




**CitiPower and Powercor
| 2020 Ring-fencing
compliance report
| April 2021**



This page is intentionally blank.

Table of Contents

1	INTRODUCTION	4
1.1	Background	5
1.2	Purpose	5
1.3	Corporate overview	6
1.4	Definitions	7
1.5	Contact details	7
2	MEASURES TO ENSURE COMPLIANCE	8
2.1	Annual compliance report and audit	9
2.2	Prevention of cross subsidies	11
2.3	Offices, staff, branding and promotions	12
2.4	Information access and disclosure	14
2.5	Conduct of service providers	15
2.6	Staff training	16
2.7	IT system controls	17
2.8	Statement of compliance	18
3	WAIVERS	19
3.1	Waivers	20
4	COMPLIANCE AND ENFORCEMENT	21
4.1	Compliance framework	22
5	COMPLAINTS AND BREACH REPORTING	37
5.1	Complaints and investigations	38
5.2	Breach reporting	38
5.3	Material breaches	41
5.4	Other services provided	41
6	TRANSACTIONS WITH AFFILIATED ENTITIES	42

1 Introduction

1.1 Background

On 30 November 2016 the Australian Energy Regulator (**AER**) released its Electricity Distribution Ring Fencing Guideline (**Guideline**) as made under clause 6.17.2 of the National Electricity Rules (**NER**). The Guideline commenced on 1 December 2016 and incorporates amendments made from time to time.

On 17 October 2017, the AER released a final amended Ring-fencing Guideline (version 2) and accompanying Explanatory Statement against which compliance has been assessed by CitiPower and Powercor. Under clause 6.17.1 of the NER, the Guideline is binding on distributors and seeks to prevent them from providing their affiliates, operating in unregulated markets, from having an unfair advantage, thus seeking to promote competition in the provision of electricity services.

The Guideline includes provisions in the following three broad areas:

- cross-subsidisation—preventing distributors from using regulated revenues to subsidise activities in unregulated markets
- discrimination—ensuring distributors treat affiliates and third parties equally
- information sharing—providing electricity information to all parties on an equal basis.

The AER is currently reviewing version 2 of the Guideline. Until such a review is finalised and implemented, distributors are bound by version 2 of the Guideline.

1.2 Purpose

The Guideline requires CitiPower and Powercor to prepare an annual ring-fencing compliance report for submission to the AER each regulatory year.

This Annual Ring Fencing Compliance Report (**report**) has been prepared by CitiPower Pty Ltd (ACN 064 651 056) and Powercor Australia Ltd (ACN 064 651 109) (**CitiPower, Powercor, we, us, our**) for the year ended 31 December 2020 (**regulatory calendar year**). In accordance with the clause 6.2.1(a) of the Guideline, this report identifies and describes:¹

- the measures we have taken to ensure compliance with our obligations
- all 'other services' we provided
- the purpose of all transactions between us and affiliated entities
- any breaches of the Guideline.

In accordance with section 6.2.2 of the Guideline, an annual compliance report must be submitted to the AER within four months of the end of the regulatory year to which the compliance report relates. For CitiPower and Powercor, this means the annual compliance report must be submitted by 30 April of the subsequent year.

This report represents CitiPower and Powercor's annual ring-fencing compliance report for the regulatory year ending 31 December 2020. This report covers the period from 1 January 2020 to 31 December 2020.

This annual compliance report is accompanied by an independent assessment of compliance conducted by Deloitte, a suitably qualified independent authority (Attachment A). The assessment has been prepared in accordance with Australian Standards on Assurance Engagements ASAE 3100 Compliance Engagements issued by the Australian Auditing and Assurance Standards Board. Deloitte has conducted its assessment on a

¹ AER, Ring fencing Guideline, version 2, October 2017, 6.2.1(b).

reasonable assurance basis in accordance with the AER's Ring fencing compliance reporting best practice manual version 2.²

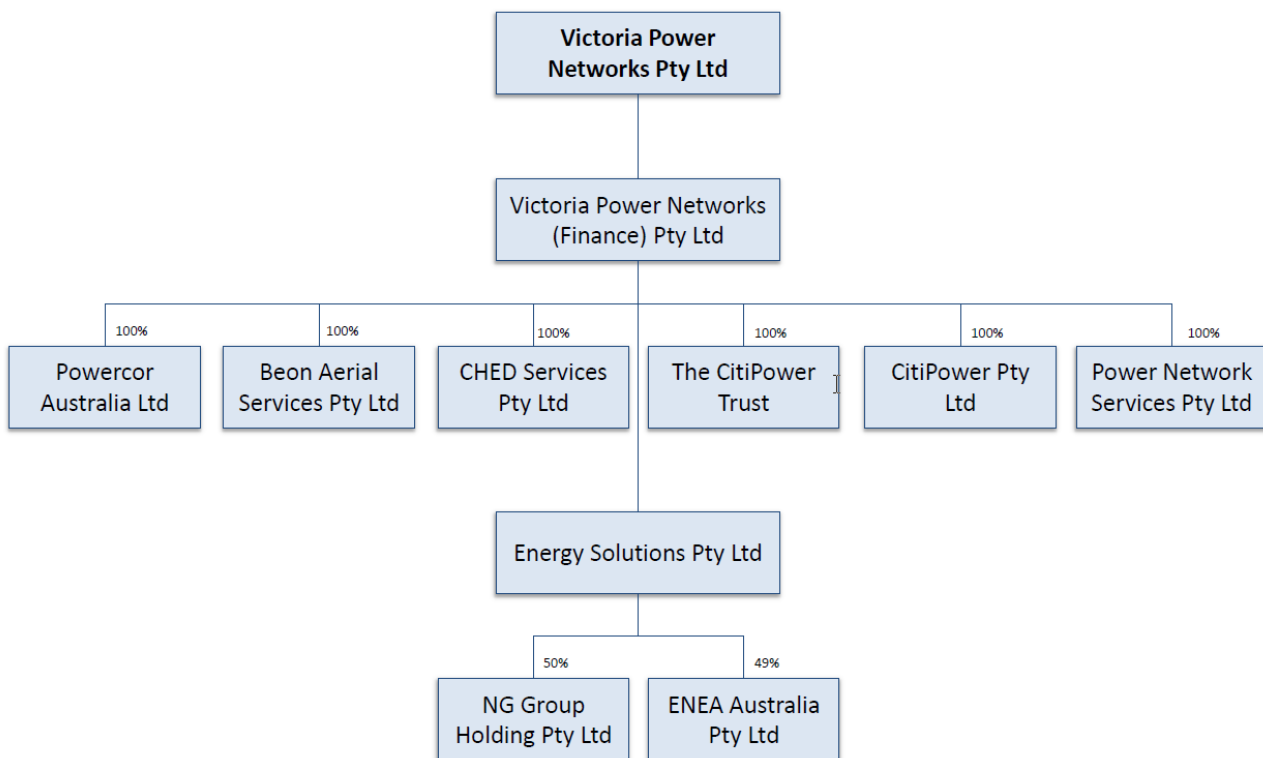
We are not aware of any new material breaches of the obligations outlined in the Guideline. We note we did discover an immaterial breach in September 2020 and reported this to the AER within five business days as required under the Guideline.³ Please see section 5.2 for further information.

This report should be read together with our compliance strategy and waivers as published on our and the AER's websites.

1.3 Corporate overview

The figure below overviews our corporate structure at the end of 2020.

Figure 1 Overview of the CitiPower and Powercor corporate structure



Source: CitiPower and Powercor

Energy Solutions Pty Ltd trading as Beon Energy Solutions (**Beon**), CHED Services and Power Network Services (known as Network Services) are directly affiliated with us:

- Beon provides large-scale renewable energy and infrastructure projects, as well as design, construction and maintenance services which are contestable energy services for the purposes of the Guideline
- CHED Services Pty Ltd provides corporate services primarily to us, as well as to affiliates

² AER, Ring-Fencing Guideline compliance reporting best practice manual version 2, July 2019

³ AER, Ring fencing Guideline, version 2, October 2017, 6.3.

- Power Network Services Pty Ltd provides design and field services primarily to us, as well as to affiliates and third parties.
- Beon Aerial Services (ABN 39 639 114 257), which provides LiDAR vegetation management services to CitiPower, Powercor and United Energy.

Beon also has ownership interests in other entities, specifically:

- Next Generation Electrical Group Pty Ltd (ABN 20 152 831 028) (**NG/E**), which provides engineering, procurement and construction services, which are contestable electricity services for the purposes of the Guideline.
- ENEA Australia Pty Ltd (ABN 32 610 146 104) (**ENEA**), which provides advice and support for companies in the energy sector. To CitiPower and Powercor, they provide a range of services including code reviews, forecasting, case studies, strategy modelling, policy writing, financial analysis, risk modelling, tax support and strategy development. The activities of ENEA do not fall within the definition of contestable electricity services, and thus are not a related electricity service provider for the purposes of the Guideline. For completeness, they are included within this ring-fencing compliance report to ensure appropriate controls exist between ENEA and Beon.

Other indirect affiliates do not appear in our corporate structure because they have other distinct parent ownership (or ownership shareholdings), or operate networks in distinct locations and with different management. We have not included those indirect affiliates within this compliance report.

1.4 Definitions

Unless otherwise defined, terms used in this report have the meaning given to them in section 1.4 of the Guideline.

1.5 Contact details

The contact person for further details in relation to this report is:

Brent Cleeve
 Head of Regulatory Policy and Compliance
 CitiPower, Powercor and United Energy
 40 Market Street, Melbourne VIC 3000
 Ph. (03) 9683 4465

2 Measures to ensure compliance

2.1 Annual compliance report and audit

Clause 6.2.1(b)(i) of the Guideline requires that the annual compliance report must identify and describe, in respect of the regulatory year, the measures the distributor has taken to ensure compliance with its ring-fencing obligations.

We have applied the Guideline in accordance with our understanding of it as detailed in our compliance strategy.⁴

Deloitte conducted its 2020 regulatory year audit in two stages, with the first part conducted in November 2020 and the second part conducted in March 2021.

The scope of the Deloitte engagement included:

- interviewing key staff members responsible for legal, accounting and operational activities
- understanding the process for identifying and reporting breaches of the Guideline
- examining, on a test basis, the key controls that exist and the evidence supporting compliance
- reviewing the compliance report prepared by management and confirmed that the report has been prepared in accordance with the Guideline.

Deloitte is a suitably qualified independent auditor in accordance with the Guideline and the AER's audit guidance note.

2.1.1 Key risk areas

The ring fencing audit and feedback from the AER relating to the 2019 year highlighted risk areas where we should focus our efforts to continue to improve our controls.

The key risk areas identified were:

- framework to monitor identified potential breaches and to rectify these within a timely manner, where:
 - there was no formal documented policy for reporting breaches to the regulatory compliance team
 - the materiality guideline adopted by the business was not consistent with the guidance in the AER best practice compliance manual which may result in inconsistent assessments of breaches identified
 - training materials did not contain a clear policy for reporting breaches
 - there was limited information on reporting of breaches on the intranet
- attestations, where these are not completed in a timely manner
- staff sharing register, where the register was not considered to be sufficiently comprehensive
- training, where the ring-fencing online training failed to achieve a satisfactory completion rate
- building control, where ENEA and N/GE staff were not included in the building access controls

IT risks included:

⁴ <https://www.aer.gov.au/system/files/Compliance%20Plan%20-%205%20May%202017.pdf>

- affiliate staff gaining access to confidential information of the regulated business through inappropriate access to ring-fenced IT systems
- Powercor staff moving to Beon and retaining access to IT systems of the regulated business
- a lack of automation of updating employee restrictions and email addresses when staff transfer between CitiPower/Powercor and Beon

2.1.2 Strengthening of controls to address key risk areas

In 2020 we undertook the following activities to strengthen our controls in response to auditor and internal feedback:

1. Implementation plan – we developed a plan detailing how we would implement our auditor’s recommendations from the 2019 audit. This included accountabilities and deliverables. We successfully delivered on all the auditor recommendations by the deadlines we set ourselves. This outcome was then reported to the Risk Management Compliance Committee.
2. Ring-fencing champions working group – on the advice of our independent auditors, we created a ring-fencing champions working group which meets every month to discuss breaches and control. The represented parts of the business are: IT, Finance, Procurement, Network Services, Facilities, Legal, Regulation, Human Resources and Contact Centre. These groups were chosen because they represent ‘at-risk’ parts of the business. Either there have been breaches in prior years directly related to these areas, or we have identified that breaches in these areas are theoretically possible. In the champions meetings, Regulation provides an update on ring-fencing controls, changes and anything identified as being potentially problematic. Anyone from the champions group or the business at large can request for an item to be put on the agenda; this can include concerns around control efficacy or if a potential breach has been identified. All agenda items are discussed and actions are taken to follow up appropriately.
3. Breach reporting policy – developed a comprehensive materiality and breach reporting policy in consultation with key at-risk business units and the ring-fencing champions working group. The policy was developed with input from the champions who each reviewed and marked up the policy as it was drafted. Further, these champions presented the draft policy in their team meetings to gain feedback from staff. The policy sets out our process to identify, investigate and report breaches as they arise. We committed to using this policy should breaches arise. The assessment framework in the policy is consistent with the AER’s own framework used to assess the materiality of breaches. This policy is available to all staff on the intranet, and additionally was provided to all champions who in turn presented the final policy at their subsequent team meetings. The champions provide a touchpoint for their teams and regularly train their teams on the policy.
4. Confidential information review – as part of the implementation plan, in August 2020 we undertook a comprehensive review of confidential information of the regulated business. This included reviewing all at-risk systems in the business, being those which potentially may house confidential information for the purposes of ring-fencing. As a result of this review, we concluded that the existing list of ring-fenced IT systems was still appropriate and that the list did not need to be changed. We further reviewed and analysed our controls that prevented confidential information being shared with unregulated affiliates. We assessed that our controls which have been progressively refined after each audit are succeeding at preventing confidential information of the regulated business being accessed by our unregulated affiliates and that no change was required.
5. Automating attestations—in the prior year, responsibility for obligations were assigned to key staff in a position to ensure compliance or who were working in high risk areas. These staff provided periodic

paper attestations of compliance to the Regulation team which centrally monitored and enforced compliance. In 2020, we partially automated the verifying and attestation process by replacing the paper system with an electronic system called Quantate Compliance. Quantate Compliance removes the need for paper-based attestations, which we have used in the past. In Quantate, staff with ring-fencing responsibilities are sent an email prompt reminding them to complete their attestations. They then complete the attestation in Quantate. If they do not complete the attestation in a timely manner, they are sent repeated reminders until they complete it.

6. Strengthened staff sharing register – we comprehensively reviewed and updated our staff and office sharing register. It was broadened to include more detail around roles, as well as an analysis of each role against the provisions of the ring-fencing guideline.
7. IT access controls—automated access controls to a number of IT systems containing confidential electricity information, continued to complete in-person training with system owners of ring-fenced IT systems, completed a six-monthly full security review over IT systems, and continued to undertake monthly and six-monthly attestations (see section 2.7 for more detailed information).
8. Building access controls – we expanded the scope of the facilities controls to include staff from ENEA and NG/E.
9. Training – the online ring-fencing training was redesigned and redeployed in 2020 and rolled out again to all office-based staff. Further, in late 2020 we developed a separate field staff specific ring-fencing training which has now been rolled out. The training covers issues specific to field staff, who are likely to interact with the public. It emphasises the requirement to not recommend affiliates to the public.

Controls are continuing to evolve and will continue to be expanded upon and prioritised in 2021.

2.2 Prevention of cross subsidies

2.2.1 Legal separation

In accordance with clause 3.1 of the Guideline, CitiPower and Powercor may provide distribution services and transmission services but must not provide other services.

CitiPower Pty Ltd (ACN 064 651 056) and Powercor Australia Ltd (ACN 064 651 109) are registered in Australia by Australian Securities and Investment Commission (**ASIC**) under the *Corporations Act 2001* (Cth) and are, for the purposes of the Guideline, legal entities.

CitiPower and Powercor are stand-alone electricity distribution network service providers that only provide distribution services within our licensed distribution service area. Set out below are the categories of distribution services we provided during 2020, which are consistent with the AER's Victorian electricity distribution network service provider's final determination for the 2016–2020 regulatory control period:

- standard control services
- alternative control services
- negotiated and unclassified services, as approved in our waiver application.

We provided these distribution services to:

- electricity retailers
- end-use customers
- others—registered electrical contractors (**REC**), builders, developers, public lighting authorities including local councils and VicRoads and other distribution network service providers.

We have not provided any other material services as prescribed under the Guideline.

A separate affiliated entity, Beon, was established to perform “other services” outside distribution and transmission services which are performed by CitiPower and Powercor.

2.2.2 Establish and maintain accounts

In accordance with clause 3.2 of the Guideline, we establish and maintain appropriate internal accounting procedures to demonstrate the extent and nature of transactions between CitiPower and Powercor and affiliated entities.

Established documented work procedures are in place for Finance staff which provides instruction on how accounts are to be separated.

During the year we maintained a separate set of accounts for our businesses that are separate from our affiliate's accounts. Our 31 December 2020 financial statements were subject to an annual statutory audit engagement and our internal accounting procedures will be provided to the AER through the annual Regulatory Information Notice (**RIN**) responses in April 2021.

It is standard practice that monthly reviews of the financial balance sheets are undertaken to confirm that transactions have been allocated to the correct accounts. Discrepancies are immediately rectified. Established documented work procedures are in place for Finance staff which provides instruction on how costs are to be allocated amongst accounts.

During the year we ensured that costs for distribution services were allocated in accordance with the Cost Allocation Principles. Our Cost Allocation Methodology (**CAM**), as approved by the AER, is also the basis of our annual audit during the RIN process, the results of which will be provided to the AER in April 2021.

Responsibility for compliance with the CAM principally rests with CitiPower and Powercor's Chief Financial Officer. The day-to-day responsibility for the CAM, including updating, maintaining, applying, internally monitoring and reporting on its application, including ensuring compliance is the responsibility of the finance team.

Our integrated business management system (**SAP**) is used to collect and record expenses and revenues including:

- the Chart of Accounts classifies all expenses and revenues by General Ledger account numbers, which map to reporting categories on the balance sheet, and profit and loss statement
- each expense or revenue transaction is also assigned to a profit centre. Each cost item is assigned to a function code and in some cases an activity type
- the records maintained in the SAP system, the processes for inputting records into the SAP system and corporate service break down of fees can be reviewed.

The basis of directly attributing costs in accordance with the CAM can therefore be readily verified by an independent third party and the outcome can be replicated.

Each month, Finance representatives complete attestations confirming separate accounts have been maintained.

2.3 Offices, staff, branding and promotions

2.3.1 Physical separation/co-location

In accordance with clause 4.2.1 of the Guideline, CitiPower and Powercor use offices that are separate from any offices from which affiliated entities provide contestable services.

CitiPower and Powercor are located at 40 Market Street, Melbourne, whilst Beon is located at 11 Tavistock Place, Melbourne.⁵

We note the following key controls to ensure the ongoing physical separation from affiliates:

- Beon, NG/E and ENEA staff are restricted from accessing Market Street through their security access passes.
- Every morning, the facilities team run a check of everyone with access to the Market Street office. If any affiliate staff are identified as having access without a valid reason under the ring-fencing guideline, then they are immediately barred from accessing Market Street in the Gallagher security system. Access is then modified to ensure entry to restricted floors is not allowed going forward.
- Monthly reports are run by the facilities team to demonstrate staff building access at a point in time. This report is reviewed by the Facilities Manager to ensure the accesses for the contestable service providers' staff remain restricted as appropriate for compliance with the Guideline, and any discrepancies are rectified. An attestation is then completed by the Facilities Manager on a monthly basis.

2.3.2 Staff sharing

In accordance with clause 4.2.2 of the Guideline, CitiPower and Powercor staff that are involved in the provision or marketing of direct control services are not involved in the provision or marketing of contestable services for affiliated entities.

CitiPower and Powercor maintain a staff sharing register, which is reviewed on an annual basis and was comprehensively reviewed and updated to include more detail in 2020. The staff sharing register is available publicly on the CitiPower/Powercor website.

2.3.3 Branding and cross promotion

In accordance with clause 4.2.3 of the Guideline, CitiPower and Powercor use branding that is independent and separate from that used by affiliated entities in providing contestable services. Also, CitiPower and Powercor do not advertise or promote direct control services and contestable services together, or contestable services provided by affiliate entities.

2.3.4 Office and staff registers

In accordance with clause 4.2.4 of the Guideline, CitiPower and Powercor has established, maintained and kept registers of offices and staff to which the staff sharing and office sharing obligations do not apply.

To ensure CitiPower and Powercor do not confer an unfair advantage on affiliates, we are required to publish staff sharing and office sharing registers.

In accordance with the Guideline, certain staff are allowed to be used, or shared, by us and our affiliates. Staff must be included on the register if they are eligible to be shared provided they:

- do not have access to electricity information - per cl. 4.2.2(b)(i)(a)
- have access to electricity information but do not have the opportunity, in performing their the roles, functions or duties of their position, to use electricity information to engage in discriminatory conduct - per cl. 4.2.2(b)(i)(b)

⁵ For completeness, we note that ENEA Consulting is located at Level 12, 360 Elizabeth Street, Melbourne VIC 3000; and NG/E is located at 3 Stewart Street, Richmond, Vic 3121.

- fall within a list of specific functions as outlined - per cl. 4.2.2(b)(i)(c), or
- are an officer for us and the related electricity service provider - per cl. 4.2.2(d).

The publicly available staff sharing register comprises of a description of the shared staff positions and the services they provide, with which entity they are shared and the reason they may be shared. The ring-fencing compliance strategy published on our website describes the access to, and way in which, shared staff use electricity information in performing their roles in more detail.

The Guideline also allows certain offices to be shared. The office register includes a list of all offices where staff listed on the staff sharing register are located, or the location of staff that only have access to electricity information for the purpose of providing corporate services. Not all staff at the listed locations are shared.

The staff and office sharing registers were comprehensively updated in 2020, and can be found on our website at <https://www.citipower.com.au/what-we-do/the-network/codes-and-guidelines/> and <https://www.powercor.com.au/what-we-do/the-network/codes-and-guidelines/>.

2.4 Information access and disclosure

2.4.1 Protection of confidential information

In accordance with clause 4.3.3 of the Guideline, CitiPower and Powercor do not disclose confidential information to any person, including affiliated entities, except in specified circumstances.

We consider that the protection of confidential information is a key ring fencing compliance risk. In accordance with the information sharing provisions of the Guideline we keep an information sharing protocol which outlines the circumstances under which we will provide information to affiliates and other legal entities. An information register is also kept to give effect to the principle of equal access to information. The operation of the register is described in the protocol.

2.4.2 Disclosure and sharing of information

In accordance with clause 4.3.4 of the Guideline, CitiPower and Powercor provide access to any confidential information that is disclosed to an affiliated entity on an equal basis.

For the period 1 January 2020 to 31 December 2020, no confidential information was shared by CitiPower and Powercor and its affiliated entities, and no requests for access to our information register by competitors or potential competitors was received.

2.4.3 Information register

In accordance with clause 4.3.5 of the Guideline, CitiPower and Powercor has established, maintained and kept registers of affiliated entities and all legal entities who provide contestable services.

The information register is one of the Guideline's mechanisms to ensure we provide eligible confidential electricity information to affiliates and third parties on an equal basis. Consistent with the Guideline, our register operates in the following way:

- affiliates, and non-affiliated entities that compete or are seeking to compete with our affiliates, who request access to confidential electricity information will be placed on the register (registered parties)
- registered parties must provide us with a description of the kind and purpose of confidential electricity information they would like to receive
- if an affiliate requests (and is provided with) information that matches the kind and purpose of information described by non-affiliated registered parties, that information will be provided to those non-affiliated registered parties on an equal basis

- if an affiliate has paid a fee to receive eligible confidential electricity information (in accordance with rules or procedures), then other registered parties will receive a notification that they can receive the same information if the same fee is paid
- information will be provided to registered parties on terms and conditions that require them to comply with the obligation to protect the information and to only disclose it to third parties (including affiliates) only on the basis of clause 4.3.2 and 4.3.3 (a)-(d) of the Guideline

Both the information sharing protocol and Information register are subject to an annual review and can be found here - <https://www.citipower.com.au/what-we-do/the-network/codes-and-guidelines/> and <https://www.powercor.com.au/what-we-do/the-network/codes-and-guidelines/>. In 2020 we added one non-affiliated party to the register at their request.

2.4.4 Website

In accordance with our current business practice, information for our corporate websites must be approved by Corporate Affairs prior to publication. Our training to Corporate Affairs has ensured these staff are aware of their obligations to not promote affiliates or their services on the website.

There are no references to affiliated contestable service providers on our websites. An annual review is conducted to continue to ensure that the website continues to be compliant.

2.4.5 Call centre and printed materials

Scripts used by Contact Centre staff contain no references which could advantage affiliated entities. These scripts are reviewed annually.

To date we have not identified any printed material which advertises or promotes services provided by a related electricity service provider.

2.5 Conduct of service providers

In accordance with clause 4.4.1 of the Guideline, CitiPower and Powercor ensure that any new or varied agreement that it enters with a service provider requires the service provider to comply with the obligations relating to non-discrimination, office sharing, staffing and the protection of confidential information.

A legal review was undertaken in 2019 on our existing set of standard terms and conditions for service providers to ensure that any new or varied contracts are aligned with the Guideline.

Procurement staff were trained on the principles of ring-fencing in September 2017 and again in July 2019. The July 2019 training was an in-person group session conducted by the Regulation team and focused on how to apply ring-fencing principles when engaging a service provider. The in-person training was intended to be provided again in July 2020 however due to COVID this was pushed back and eventually delivered in January 2021.

A Regulation team member is available at all times to assist Procurement staff with ring-fencing queries.

The standard ring-fencing terms and conditions used in procurement contract and purchase orders are periodically reviewed by Procurement and Legal.

Procurement have implemented ring-fencing related KPIs so that their staff are financially incentivised by the company's bonus scheme to prevent ring-fencing breaches.

A decision framework to identify applicable contracts where ring-fencing clauses should be included is on the intranet. Procurement are made aware of this framework repeatedly at their team meetings, and additionally

regulation provides periodic training to the Procurement team, where this framework is covered and promoted to the team.

No breaches were identified in 2020 in the procurement space.

2.6 Staff training

Since 2018, we have had mandatory ring-fencing training for all office staff. This training was comprehensively refreshed in 2020. The training is required to be completed by all corporate staff and new employees as part of their induction training. Where training has not been completed, reminder emails are sent out from the Training team's automated iLearn platform to noncompliant individuals, and separately from the General Manager of Regulation, strongly encouraging noncompliant individuals to complete the training.

Staff in the following corporate functions are required to complete training:

- Finance
- Contact Centre
- Connections
- Corporate Affairs
- Network Services
- Program Delivery
- Construction and Maintenance
- Design
- Network Technologies
- IT
- Planning
- Regulation.

The training covers the following topics and ring fencing clauses:

- Clause 3—Prevention of cross subsidies
- Clause 4.1—Obligation not to discriminate
- Clause 4.2—Offices, staff, branding and promotions
- Clause 4.3—Information access and disclosure

The training discussed the importance of complying with ring-fencing and the ramifications for not doing so. It also provided guidance for staff on the process to follow when they have ring-fencing queries. This includes seeking guidance from managers and sending queries to an internal ring-fencing mailbox to be answered by the Regulation team.

In late 2020 we developed a separate field staff specific ring-fencing training which has now been rolled out. The training covers issues specific to field staff, who are likely to interact with the public. It emphasises the requirement to not recommend affiliates to the public.

As of March 2021, our completion rate for the online training is 91%.⁶ The 9% who did not complete the training are largely staff who were on extended leave during the 2020 year – for instance staff on parental leave.

The online training is only one part of a much broader ring-fencing awareness program in the business.

The ring-fencing champions program complements the ring-fencing awareness program by reinforcing awareness with nominated champions from high-risk business units. These champions are then responsible for reinforcing awareness and compliance in their business unit.

When taken together, the online training combined with other awareness activities provides our employee base a strong level of awareness and knowledge about ring-fencing

2.7 IT system controls

IT access continues to be a key risk area, which past audits have identified as an area for improvement. In 2020 we reported no breaches relating to IT access controls.

In 2020, we worked further to strengthen our IT access controls and continued to reinforce existing controls. Amongst other actions, this included:

- The Regulation team conducted tailored in-person training to IT Service Desk staff, who have a level of control over access approvals in certain circumstances. The training covers the IT access decision tree which was developed by Regulation and is available to all Service Desk staff. It further covers the principles of ring-fencing as they apply to Service Desk staff.
- We continued to obtain monthly attestations from IT system owners to ensure that accesses to the various systems are appropriate, and continued to obtain a six-monthly attestation for the IT security review
- The IT attestation timeframe was amended, with responsible IT staff now required to complete monthly attestations on the first of the following month for the prior month.

Further, following audits into Identity and Access Management (IdAM, by Internal Audit) and Ring Fencing (by Deloitte), IT undertook a series of projects to improve Identity and Access Management across all entities. The projects identified and confirmed that employee information, inclusive of access, is owned by the business and IT facilitates change requests from Human Resources (HR) and Payroll (Finance).

Further to the proactive controls within IT for account provisioning, IT conducted a series of workshops with business representatives from Human Resources and Finance to further improve business processes and ensure changes are coordinated, communicated and completed in a consistent and timely manner.

Today, there are two types of key IT controls deployed:

- Preventative controls - consistent and accurate requests from the business, continued training and awareness within IT. Requests from IT staff include: contacting Regulation when unsure of ring-fencing controls, business owners being required to approve access and permissions, regular training to the IT Service Desk and reminders to IT system business owners of their ring-fencing obligations.
- Detective controls – monthly and six-monthly IT attestations, instigated from IT, and IT security audits and the ring-fencing audit.

⁶ This is a blended rate across CitiPower, Powercor and United Energy.

2.8 Statement of compliance

Other than the immaterial breaches set out in section 5.2, we confirm that we are compliant with the Australian Energy Regulation's (AER) Ring-fencing guideline (the Guideline) for the year-ended 31 December 2020.

3 Waivers

3.1 Waivers

Section 5 of the Guideline allows for a distribution network service provider (DNSP) to seek a waiver of obligations under clauses 3.1, 4.2 and/or 4.4.1(a) if certain conditions are met.

We sought three waivers in respect to:

- the provision of negotiated and unclassified services until the end of the current regulatory period when these services will be reclassified
- use of the Powercor Network Services brand (which includes the term 'Powercor') when undertaking unregulated services for large commercial and industrial customers
- use of the CitiPower and Powercor brand when undertaking unregulated field services for large commercial and industrial customers.

All waivers were granted by the AER, with an expiry date of 31 December 2019 for the branding waivers.

As required, we undertook significant implementation projects to transition to full compliance with respect to our branding waiver, which were completed by 31 December 2019.

Each of these waivers is maintained and kept in a register (including variations) in accordance with the Guideline and are publicly available on our website - <https://www.citipower.com.au/what-we-do/the-network/codes-and-guidelines/> and <https://www.powercor.com.au/what-we-do/the-network/codes-and-guidelines/>

4 Compliance and enforcement

4.1 Compliance framework

A corporate objective for CitiPower and Powercor is achieving full compliance with external obligations and audit requirements. Clause 6.1 of the Guideline requires distributors to establish and maintain appropriate internal procedures to ensure it complies with its obligations under the Guideline.

To this end, we have established frameworks, policies and processes designed to manage, monitor and report on compliance and to minimise the potential for breaches, fines or penalties, or loss of our distribution license. This has been prepared in accordance with the Australian Standard Compliance Programs (AS/ISO 19600:2015).

The Board has responsibility for ensuring the overall performance and has established a Risk Management and Compliance Committee (**RMCC**) to consider more complex issues in the areas of audit, risk management and compliance. The Executive Management Team (**EMT**) and the Chief Executive Officer are responsible for the effective management and compliance with all applicable regulation compliance obligations including ensuring all breaches are managed and reported appropriately.

Responsible managers within our businesses have been assigned to, and are responsible for, meeting compliance for specific economic regulation obligations. These obligations are allocated based on the activities of their position and include identification, management and reporting of any compliance breaches.

The Regulation Group is responsible for the overall regulatory compliance policy and framework, and ensures this policy is appropriate and effective in managing the economic regulation compliance risks of our businesses. The status of our economic regulation obligations are monitored, reviewed and where applicable, reported to the EMT and RMCC.

CitiPower and Powercor have assigned ring fencing authorities and responsibilities to our staff/teams, as set out in Table 1 below.

Table 1 Assigned authorities and responsibilities

Staff/team	Authorities and responsibilities
General Manager Regulation	<ul style="list-style-type: none"> • Approval of ring-fencing strategy
Regulation group	<ul style="list-style-type: none"> • Ensure the list of regional offices remains up-to-date by reconfirming the analysis that identified the offices, as appropriate, and updating the list, if the criteria in the Guideline change • Maintain a list of all the services offered by CitiPower/Powercor and ensure the delivery of them remains compliant with the Guideline obligations • Manage the confidential information disclosure and sharing process, including ensuring the information register and information sharing protocol are up-to-date • Manage the ring-fencing compliance monitoring and reporting process, including reporting to the Risk Management and Compliance Committee • Provide advice and support to managers, who are responsible for the ring fencing obligations • Ensure the staff, office and waiver registers are kept up-to-date • Manage the breach reporting process • Be a resource for all staff in the business to seek ring-fencing advice • Provide specific ring-fencing training as needed throughout the business
Finance group	<ul style="list-style-type: none"> • Create and maintain procedures that demonstrate the extent/nature of transactions between the distribution business and affiliated entities • Maintain records that demonstrate the process for allocating costs between Distribution Services carried out by CitiPower/Powercor and non-distribution services provided by an affiliated entity
Human Resources group, Corporate Affairs and Call centre	<ul style="list-style-type: none"> • Ensure that CitiPower/Powercor's approach to remuneration, incentives and benefits does not create an incentive for staff to act in a manner that is contrary to the Guideline • Ensure that there is no printed material or call centre scripts cross promoting CitiPower/Powercor and contestable businesses
Procurement	<ul style="list-style-type: none"> • Ensure that new and varied supplier contracts incorporate the amended terms and conditions as part of their contract management system • Incentivise procurement staff to ensure compliance with ring-fencing
Information technology	<ul style="list-style-type: none"> • Ensure that IT controls are effective to prevent access to confidential information by contestable businesses • Periodically review and complete attestations to ensure there are no IT access breaches

All employees

- Notify their manager and the Regulation group of new commercial opportunities so ring-fencing implications can be considered
- Ensure CitiPower/Powercor's competitors are not discriminated against, due to preferential treatment being given to their affiliates
- Refer any requests for confidential information by an affiliate or external party to the Regulation group
- Report any suspected breaches of the Guideline to the Regulation group or via email to the ring fencing mailbox

We use the Quantate Compliance Program for assigning and tracking compliance responsibilities. The ring-fencing obligations are included in this system. Further, as of 2020, we include the monthly and biannual ring-fencing attestations in Quantate.

Table 2 below summarises the controls taken to comply with each ring-fencing obligation.

Table 2 Controls for Guideline obligations

Guideline clause	Guideline text	Preventative controls	Detective controls
3 Prevention of cross subsidies			
3.1 Legal separation	<p>(a) A DNSP must be a legal entity</p> <p>(b) Subject to this clause 3.1, a DNSP may provide distribution services and transmission services, but must not provide other services.</p>	<ul style="list-style-type: none"> CitiPower and Powercor are separate legal entities with a registered Australian Business Number (ABN) which is distinct from its affiliated entities that provide “other services” A separate affiliated entity Beon was established to perform “other services” outside distribution and transmission services which are performed by CitiPower and Powercor A waiver was obtained from the AER in relation to unclassified services that are provided by the DSNP. This waiver expires on 30 June 2021 and the unclassified services will then become alternative control services 	<ul style="list-style-type: none"> A monthly review of general ledger accounts is performed by the finance team and attestation is provided by the Financial Controller that no breaches of this requirement have occurred
3.2 Establish and maintain accounts	(a) A DNSP must establish and maintain appropriate internal accounting procedures to ensure that it can demonstrate the extent and nature of transactions between the DNSP and its affiliated entities.	<ul style="list-style-type: none"> A separate general ledger is maintained for CitiPower/Powercor and its affiliates with separate GL accounts for transaction between affiliates 	<ul style="list-style-type: none"> A monthly review of general ledger accounts is performed by the finance group and an attestation is provided by the Financial Controller that no breaches in this requirement have occurred
3.2.1 Separate accounts			

3.2.2 Cost allocation and attribution

(a) A DNSP must allocate or attribute costs to distribution services in a manner that is consistent with the Cost Allocation Principles and its approved CAM, as if the Cost Allocation Principles and CAM otherwise applied to the allocation and attribution of costs between distribution services and non-distribution services.

(b) A DNSP must only allocate or attribute costs to distribution services in accordance with clause 3.2.2(a), and must not allocate or attribute other costs to the distribution services it provides.

(c) A DNSP must establish, maintain and keep records that demonstrate how it meets the obligations in clauses 3.2.2(a) and 3.2.2(b).

- Costs are attributed using profit centres and function codes within the ERP system (SAP) in line with the approved CitiPower and Powercor's Cost Allocation Methodology

- A quarterly review of cost attribution is performed by the finance team and attestation provided by the Financial Controller that this has been performed and whether any breaches have been identified

Guideline clause	Guideline text	Preventative controls	Detective controls
4 Functional separation			
4.1 Obligation to not discriminate	<p>(b) A DNSP must not discriminate (either directly or indirectly) between a related electricity service provider and a competitor (or potential competitor) of a related electricity service provider in connection with the provision of:</p> <ul style="list-style-type: none"> i. direct control services by the DNSP (whether to itself or to any other legal entity); and / or ii. contestable electricity services by any other legal entity. <p>(c) Without limiting its scope, clause 4.1(b) requires a DNSP to:</p> <ul style="list-style-type: none"> i. in dealing or offering to deal with a related electricity service provider, treat the related electricity service provider as if it were not a related electricity service provider (that is, as if it had no connection or affiliation with the DNSP); ii. in like circumstances, deal or offer to deal with a related electricity service provider and a competitor (or potential competitor) of the related electricity service provider on substantially the same terms and conditions; iii. in like circumstances, provide substantially the same quality, reliability and timeliness of service to a related electricity service provider and a competitor (or potential competitor) of the related electricity service provider; iv. subject to clause 4.3.3(b), not disclose to a related electricity service provider information the DNSP has obtained through its dealings with a competitor (or potential competitor) of the related electricity service provider where the disclosure would, or would be likely to, provide an advantage to the related electricity service provider. 	<ul style="list-style-type: none"> • Mandatory online training of CitiPower and Powercor staff on the ring-fencing requirements is performed annually • Approval of project costs and scheduling so that contestable services are not prioritised over direct control services 	<ul style="list-style-type: none"> • An annual review of ring fencing obligations by each responsible manager and General Manager and declaration of any breaches/no breaches occurring in relevant area of the business. This is then signed off by the relevant General Manager

Guideline clause	Guideline text	Preventative controls	Detective controls
4.2 Offices, staff, branding and promotions 4.2.1 Physical separation / co-location	(a) Subject to this clause 4.2.1, in providing direct control services, a DNSP must use offices that are separate from any offices from which a related electricity service provider provides contestable electricity services.	<ul style="list-style-type: none"> CitiPower and Powercor have a separate office from Beon, ENEA and NG/E Beon, ENEA and NG/E staff are physically restricted from accessing certain floors of CitiPower and Powercor office through the use of the Gallagher security system (through electronic access cards and security doors) An office sharing register is maintained and reviewed by CitiPower/Powercor 	<ul style="list-style-type: none"> On a monthly basis, the Operations Manager Facility Management Services performs both a daily and monthly review of physical access restrictions for the CitiPower/Powercor building to identify any Beon, ENEA and NG/E Staff who have inappropriate access
4.2.2 (a) Staff sharing	(a) Subject to this clause 4.2.2, a DNSP must ensure that its staff involved in the provision or marketing of direct control services are not also involved in the provision or marketing of contestable electricity services by a related electricity service provider.	<ul style="list-style-type: none"> All office-based staff complete a mandatory online ring-fencing training, and an in-person induction course that includes a module on ring-fencing. These courses cover the requirement for staff to not provide or market contestable electricity service by a related electricity service provider. The online training was comprehensively updated and relaunched in 2020 	<ul style="list-style-type: none"> An annual review is performed by the Regulation group for any changes to job descriptions or new roles to ensure that any shared staff are identified, and that shared staff are not in breach of the ring-fencing requirements
4.2.2 (c) Staff sharing	(c) The remuneration, incentives and other benefits (financial or otherwise) a DNSP provides to a member of its staff must not give the member of staff an incentive to act in manner that is contrary to the DNSP's obligations under this Guideline.	<ul style="list-style-type: none"> On an annual basis the Head of Business Performance Management reviews the remuneration, incentives and other benefits of staff working for CitiPower and Powercor to ensure that these do not incentivise them to breach the ring-fencing requirements 	

Guideline clause	Guideline text	Preventative controls	Detective controls
4.2.3 (a) Branding and cross-promotion	<p>(a) A DNSP:</p> <p>i. must use branding for its direct control services that is independent and separate from the branding used by a related electricity service provider for contestable electricity services, such that a reasonable person would not infer from the respective branding that the DNSP and the related electricity service provider are related;</p> <p>ii. must not advertise or promote its direct control services and its contestable electricity services that are not direct control services together (including by way of cross-advertisement or cross-promotion);</p> <p>iii. must not advertise or promote contestable electricity services provided by a related electricity service provider other than the DNSP itself.</p>	<ul style="list-style-type: none"> Contact centre scripts are utilised for scenarios where a customer requests contestable electricity services Phone calls to the contact centre are monitored to detect any instances of cross-promotion A monthly attestation is provided that this has occurred and whether any breaches identified were reported Mandatory online training on the ring-fencing requirements undertaken by all staff. In 2020 this online training was comprehensively updated and relaunched In 2019, all field branding of the regulated business was separately from branding used by related electricity service providers 	<ul style="list-style-type: none"> An annual review of the CitiPower/Powercor website and social media content for any inappropriate co-branding or cross promotion
4.2.4 Office and staff registers	<p>A DNSP must establish, maintain and keep a register that identifies:</p> <p>(a) the classes of offices to which it has not applied clause 4.2.1(a) by reason of clauses 4.2.1(b)i. or 4.2.1(b)iii.; and</p> <p>(b) the nature of the positions (including a description of the roles, functions and duties) of its members of staff to which it has not applied clause 4.2.2(a) by reason of clauses 4.2.2(b)i.a., 4.2.2(b)i.b., 4.2.2(b)iii. or 4.2.2(d);</p> <p>and must make the register publicly available on its website.</p>		<ul style="list-style-type: none"> Annual review of the Staff and Office sharing register and verification it is publicly available on the website Additional ad-hoc reviews of staff and office sharing register when arrangements change and an update is required

Guideline clause	Guideline text	Preventative controls	Detective controls
<p>4.3 Information access and disclosure</p> <p>4.3.2 Protection of confidential information</p>	<p>Subject to this clause 4.3, a DNSP must:</p> <p>(a) keep confidential information confidential; and</p> <p>(b) only use confidential information for the purpose for which it was acquired or generated.</p>	<ul style="list-style-type: none"> • Beon, ENEA and NG/E staff are restricted from accessing confidential electricity information through IT access controls 	<ul style="list-style-type: none"> • Monthly review of IT user access to monitor any inappropriate access to systems for Beon, ENEA and NG/E staff • Bi-annual review of IT user access for any inappropriate access to systems by Beon, ENEA and NG/E staff. As a part of this process the business owners of each ring-fenced application must approve access and permissions
<p>4.3.3 Disclosure of information</p>	<p>A DNSP must not disclose confidential information to any person, including a related electricity service provider, unless:</p> <p>(a) the DNSP has first obtained the explicit informed consent of the relevant customer, or prospective customer, to whom the confidential information relates;</p> <p>(b) the disclosure is required by, or for the purpose of complying with any law;</p> <p>(c) the disclosure is necessary to enable the DNSP to provide its distribution services, its transmission services or its other services (including by acquiring services from other legal entities);</p> <p>(d) the information has been requested by or on behalf of a customer, or potential customer, of another legal entity, and the disclosure is necessary to enable the legal entity to provide its transmission services, contestable electricity services or other services to the customer or potential customer;</p> <p>(e) the disclosure is solely for the purpose of providing assistance to another Network Service Provider to the extent necessary to respond</p>	<ul style="list-style-type: none"> • Information sharing protocol and information sharing register is publicly available • Beon, ENEA and NG/E staff are restricted through IT access controls from confidential information • Tailored mandatory training for IT system owners on how ring fencing relates to access and disclosure • Decision matrix on IT access approval process and ring fencing considerations provided to IT system owners 	<ul style="list-style-type: none"> • Monthly review of IT user access to monitor any inappropriate access to systems for Beon, ENEA and NG/E staff • Bi-annual review of IT user access for any inappropriate access to systems by Beon, ENEA and NG/E staff. As a part of this process the business owners of each ring-fenced application must approve access and permissions

Guideline clause	Guideline text	Preventative controls	Detective controls
	<p>to an event (such as an emergency) that is beyond the other Network Service Provider's reasonable control;</p> <p>(f) the disclosure is solely for the purposes of research by a legal entity other than a related electricity service provider of the DNSP;</p> <p>(g) where another DNSP is an affiliated entity of the DNSP, the disclosure is to the part of that other DNSP that provides that other DNSP's direct control services; or</p> <p>(h) a related electricity service provider of the DNSP has requested the disclosure and the DNSP complies with clause 4.3.4 in relation to that confidential information.</p>		
4.3.4 Sharing of information	<p>(a) Subject to clause 4.1(c)iv. and to this clause 4.3.4, where a DNSP shares confidential information with a related electricity service provider, or where confidential information that a DNSP has disclosed under clause 4.3.3(f) is then disclosed by any person to a related electricity service provider of the DNSP, the DNSP must provide access to that confidential information (including the derived information) to other legal entities on an equal basis.</p> <p>(b) A DNSP is only required by clause 4.3.4(a) to provide information to a legal entity where:</p> <p>i. the legal entity has requested that it be included on the information register in respect of information of that kind; and</p> <p>ii. the legal entity is competing, or is seeking to compete, with the DNSP, or a related electricity service provider of the DNSP, in relation to the provision of contestable electricity services.</p> <p>(c) A DNSP is not required by clause 4.3.4(a) to provide information to a legal entity where the DNSP has disclosed the information in the circumstances set out in clauses 4.3.3(a) to (e).</p>	<ul style="list-style-type: none"> • Information sharing protocol and information sharing register is publicly available • Beon, ENEA and NG/E staff are restricted through IT access controls from confidential information • Tailored mandatory training for IT system owners on how ring fencing relates to access and disclosure • Decision matrix on IT access approval process and ring fencing considerations provided to IT system owners • 	<ul style="list-style-type: none"> • Monthly review of IT user access to monitor any inappropriate access to systems for Beon, ENEA and NG/E staff • Bi-annual review of IT user access for any inappropriate access to systems by Beon, ENEA and NG/E staff. As a part of this process the business owners of each ring-fenced application must approve access and permissions

Guideline clause	Guideline text	Preventative controls	Detective controls
	<p>(d) Without limiting clause 4.3.4(a), a DNSP must establish an information sharing protocol that sets how and when it will make the information referred to in clause 4.3.4(a) available to legal entities, and must make that protocol publicly available on its website.</p> <p>(e) Where a DNSP discloses information referred to in clause 4.3.4(a) to any other legal entity under this clause 4.3.4, it must do so on terms and conditions that require the other legal entity to comply with clause 4.3.2 and 4.3.3(a) to (d) in relation to that information as if the other legal entity was a DNSP.</p>		
4.3.5 Information register	<p>(a) A DNSP must establish, maintain and keep a register of all:</p> <ul style="list-style-type: none"> i. related electricity service providers; ii. other legal entities who provide contestable electricity services but who are not affiliates of the DNSP; <p>Who request access to information identified in clause 4.3.4(a), and must make the register publicly available on its website.</p> <p>(b) For each legal entity that has requested that a DNSP provide access to information identified in clause 4.3.4(a), the DNSP's information register must:</p> <ul style="list-style-type: none"> i. identify the kind of information requested by the legal entity; and ii. describe the kind of information requested by the legal entity in sufficient detail to enable other legal entities to make an informed decision about whether to request that kind of information from the DNSP. <p>(c) A legal entity may request that the DNSP include it on the information register in relation to some or all of the kinds of information that the DNSP is required to provide under clause 4.3.4(a), and the DNSP must comply with that request.</p>	<ul style="list-style-type: none"> • Information sharing protocol and information sharing register is publicly available 	

Guideline clause	Guideline text	Preventative controls	Detective controls
<p>4.4 Service providers</p> <p>4.4.1 Conduct of service providers</p>	<p>A DNSP:</p> <p>(a) must ensure that any new or varied agreement between the DNSP and a service provider, for the provision of services to the DNSP that enable or assist the DNSP to supply direct control services, requires the service provider to comply, in providing those services, with:</p> <p>i. clauses 4.1, 4.2.1, 4.2.2 and 4.3.2 of this Guideline; and</p> <p>ii. clause 4.2.3 of this Guideline in relation to the brands of the DNSP; as if the service provider was the DNSP.</p> <p>(b) must not, directly or indirectly, encourage or incentivise a service provider to engage in conduct which, if the DNSP engaged in the conduct itself, would be contrary to the DNSP's obligations under clause 4 of this Guideline.</p>	<ul style="list-style-type: none"> • Standard terms and conditions for CitiPower/Powercor supply contracts have been amended to include compliance with ring-fencing requirements. Purchase orders include ring-fencing clauses. These standard terms and conditions are included in all new and amended contracts for suppliers involved in the provision of direct control services • All non-compliant contracts from the prior audits have either expired or have been amended to include ring fencing clauses • Internal controls implemented within the procurement team to ensure Beon procurement staff cannot see CitiPower/Powercor tenders • Decision matrix provided to procurement staff to apply in contract negotiations • Procurement staff incentive scheme amended to include ring-fencing KPIs 	

Guideline clause	Guideline text	Preventative controls	Detective controls
5 Waivers			
5.7 Waiver register	<p>(a) A DNSP must establish, maintain and keep a register of all waivers (including any variation of a waiver) granted to the DNSP by the AER under clause 5 of this Guideline, and must make the register publicly available on its website.</p> <p>(b) The register established under clause 5.7(a) must include:</p> <p>i. the description of the conduct to which the waiver or interim waiver applies; and</p> <p>ii. the terms and conditions of the waiver or interim waiver;</p> <p>as set out in the AER’s written decision, provided by the AER to the DNSP, to grant (or vary) the waiver or interim waiver.</p>	<ul style="list-style-type: none"> Waiver register is maintained and publicly available 	
6 Compliance and Enforcement			
6.1 Maintaining compliance	<p>A DNSP must establish and maintain appropriate internal procedures to ensure it complies with its obligations under this Guideline. The AER may require the DNSP to demonstrate the adequacy of these procedures upon reasonable notice. However, any statement made or assurance given by the AER concerning the adequacy of the DNSP’s compliance procedures does not affect the DNSP’s obligations under this Guideline.</p>	<ul style="list-style-type: none"> Mandatory online training on the ring-fencing requirements Tailored in-person trainings for different parts of the business which have particular obligations, such as procurement, the contact centre, IT and the service desk 	<ul style="list-style-type: none"> General Manager annual compliance review and declaration
6.1 Compliance reporting	<p>(a) A DNSP must prepare an annual ring-fencing compliance report each regulatory year in accordance with this clause 6.2.1, and submit it to the AER in accordance with clause 6.2.2.</p>	<ul style="list-style-type: none"> Mandatory online training on the ring-fencing requirements A mailbox is maintained by the Regulation group for 	

Guideline clause	Guideline text	Preventative controls	Detective controls
6.2.1 Annual compliance reporting	<p>(b) The annual compliance report must identify and describe, in respect of the regulatory year to which the report relates:</p> <ul style="list-style-type: none"> i. the measures the DNSP has taken to ensure compliance with its obligations under this Guideline; ii. any breaches of this Guideline by the DNSP, or which otherwise relate to the DNSP; iii. all other services provided by the DNSP in accordance with clause 3.1; and iv. the purpose of all transactions between the DNSP and an affiliated entity. <p>(c) The annual compliance report must be accompanied by an assessment of compliance by a suitably qualified independent authority.</p> <p>d) Annual compliance reports may be made publicly available by the AER.</p>	<p>CitiPower/Powercor to report any potential breaches</p> <ul style="list-style-type: none"> • A materiality and breach reporting policy is available to all staff on the intranet • A monthly ring-fencing champions meeting is held to identify and assess any ring-fencing issues as they arise 	
6.2.1 Timing of Annual compliance reporting	<p>(a) A DNSP must submit its annual compliance report to the AER within four months of the end of the regulatory year to which the compliance report relates.</p>	<ul style="list-style-type: none"> • Independent assessment of compliance conducted by Deloitte, a suitably qualified independent authority 	
6.3 Compliance breaches	<p>A DNSP must notify the AER in writing within five business days of becoming aware of a material breach of its obligations under this Guideline. The AER may seek enforcement of this Guideline by a court in the event of any breach of this Guideline by a DNSP, in accordance with the NEL.</p>	<ul style="list-style-type: none"> • Mandatory online training on the ring-fencing requirements • A breach register is maintained and updated by the Regulation group • A materiality and breach reporting policy is available to all staff on the intranet. In this policy we commit to report all potential breaches to the AER within five business days 	<ul style="list-style-type: none"> • General Manager annual compliance review and declaration

5 Complaints and breach reporting

5.1 Complaints and investigations

We have not received complaints about our compliance with the Guideline during the 2020 regulatory year.

In the event that a complaint is received, we have established internal policies and procedures for responding in a timely manner and ensuring a satisfactory outcome.

5.2 Breach reporting

We have a thorough process in place to identify, investigate and report breaches as they arise.

Identify:

We have various means of identifying potential breaches as they arise, including:

- emails to the ring-fencing inbox. The inbox provides a means for staff to raise ring-fencing related concerns. The Regulation group monitors this inbox and carefully reviews all matters raised
- through monthly, quarterly, six-monthly and annual attestations, which are now managed through the Quantate system. The business completes attestations in a range of areas such as finance, IT, contact centre, facilities, printed materials and website monitoring
- through walk-up consults or phone calls with the Regulation group
- in meetings relating to business activities where ring-fencing issues or concerns may arise
- in the monthly ring-fencing champions meetings
- through annual ring-fencing audits, conducted by Deloitte.

Investigate:

We use a range of investigative tools to further understand the matters that give rise to a potential breach. This may include, for example:

- interviewing staff members (whether internal or from an affiliate) as to the particulars of a matter
- creating a timeline of events leading to the potential breach
- consulting with internal experts on processes and/or procedures
- seeking written evidence or other documentation, such as emails, invoices, contracts, manuals etc.

Investigations may be conducted by the Regulation group, Legal team, Internal Audit team, or a combination of these teams, on a particular matter.

Assess:

Should a matter be assessed to be contrary to the requirements set out in the Guideline, we will assess the materiality of the breach with reference to the following factors:

- relevant background information (e.g. documentation, environment) and context that has led to the breach
- the duration, recurrence and exposure of the breach, if relevant
- the seniority of staff who have committed the breach
- the purpose for which the Guideline was introduced and harm that it is seeking to prevent, and how the breach fits into that context

- the potential impact on competition and competitors in the market(s) or related market(s) arising from the breach
- whether the breach is an isolated incident or reflects a systemic issue.

Report:

Where we identify a breach, whether material or immaterial, we report this to the AER within five business days.

For any breach, whether material or immaterial, we add the breach to our breach reporting register and provide this to our auditors during the yearly audit.

Where we assess there is no breach, we may take action to strengthen or clarify the control environment or if not required take no action.

Table 3 below sets out the immaterial breach which occurred during the 2020 regulatory year, and carryover breaches from the prior year.

Table 3 Immaterial breaches during the 2020 regulatory year

Obligation	Details	Remedy	Materiality assessment
Branding and cross-promotion 2020	<p>An employee of our unregulated affiliate, Beon, noticed that two former Powercor Network Service employees were using incorrect branding in their email signatures, and emailed the ring-fencing inbox advising us of this on 2 September 2020.</p> <p>We assessed that there may be a low risk of impact on the contestable market.</p> <p>Given there were only two cases identified of Network Services staff with non-compliant email signatures, and the majority of Network Services' work is exclusively for Powercor, we considered the impact on the contestable market to be low.</p>	<p>We held immediate discussions with Deloitte, our independent auditor. Based on their advice, we immediately instituted a remediation strategy.</p> <p>We issued a reminder to all employees of Network Services informing them of the rebrand and instructing them on how to change their email signatures if they had not done so already.</p> <p>In response to our self-reporting of this breach, the AER assessed that we had appropriately investigated and responded to this breach. The AER took no further action.</p>	Immaterial

Obligation	Details	Remedy	Materiality assessment
Branding Carry over breach from 2019 which was identified and addressed in 2020. ⁷	<p>In May 2019, an email to the ring-fencing inbox alerted us to the fact that Beon invoices were referencing Powercor.</p> <p>We assessed this breach to be immaterial and in the 2019 audit our independent auditors agreed.</p>	<p>After becoming aware of the breach, we worked with IT to understand the scale of the problem. IT identified that a new Beon email would need to be set up, and also that IT would need to reconfigure SAP to ensure that Beon invoices no longer referenced Powercor. This reconfiguring of SAP was a significant piece of work that took some time to complete.</p> <p>This work was completed in January 2020. As such, we are recognising this as an immaterial carry-over breach as full remediation was not completed until January 2020.</p>	Immaterial

⁷ Please see 2019 compliance report for further detail.

Obligation	Details	Remedy	Materiality assessment
Staff sharing Carry over breach from 2019 which was identified and addressed in 2020.⁸	<p>In 2019, we had six shared staff who were absent from the staff sharing register.</p> <p>We considered that this is an immaterial breach and reported it in the 2019 compliance reports. Our independent auditors agreed it was immaterial.</p>	<p>The staff sharing register was updated in 2020 to contain a more granular listing of roles and responsibilities for those shared staff, as well as to include staff shared with ENEA and Next Generation Electrical.</p>	<p>Immaterial</p>
Branding Carry over breach from 2019 which was identified and addressed in 2020.⁹	<p>On 19 December 2019, a Powercor staff member commenced a short term secondment to Beon, which concluded on 3 March 2020. He retained his @powercor email address during this time. The role at Beon involved co-ordinating planned outages associated with transmission maintenance activities undertaken by PNS for third parties. We assessed this breach to be immaterial and our independent auditors agreed. The breaching period was short. The individual only dealt with AusNet Transmission, who is aware of the commercial arrangements for maintenance activities and that the individual was acting on behalf of Beon, not Powercor. The individual had no communication with any other external party that would lead to Beon gaining a competitive advantage. The risk of harm to competition due to this isolated incident was very low.</p>	<p>IT processes and procedures were updated and developed to capture staff who undertake a secondment to Beon. @Powercor email addresses are now automatically removed upon transition.</p>	<p>Immaterial</p>

5.3 Material breaches

We are not aware of any material breach of our obligations under the Guideline during the 2020 regulatory year.

Pursuant to our obligations under the Guideline, we will notify the AER within five business days of becoming aware of any breaches of our obligations.

5.4 Other services provided

We are not aware of having provided 'other services'—being services that are not transmission or distribution services—over 2020.

⁸ Please see 2019 compliance report for further detail.

⁹ Please see 2019 compliance report for further detail.

6 Transactions with affiliated entities

A list of the transactions between the distributors and affiliates is provided in Tables 4 and 5 below.

Table 4 CitiPower transactions with affiliates

Affiliate	Transaction	Nature of transaction	Value in 2019 (\$000)	Value in 2020 (\$000)
CHED Services	Corporate services	For the provision of management, administration, back office and other business functions	\$40,162	\$43,011
CHED Services	IT projects	For the provision of IT system enhancements	\$10,633	\$17,117
CHED Services	Infill insurance ¹⁰	For the provision of insurance on excesses	\$1,555	\$576
Power Network Services	Network services	For the provision of construction, maintenance, faults, emergency and related services	\$164,018	\$186,183
Power Network Services	Depot maintenance	For the use of distributor owned depots	\$91	\$108

Source: CitiPower

¹⁰ The premium that the Discretionary Risk management Fund charges the distribution businesses is set following an independent actuarial assessment performed by Marsh. As part of the actuarial review, Marsh will review past claims and future forecast losses. Factors such as claims history, changes in deductible levels etc can impact premium amounts.

Table 5 Powercor transactions with affiliates

Affiliate	Transaction	Nature of transaction	Value in 2019 (\$000)	Value in 2020 (\$000)
CHED Services	Corporate services	For the provision of management, administration, back office and other business functions	\$87,203	\$91,420
CHED Services	IT projects	For the provision of IT system enhancements	\$24,357	\$38,326 ¹¹
CHED Services	Infill insurance ¹²	For the provision of insurance on excesses	\$4,903	\$2,352
Power Network Services	Management services	For the provision of management services	\$300	\$120
Power Network Services	Network services	For the provision of construction, maintenance, faults, emergency and related services	\$406,314	\$451,591
Power Network Services	Depot maintenance	For the use of distributor owned depots	\$391	\$513
Power Network Services	Capex lease	For the use of distributor owned fleet	\$2,553	\$2,108
Power Network Services	Corporate services	For secondment of staff to Beon through PNS ¹³	\$20,404	\$22,081
Beon Aerial Services	Corporate services	For secondment of staff to Beon Aerial Services	\$0	\$408

Source: Powercor

There are no contracts between CitiPower/Powercor and United Energy.

¹¹ This figure does not align with the Regulatory Information Notices because for the purposes of ring-fencing we have included in this category IT capex on Alternative Control Services, metering and public lighting, Standard Control Services and digital innovation.

¹² The premium that the Discretionary Risk management Fund charges the distribution businesses is set following an independent actuarial assessment performed by Marsh. As part of the actuarial review, Marsh will review past claims and future forecast losses. Factors such as claims history, changes in deductible levels etc can impact premium amounts.

¹³ The majority of Beon staff are contractually employed by Powercor, as they are seconded through our affiliated entity PNS. It was financially prohibitive to transfer employment contracts from Powercor to Beon when the ring-fencing guideline came into effect. Further, management have disclosed the arrangement to the AER and it was not identified by the AER to be of concern.