence			
		Immaterial	Minor	Moderate	Major
Likelihood	Almost Certain	Medium	Medium	High	High
	Likely	Low	Medium	High	High
	Possible	Low	Medium	High	High
	Unlikely	Low	Low	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 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.

14. An audit priority rating can be calculated by assessing the individual participant's adequacy of controls and applying the matrix below.[3]

Table 6: Audit priority rating matrix

	Adequacy of control		
	Weak	**Moderate**	**Strong**
High	**AP1**	**AP1**	**AP2**
Medium	**AP2**	**AP2**	**AP3**
Low	**AP3**	**AP4**	**AP4**

Table 7: Level of examination required

Audit Priority (AP) Score	Level of effort to be dedicated to risk area
AP1	Examine all risks in this area. Undertake thorough compliance testing and review effectiveness of controls to manage risk
AP2	Examine at least 75% of risks in this area. Undertake moderate compliance testing and review effectiveness of controls to manage risk.
AP3	Examine at least 40% of risks in this area. Undertake light compliance testing and select a small sample of business processes to review controls.
AP4	Examine at least 25% of risks in this area. Undertake desktop review and interviews.

Breach Materiality levels

15. Instances of non-compliance or breaches can be categorised using the following compliance rating scale.

[3] While groups of participants (eg, distributors) may all face the same inherent risks, once that risk has been adjusted for strength of controls, this may result in different focus areas.

Table 8: Breach materiality levels

Rating	Criteria
1	• breach has significant to moderate financial impact on one or more participants and/or one or more end-consumers or • breach has low financial impact on multiple market participants and/or end-consumers and/or • breach may have affected decisions of market participants that would have a significant financial impact on the participant or on the market and/or • breach will result in the Authority being unable to monitor compliance with a different obligation of the audited participant or another participant and a breach of that obligation could result in a Rating 1 breach occurring • breach may result in significant reputational impact on market participant and market and • if cause of non-compliance is not dealt with immediately there will be on-going financial and reputational impacts.
2	• breach has low financial impact on one market participant and/or • breach may have affected decisions of market participants that would have a moderate-low financial impact on the participant or the market and/or • breach may have moderate to low reputational impact on market participant and market and • breach will result in the Authority being unable to monitor compliance with a different obligation of the audited participant or another participant and/or • if the breach is not addressed within three-six months there will be on-going financial and reputational impacts and may result in Rating 1 breaches occurring.
3	• breach has no financial impact on market participants and/or • breach would not have affected decisions of market participants and/or • breach had no reputational impact on market participant or market and/or • market participant has complied with intent of rule if not wording and • breach should be addressed within 6-12 months to ensure similar breaches do not recur.

Assessment of compliance risks / Likelihood

16. General audit findings can be categorised using the risk rating scale. Examples of general audit findings include:

    (a) compliance risks noted (that may or may not have manifested as a breach but has the potential to do so)

    (b) breaches noted that have nil or negligible impact (and therefore rated as Compliance Rating 3) but that are associated with compliances risk, which, if not addressed shall lead to Compliance Rating 2 or Compliance Rating 1 breaches occurring.

17. Risk ratings can be assigned using the following rating scale:

Table 9: Risk rating matrix

		Consequence of risks associated with finding			
		Immaterial	Minor	Moderate	Major
Likelihood of risk manifesting if finding not addressed	Almost Certain	Medium	Medium	High	High
	Likely	Low	Medium	High	High
	Possible	Low	Medium	High	High
	Unlikely	Low	Low	Medium	Medium
	Rare	Low	Low	Medium	Medium

Table 10: Risk ratings

Risk Rating	Description
High	Finding may have major impact on settlement or other market outcomes, on market participants and/or end-consumer if not addressed immediately. These findings required executive attention (eg, CEO/Board level attention).
Medium	Finding may have a moderate impact on settlement or other market outcomes, on market participants and/or end-consumer if not addressed within 6-12 months. These findings require management level attention (eg, group manager).
Low	Finding may have a minor impact on settlement or other market outcomes, on market participants and/or end-consumer if not addressed within 6-12 months if not addressed within 12-24 months. These findings require team management level attention (eg, assistant managers, team leaders, etc).

Risk assessment procedures

Overview

18. Risk assessment procedure is a three step process involving:

    (a) identifying the compliance risks faced by the audited entities or participants

    (b) analysing the above risks

    (c) evaluating the risks using the criteria to determine audit priority areas.

19. The risk assessment procedure will be undertaken as:

    (a) an initial risk assessment, when these procedures are first implemented

    (b) updating of risk assessment undertaken at regular intervals. The updated assessment will be incremental in nature, aimed at identifying new risks and (if relevant) modifying previously identified risks to ensure that audit priority areas are determined based on up to date risk definitions.

Identifying risks

20. Risks faced by all participants who are subject to the audit regime shall be identified and reviewed on a regular basis.[4]

21. A risk (in the context of these procedures) is defined as the risk of non-compliance with, deviation from, or inconsistency with:

    (a) a participant's obligations under the Code

    (b) the Authority's statutory objectives.

22. The following should be taken into account when identifying risks in respect of a participant or group of participants:

    (a) historical audit findings of reported instances of non-compliance and compliance risk

    (b) challenges faced by participants in other electricity markets

    (c) other reported instances of non-compliance (if available)

    (d) observations of the market, trends and statistics (where available).

Analysing risks

23. A qualitative assessment of the risks identified in section Identifying risks can be used to establish the following:

    (a) The cause and source of each risk (ie, how would the risk manifest itself?) for the participant under audit.[5] Where the cause or source of a risk will be a key determinant of audit scope. For example, if a piece of software or other tool is a risk source (eg, erroneous loss factors calculated due to a fault tool), then software testing could be in scope of the audit.

    (b) How the risk can be controlled by the participant, or whether the risk is a consequence of a breach by another participant.

    (c) Given the above, how likely it is that the risk will manifest itself (in the absence of any controls).[6] What parties would be affected if the risk manifested, and the consequence of the risk manifesting.[7]

    (d) What types of controls exist to manage the risk.[8]

---

[4] Examples of risks in the context of the audit regime may include the following:

(i) participant provides incorrect or incomplete metering data or other information to reconciliation manager or other entity involved in settlement

(ii) participant does not provide ICP information to registry when a customer switch has occurred

(iii) participant fails to update loss factors or calculates loss factors incorrectly

(iv) participant's meter readings are inaccurate.

[5] Note that there may be multiple causes/sources for a particular risk ranging from incorrect/faulty data inputs, faulty software, human error, fraudulent intervention, etc.

[6] Classification of the likelihood of risk can be found in Table 1.

[7] Classification of consequence can be found in Table 2.

Evaluating risks

24. Each risk identified in section Identifying risks and analysed in section Analysing risks (for each participant) can be evaluated to determine the level of examination required.[9]

25. Scope and focus areas can be set based on the risk evaluation results as follows:

    (a) Audit Priority Area 1 (AP1):

        (i) examine all risks in this area

        (ii) audit compliance with all Code obligations relating to this risk area

        (iii) audit software or tools used to implement all Code obligations relating to this risk area

        (iv) where applicable, review the appropriateness and adequacy of Information Communication (ICT) systems and associated ICT procedures used to support the implementation of Code obligations in this risk area

        (v) review the effectiveness and appropriateness of controls used to implement Code obligations relating to this risk area.

    (b) Audit Priority Areas 2 (AP2):

        (i) select 75% of the risks in AP2, ensuring that all risks are examined over time

        (ii) audit compliance with the Code obligations which map to the selected risks

        (iii) test software or tools used to implement the Code obligations which map to the selected risks

        (iv) where applicable, review the appropriateness and adequacy of Information ICT systems and associated ICT procedures used to support the implementation of Code obligations in this risk area

        (v) review the effectiveness and appropriateness of controls used to implement the majority of Code obligations which map to the selected risks.

    (c) Audit Priority Area 3 (AP3):

        (i) select 40% of the risks in AP3, ensuring that all risks are examined over time

        (ii) audit compliance with the Code obligations which map to the selected risks

---

[8] Classification of the adequacy of controls can be found in Table 3.

[9] Classification of the level of audit priority and level of examination require can be found in Table 7.

(iii) review the effectiveness and appropriateness of controls used to implement a minority of Code obligations which map to the selected risks.

(d) Audit Priority Area 4 (AP4):

(i) select 25% of the risks in AP3, ensuring that all risks are examined over time

(ii) audit compliance with the Code obligations which map to the selected risks

(iii) in undertaking audit procedures in each of the Audit Priority areas, follow the risk-based audit procedures pertaining to the relevant risk area (AP1, AP2, AP3 or AP4)[10]

(iv) these principles are not rigid and from time to time it may be necessary to vary the scope or increase the level of scrutiny applied to AP2, AP3 and AP4 areas.

[10] These are described in more detail in the proposed auditor requirements.