

Electricity Distribution Ring-fencing Guideline

Compliance Reporting
Best Practice Manual
Version 3

February 2022

© Commonwealth of Australia 2022

This work is copyright. In addition to any use permitted under the Copyright Act 1968 all material contained within this work is provided under a Creative Commons Attributions 3.0 Australia licence with the exception of:

- the Commonwealth Coat of Arms
- the ACCC and AER logos
- any illustration diagram, photograph or graphic over which the Australian Competition and Consumer Commission does not hold copyright but which may be part of or contained within this publication.

The details of the relevant licence conditions are available on the Creative Commons website as is the full legal code for the CC BY 3.0 AU licence.

Inquiries about this publication should be addressed to:

Australian Energy Regulator

GPO Box 520

Melbourne VIC 3001

Tel: 1300 585 165

AER Reference: 65292 - #12431808v5

Amendment Record

Version	Date	Pages
1	June 2018	20
2	July 2019	19
3	March 2022	17

Shortened forms

Shortened Form	Extended Form
ACCC	Australian Competition and Consumer Commission
AER	Australian Energy Regulator
current guideline	Ring-fencing guideline – Electricity distribution (version 3), November 2021
DNSP	distribution network service provider
RIN	Regulatory Information Notice

Contents

Shortened forms.....	1
1 Introduction	3
1.1 Purpose of this manual.....	3
1.2 The Ring-fencing Guideline	3
1.3 Terminology	4
2 Registers.....	5
3 Annual Compliance Report	6
3.1 Pre- and post-assessment.....	6
3.2 Compliance protocols.....	6
3.3 Meaningful compliance reporting.....	7
3.4 Reporting breaches in the annual compliance report.....	7
3.5 Reporting other services.....	7
3.6 Reporting transactions with affiliated entities	8
3.7 Publication of DNSP annual ring-fencing compliance and independent assessment reports	8
4 Independent compliance assessment	9
4.1 What is a ‘suitably qualified independent authority’?.....	9
4.1.1 Independence.....	9
4.1.2 Suitably qualified	9
4.1.3 Demonstrating that an assessor is suitably qualified and independent	9
4.2 Assurance level.....	10
4.3 Types of assessment	11
4.4 Expectations of independent assessor	11
5 AER compliance reporting	12
6 Our approach to handling ring-fencing complaints.....	13
7 Compliance breaches	14

1 Introduction

1.1 Purpose of this manual

The purpose of this compliance reporting manual (the manual) is to inform electricity distribution network service providers (**DNSPs**) of the **AER's** view of best practice regarding the compliance reporting obligations under the **Ring-fencing Guideline – Electricity Distribution (the Guideline)**.¹ This manual should be read in conjunction with the **Guideline** and its accompanying explanatory statement.² This manual covers the entire suite of compliance obligations set out in the **Guideline**, including:

- breach reporting;
- maintenance of registers;
- annual compliance reporting;
- annual independent assessments of compliance; and
- complaints and investigations.

This manual provides clarity to **DNSPs** on the **AER's** interpretation of the compliance reporting requirements in the **Guideline**. This manual does not impose additional requirements on **DNSPs**. The requirements of the Guideline are binding under clause 6.17.1 of the **National Electricity Rules**.

This manual is consistent with the **AER's** *Strategic Plan 2020-2025*.³

This manual may be updated from time to time by the **AER**. All changes will be designed to increase clarity on how **DNSPs** should satisfy compliance reporting requirements under the **Guideline**.

1.2 The Ring-fencing Guideline

The **Ring-fencing Guideline – Electricity Distribution** was made under clause 6.17.2 of the **National Electricity Rules**. It was first published in November 2016 and amended in October 2017 and November 2021.

The objective of the **Guideline** under clause 1.1.1 is to:

- promote the **National Electricity Objective** by providing for the accounting and functional separation of the provision of **direct control services** by **DNSPs** from the provision of other services by them, or by their **affiliated entities**; and
- promote competition in the provision of electricity services.

¹ AER, *Ring-fencing Guideline – Electricity Distribution – Version 3*, November 2021.

² AER, *Ring-fencing Guideline – Electricity Distribution – Version 3 – Explanatory Statement*, November 2021.

³ AER, [Strategic Plan 2020-2025](#), December 2020

The **Guideline** seeks to accomplish this objective by imposing obligations on **DNSPs**, targeted at, among other things:

- cross-subsidisation, with provisions that aim to prevent a **DNSP** from providing **other services** that could be cross-subsidised by its **distribution services**; and
- discrimination, with provisions that aim to:
 - prevent a **DNSP** conferring a competitive advantage on its **related electricity service providers** that provide **contestable electricity services**; and
 - ensure a **DNSP** handles ring-fenced information appropriately.

1.3 Terminology

For the purposes of this manual, all bold terms have the meaning defined in clause 1.4 of the **Guideline** or the **National Electricity Rules**.

2 Registers

The Guideline requires **DNSPs** to maintain four publicly available registers which must be updated no later than 15 January, 15 April, 15 July and 15 October each year. These registers are:

- office and staff register;⁴
- information register;⁵
- waiver register;⁶ and
- regulated stand-alone power systems register.⁷

In addition, the **DNSP** must establish a publicly available information sharing protocol.⁸

DNSPs should carefully consider the form, content and accessibility of these registers. A register or protocol that is generic or high level may not contain enough detail to fulfil the requirements of the **Guideline**. To assist **DNSPs** a template for office and staff sharing registers is on our website. Where possible **DNSPs** should follow this format to ensure the information provided is relevant and accessible to interested third parties.

If members of the public struggle to locate these registers and protocols on the website, they may not have the effect of preventing discrimination intended by the **Guideline**.

In addition to updating the office and staff sharing register quarterly **DNSPs** should update this register when it sees fit, for example, when new information needs to be added.

Information on the registers should be retained for a sufficient period to allow the information to be effectively accessed by third parties, including **related electricity service providers** and other legal entities who provide **contestable electricity services** but who are not **affiliated entities**. **DNSPs** should also ensure that the terms of their information sharing protocol do not unnecessarily restrict the ability of any **legal entity** to access information on the register or be added to the **information register**.

⁴ Required by clause 4.2.4 of the **Guideline**

⁵ Required by clause 4.3.4 of the **Guideline**

⁶ Required by clause 5.7 of the **Guideline**

⁷ Required by clause 6.2.3 of the **Guideline**.

⁸ Required by clause 4.3.3(d) of the **Guideline**

3 Annual Compliance Report

Clause 6.1 of the **Guideline** requires that a **DNSP** establish and maintain appropriate internal procedures to ensure it complies with its obligations under the **Guideline**.

Clause 6.2.1 (a) of the **Guideline** mandates that a **DNSP** prepare an annual report on ring-fencing compliance and submit it to the **AER**. Clause 6.2.1(b) of the **Guideline** lays out 4 categories of information that must be included in all annual compliance reports.

Annual compliance reports should be accompanied by a cover letter signed by the CEO or acting-CEO of the **DNSP** attesting that the contents of the report are accurate to the best of their knowledge.

The following sections provide further information on the AER's view on compliance reporting that may assist when preparing the compliance reports.

3.1 Pre- and post-assessment

The **AER** may communicate with the **DNSP** prior to or after the independent assessments to provide the **DNSP** and assessor with an opportunity to discuss their compliance reports. The **AER** may request meetings with a **DNSP** or multiple **DNSPs** and the **DNSP's** chosen independent assessor(s) prior to the commencement of the assessment and after the annual report and independent assessment has been submitted.

When required the **AER** will inform the **DNSP** in writing of a pre and/or post-assessment meeting and will coordinate with the **DNSP** and the independent assessor to organise these meetings. Not all **DNSPs** will require pre and/or post-assessment meetings every year. Pre-assessment meetings will be organised in January or February prior to the submission of the annual compliance report. Post-assessment meetings will be organised in June or July following the lodgement of annual compliance reports.

3.2 Compliance protocols

Sub-clause 6.2.1(b)i states that a **DNSP** must identify and describe "the measures the **DNSP** has taken to ensure compliance with its obligations under this **Guideline**". In its annual compliance report, **DNSPs** should explain how the compliance measures put in place ensures every obligation in the **Guideline** is addressed. **DNSPs** should also demonstrate in their annual report that there are a range of controls in place to address risk of non-compliance for each obligation, as relevant. For example, in assessing the appropriateness of a **DNSP's** compliance measures, the **AER** will consider whether each obligation is addressed by:

- 'preventative' controls or measures, which are designed to prevent breaches of a particular obligation in the **Guideline** from occurring;
- 'detective' controls or measures, which are designed to ensure that breaches that have already occurred can be detected or identified internally in a timely way in the future; and
- 'corrective' controls or measures, which ensure that timely and appropriate corrective or remedial action can be taken to address a breach once is detected. Having strong corrective controls in place may make breaches less likely to recur.

DNSPs may choose to structure their annual reporting by identifying ring-fencing obligations and identifying the compliance controls that apply to each obligation. Alternatively, **DNSPs** may choose to structure their annual report by identifying the main compliance controls they have put in place. If the latter approach is adopted, it is important that **DNSPs** clearly map the range of compliance controls they have in place back to each ring-fencing obligation, so that it is clear how compliance with each obligation is being met.

3.3 Meaningful compliance reporting

In general, we encourage **DNSPs** to adhere to the following principles when writing annual compliance reports:

- Report on specific measures, areas of the business, or challenges, rather than describing compliance measures in general, vague, or abstracted terms;
- Targeted reporting on areas of the business that carry greater likelihood of breaches of the **Guideline** or which have experienced previous breaches over the course of the **regulatory year**;
- Avoid jargon and technical language where possible and keep compliance reporting clear and as 'plain English' as possible; and
- Keep the report as succinct as possible and refer to previous reports if relevant.

Reporting that only describes compliance measures at a very high level can make it difficult for the reader to understand what specific measures have been undertaken. It is important that broad descriptions of overarching compliance measures are supported by more specific and tangible analyses of how those overarching compliance principles are being put into practice. In particular, **DNSPs** should consider providing greater detail on how ring-fencing safeguards are being put into practice in higher risk areas of the business, and whether those safeguards have been demonstrated to be adequate.

3.4 Reporting breaches in the annual compliance report

Under clause 6.2.1(b)ii any breaches of the **Guideline** by the **DNSP** must be reported in the annual compliance report. This means that any breaches in the reporting period (whether or not already reported to the AER) must be reported in the annual compliance report.

DNSPs should respond to any breaches or exceptions noted by the independent assessor. The response should include an explanation of the breach, actions taken to address any issues relating to the breach, an assessment of the possible detriment and the timeline for any corrective and remedial actions.

3.5 Reporting other services

Clause 3.1 of the **Guideline** sets out the specific circumstances under which **DNSPs** can provide **other services** without breaching the **Guideline**. In accordance with 6.2.1(b)iii these services must be reported in the annual compliance report.

In order to adequately demonstrate that other services are provided in accordance with the **Guideline**, **DNSPs** should describe each service clearly and in sufficient detail so that the nature of the service being provided is clear. **DNSPs** should also describe any measures or controls that have been put in place in relation to the delivery of other services to comply with the **Guideline**.

3.6 Reporting transactions with affiliated entities

Clause 6.2.1 (b)iv of the **Guideline** requires a **DNSP** to report on the purpose of all transactions between the **DNSP** and its **affiliated entities**. Where a set of individual transactions share a common purpose, the **DNSPs** may group those together with the number of transactions and the total dollar value to be recorded in their respective columns. Transactions share a common purpose if they:

- form part of the same course of transactions;
- are for the same or similar items; or
- there are other factors that indicate that the transactions are substantially similar.

DNSPs should also identify the affiliate entity involved in the transactions. Reporting on transactions with **affiliated entities** should be underpinned by accounts that conform to relevant standards and requirements in the *Corporations Act 2001*. The **AER** may require that the **DNSP** submit relevant accounts related to transactions with **affiliated entities** in accordance with clause 6.4, clause 3.2.1(a)i, and clause 3.2.1(a)ii of the **Guideline**.

To assist the **AER** in interpreting this data and maintaining a working knowledge of relevant compliance arrangements, **DNSPs** should consider providing the **AER** with a complete list of all the **DNSP's affiliated entities** as part of their annual report.

3.7 Publication of DNSP annual ring-fencing compliance and independent assessment reports

The **AER** will publish **DNSP** ring-fencing compliance reports and the accompanying independent assessment on the **AER** website.

DNSPs may also elect to provide a confidential version of the annual compliance report and/or the independent assessor's report to the **AER**. Should **DNSPs** wish to report information in confidence, they can do so in accordance with the **AER's Confidentiality Guideline**.

This process requires that **DNSPs**:

- engage with the **AER** to discuss their confidentiality claim prior to lodgement of the document. The **AER** will work with **DNSPs** to reach a shared understanding of the confidentiality issues involved;
- submit a confidentiality template, as laid out in the Confidentiality Guideline, together with public and confidential version of the annual compliance and independent assessment reports; and
- engage with our stakeholder information process. The **AER** is unlikely to disclose information publicly where we consider that stakeholders have been given enough information to satisfy the objectives of the **Guideline**. If the **AER** considers that claimed confidential information is central to achieving these objectives, we will engage with the **DNSP** to determine an approach to this information. This might involve measures such as narrowing the confidentiality claim or adjusting the information to protect sensitive elements.

4 Independent compliance assessment

Clause 6.2.1(c) of the **Guideline** requires that a **DNSP**'s annual compliance report be accompanied by an assessment of compliance by a suitably qualified independent authority. **DNSPs** will bear the cost of this assessment.

4.1 What is a 'suitably qualified independent authority'?

The **AER** will need to be satisfied that any party selected by the **DNSP** to provide an assessment of compliance is both independent and suitably qualified. We discuss each concept below.

4.1.1 Independence

Independence means that the person conducting the assessment should not be a director, **officer** or employee of the **DNSP** or an **affiliated entity** (including parent or associate companies whether in Australia or overseas), and there should be no perceived linkages or conflicts of interest that would prevent the assessor from entering into an assurance agreement.

DNSPs should engage an external third-party compliance assessor to conduct the assessment. The terms and practice of the assessment engagement should not compromise the position of the assessor as a third-party examiner of the **DNSP**'s compliance.

DNSPs may engage third-party assessors that have previously been contracted to do work for the **DNSP**. For example, a third-party that provides **Regulatory Information Notice (RIN)** auditing or other regulatory services for the **DNSP** may also be engaged to provide independent assessment of ring-fencing compliance.

DNSPs and assessors should apply established codes of conduct and standards in order to demonstrate professional independence.

We expect that **DNSPs** should rotate their independent assessors at least every five years to ensure that the assessor's independence is not compromised by performing many successive assessments of the **DNSP**'s ring-fencing compliance.

4.1.2 Suitably qualified

A suitably qualified assessor should have a track record of contracted compliance assessment and audit engagements across a range of different clients. An assessor that has only undertaken a limited number of compliance engagements, or who has only undertaken compliance engagements for a small number of clients in the past may not be judged by the **AER** to be suitably qualified. The **AER** considers that an assessor who meets the requirements in ASAE 3000, ASAE 3100, ASQC 1 or another similar standard will be suitably qualified.

4.1.3 Demonstrating that an assessor is suitably qualified and independent

In order to satisfy the requirements under clause 6.2.1(c) of the **Guideline**, the assessor's report should include a statement demonstrating that the assessor is both a "suitably qualified" and an "independent" authority. This could be achieved by:

- providing a statement regarding any relevant professional standards and codes of conduct that were applied to the assessment engagement, and why those were the most appropriate standards and codes of conduct to satisfy the **Guideline** requirements; or

- providing a conflict-of-interest statement signed by the independent assessor, which would describe any real or perceived conflicts of interest and explain how they have been managed through the course of the assessment engagement.

4.2 Assurance level

The independent assessor should be engaged to provide reasonable assurance that the **DNSP** has complied with the **Guideline**.⁹ Our view is that the most appropriate standard for this assurance is ASAE3100. This means that the assessor should provide assurance that:

- compliance measures or controls reported by the **DNSP** in its annual report are reflected in day-to-day business practices and are appropriate with respect to the **Guideline** obligations;
- all breaches that the organisation is aware of are accurately reflected in the compliance report, and that the description clearly and accurately reflects the nature and cause of each breach;
- all **other services** provided by the **DNSP** are accurately recorded in the compliance report; and
- transactions reported under 6.2.1(b)iv are an accurate reflection of all agreements, arrangements or other dealings (including in relation to the supply of goods or services) between the **DNSP** and its **affiliated entities**, and the purpose of those transactions is accurately reflected in the report.

DNSPs and their assessors should discuss with the **AER** if they consider that a different standard is more appropriate.

In order to establish the assurance level of the independent assessment, we would also expect to see the following included in the annual report and independent assessor's report:

- details of the assessment methodology and how relevant standards were used to design that methodology and implement the assessment. This could include a description of the type of sampling and auditing procedures used to assess **DNSP** compliance against ring-fencing obligations, and how the assessment methodology aligns with relevant ISO or ASAE standards chosen to guide the assessment. This statement should be sufficient to enable the **AER** to conclude that the assessment methodology was robust enough to satisfy the requirement for reasonable assurance; and
- a statement from the assessor detailing any limitations of the assessment, and areas of the assessment where information was inconsistent, incomplete, or incorrect, and the degree to which this has negatively impacted the assurance level.

The **AER** considers that the assurance level required to demonstrate compliance in relation to ring-fencing is higher than in other circumstances, such as **RIN**. This is due to the highly qualitative nature of ring-fencing compliance. The **AER** may consider requesting a lower level of assurance in future years, or limiting the scope of the assessment, once **DNSPs** establish a solid base of demonstrated compliance.

The assessor's report should clearly identify the nature of any issues, concerns, and recommendations for improvement that were raised in the course of the independent assessment that may or may not have been subsequently addressed by the **DNSP**.

⁹ "Reasonable assurance" is defined in Australian Standards Board, ASAE3000: Assurance Engagements Other than Audits or Reviews of Historical Financial Information.

4.3 Types of assessment

DNSP independent assessments should provide reasonable assurance covering all obligations within the **Guideline**. However, the **AER** may request the **DNSP** to target specific compliance areas in the independent assessment. This could allow the **AER** to target specific areas of compliance for independent assessment in the future or opt for an independent assessment on the basis of limited assurance. Changes to the scope of future reviews would be contingent upon **DNSPs** establishing a solid base of demonstrated compliance. Prior to adjusting the mode of assessment the **AER** would consult with **DNSPs**.

4.4 Expectations of independent assessor

Broadly speaking, the **AER** expects that an independent assessment of compliance should clearly address core ring-fencing compliance issues, including but not limited to:

- were any previously unknown or unreported compliance breaches discovered as a result of the assessment?
- what areas of ring-fencing compliance were identified as being weak or at risk of future breaches and why?
- what areas of ring-fencing compliance were identified as being strong or at low risk of future breaches and why?
- what recommendations does the assessor have to improve the **DNSP's** ring-fencing compliance framework?

The **DNSP** may also provide information to the **AER** regarding how the **DNSP** intends to respond to any recommendations for improvement raised by the independent assessor.

5 AER compliance reporting

The **AER** may report on ring-fencing compliance from time to time, drawing upon **DNSP** annual compliance reporting, breach reporting and our own investigations. The purpose of this reporting will be twofold:

- To increase the transparency of the ring-fencing regime in order to maintain confidence in the competitiveness of markets for contestable electricity services. This will support achieving the **Guideline**'s objective of promoting competition in the provision of electricity services; and
- To aid **DNSPs** in strengthening measures that can prevent breaches of the **Guideline** from taking place. Our reporting will focus on creating a culture of compliance by **DNSPs** and their affiliate entities, in line with our *Compliance and Enforcement Policy*.¹⁰

A **DNSP**'s compliance measures may be found to be weak as a result of the information provided in their ring-fencing compliance annual report and accompanying independent assessment. This could be evidenced by systemic breaches that have already taken place, or perceived risk that breaches may take place in the future as a result of poor compliance measures. If this occurs the **AER** will take steps, including engaging with the business and affected parties, to determine what compliance measures are required.

¹⁰ This is the up-to-date title at the time of publication.

6 Our approach to handling ring-fencing complaints

Clause 6.1 of the **Guideline** allows the **AER** to require the **DNSP** to demonstrate the adequacy of internal compliance procedures upon reasonable notice. We will seek information from **DNSPs** in response to complaints or concerns where we consider that there are reasonable grounds for investigating these matters further.

Clause 6.4 of the **Guideline** allows the **AER** to require a **DNSP** to provide a written response to a complaint or concern the **AER** raises with the **DNSP** about its compliance with the **Guideline**.

7 Compliance breaches

Clause 6.3 of the **Guideline** requires a **DNSP** to notify the **AER** in writing within 15 business days of becoming aware of breaches of its obligations under the **Guideline**. Two administrative clauses are an exception to this requirement and a **DNSP** will not be required to report breaches of these clauses within 15 days. Breaches to the two administrative clauses can be reported as part of a **DNSP**'s annual compliance report. The administrative clauses are:

- clause 6.2.2 – submitting annual compliance reports within the required timeframe; and
- clause 6.3 – failure to report a breach of the **Guideline** within the required timeframe.

The **AER** has provided 2 templates for reporting breaches under clause 6.3 of the **Guideline**:

- a cover letter template for reporting of breaches (word document); and
- a breach reporting template (spreadsheet)

The reporting template guides the form and content of the initial report. It requires the reporting of specific information, including:

- a description of the breach (obligation breached, dates over which breach occurred and the nature of the breach);
- how the breach was identified;
- the impact of the breach on achieving the **Guideline** objectives in clause 1.1.1 of the **Guideline**;
- remediation measures that the **DNSP** has taken or plans to take; and
- any past breaches of the same **Guideline** obligation.

The final column, 'other', allows **DNSPs** to add any additional information at their own discretion. These templates are available on the **AER** website.

DNSPs should email breach reports to AERringfencing@aer.gov.au and clearly identify that they are reporting a breach.

While these templates are for guidance, we strongly suggest that **DNSPs** make use of them in order to allow the **AER** to assess initial data in a timely manner. We have made the breach reporting template purposely brief to enable **DNSPs** to report promptly on breaches. In addition to the letter and spreadsheet breach report templates, a **DNSP** may provide any further attachments it considers pertinent to the matter. This can be done at the **DNSP**'s discretion and must not hold up timely reporting of breaches to the **AER**. To that end, in order to use the suggested templates effectively and ensure that the **Guideline** requirements are met:

- the template cover letter should be signed by an **officer** responsible for the most relevant division of the business; and
- **DNSPs** should report one breach per row of the breach reporting template spreadsheet. Should a **DNSP** wish to report multiple breaches at the same time they can use one breach report file to report multiple breaches, with each breach being a new row in the template.