



SA Power Networks

Ring-Fencing Guideline Compliance Report

30 June 2019

Table of Contents

1. Executive Summary4

2. Independent Assurance Report to the Partners of SA Power Networks9

3. Detailed Findings11

1. Executive Summary

1.1 Introduction

The Australian Energy Regulator (the “AER”) published the Electricity Distribution Ring-Fencing Guideline on 30 November 2016 under the National Electricity Rules (the “NER”) with amendments made on 17 October 2017 (the “Guideline”). The Guideline requires functional separation of regulated and competitive business activities to promote competition in the provision of contestable electricity services.

Under clause 6.2.1c of the Guideline, Deloitte has been engaged per the engagement letter between SA Power Networks (“SAPN”) and Deloitte dated 16 October 2019 as the qualified independent authority to provide reasonable assurance that SAPN’s Ring-Fencing Annual Compliance Report has been prepared in compliance with 6.2.1a of the Guideline as evaluated against 6.2.1b of the Guideline, in all material respects, for the period from 1 July 2018 to 30 June 2019.

1.2 Rating Applied

The ratings applied to the results of our testing are defined below based on Deloitte’s interpretation of the Guideline. The evaluation of the results of our tests as they relate to the obligations is based on applying our professional judgement and considering the available facts and circumstances.

No Exception	Requirements of the obligation have been met with no or only minor improvement opportunities. Any findings noted are considered minor and require routine efforts to correct in the normal course of business.
Exception	The requirements of the obligation have not been fully met. Findings noted require remedial action.

1.3 Summary of Findings

The following table summarises observations and recommendations against the obligations where an exception was identified. The rating of each obligation has been applied in accordance with *Section 1.2*.

Management responses to the observations and recommendations are included in the executive summary and our Detailed Findings. These do not form part of our report and therefore we do not express an opinion on these.

Legal Separation	
Guideline Reference	3.1 (b)
Guideline Obligations	A DNSP may provide distribution services and transmission services, but must not provide other services .
Observations	<p>‘Other services’ contracts not included on waiver</p> <p>The AER granted SAPN a waiver from the obligation to comply with clause 3.1 of the Guideline from 18 December 2017 to 30 September 2018 so that it may continue to provide Other Services contracted under 20 construction and maintenance contracts.</p> <p>At the time of the initial waiver submission, [REDACTED]. In September 2018 when SAPN applied for an extension to the waiver it was discovered that 4 contracts were not included in the original waiver. SAPN identified these four contracts to the AER in the waiver extension, and reported them as a material breach. On 28 September 2018, the AER granted a waiver extension in relation to the Other Services contracts until the contract expiry in 2021.</p> <p>Subsequently, SAPN identified one contract that was not included on the initial waiver or the waiver extension. This contract was included on the material breach report to the AER. SAPN has rectified this breach by replacing the contract with a new contract with Enerven as the contracting party.</p> <p>The implication of this observation is that 5 SAPN contracts to provide Other Services were not covered by a valid waiver from the obligation to comply with clause 3.1 of the Guideline.</p>

	In the 2018/19 regulatory year the Enerven commercial team has [REDACTED]. Intermittent testing on Enerven work-orders was performed by the Enerven Commercial team to identify other services performed under contracts that have not been novated to Enerven. No additional contracts were identified through this process. Any proposed amendments to the waived contracts are required to be discussed with the Regulation branch who will advise the AER of the proposed amendment, as required by the waiver notice.
Recommendation	We recommend that the Enerven commercial team establish preventative controls to ensure that a valid waiver is in place or by establishing a new contract with Enerven as the contracting party before any other services contract is fulfilled where SAPN is the contracting party.
Management Response*	Enerven have conducted a review of existing contracts to ensure there are no more contracts where SAPN are the contracting party for other services, that are not already on the existing AER-approved waiver. Preventative controls to ensure all Enerven contracts are raised with Enerven as the contracting party include central management of all contracts through the Enerven Commercial Team; providing training/advice to all relevant Enerven teams to ensure their understanding of this requirement; ongoing intermittent testing on Enerven work-order numbers.
Rating	Exception
Protection of Confidential Information	
Guideline Reference	4.3.2 (a) (b)
Guideline Obligations	A DNSP must: (a) keep confidential information confidential (b) only use confidential information for the purpose for which it was acquired or generated
Observations	<p>Enerven staff accessing critical applications</p> <p>Deloitte obtained access logs for IT applications containing confidential information ("critical applications") on a sample basis.</p> <p>We identified two staff members who were seconded to the Enerven [REDACTED] Program Management team who accessed critical applications in the period 1 July 2018 - 30 June 2019.</p> <p>One employee was seconded from the Enerven metering team to the Enerven [REDACTED] Program Management team on 9 March 2019. The staff member accessed the [REDACTED] system on 10 occasions and the [REDACTED] (" [REDACTED] ") on 18 occasions in the period 9 March 2019 – 30 June 2019. The employee accessed these systems to obtain site data in preparation for [REDACTED] site visits.</p> <p>The second employee was seconded from SAPN to Enerven on 12 January 2019. The staff member accessed [REDACTED] on 2 May 2019.</p> <p>[REDACTED] is a customer billing system and contains confidential electricity customer information. [REDACTED] is a SAPN developed application for viewing and reporting on interval metered and CT-metered customers. [REDACTED] contains confidential electricity information in accordance with the clause 4.3 Guideline definition.</p> <p>These staff members' access to critical applications was not considered for ring-fencing compliance at the commencement of their secondments. Once it was identified that these staff members had retained their access to these critical applications, the IT team reviewed and restricted these staff's IT access.</p> <p>From 1 January 2018 SAPN had manual controls in place that were intended to ensure that IT access to critical applications is reviewed prior to staff movements to Enerven.</p> <p>The control required a transfer or secondment checklist to be completed and returned when staff members are transferred or seconded to Enerven for a period greater than 6 weeks. When completing the checklist, hiring managers are required to ensure that staff access to critical applications is restricted. The checklists require the hiring managers to sign off on the following items:</p> <ul style="list-style-type: none"> • "Ensure employee is familiar with their ring-fencing obligations (employee to retake ring-fencing training if required)"; and • "Does the employee have access to any of the following restricted systems/applications? (If so, remove access where no longer required, or if still required advise Regulation Branch of the employees new position)".

	<p>In our 30 June 2018 compliance report, we identified that in the 6 months to 30 June 2018 there was no process in place to monitor whether transfer or secondment checklists had been completed by hiring managers or whether hiring managers had appropriately restricted access to controlled applications. In our 30 June 2018 compliance report we recommended that:</p> <ul style="list-style-type: none"> Human Resources ("HR") implement controls to monitor whether checklists are completed and returned; and checklists be required for all secondments, regardless of their duration. <p>At the start of the 2018/19 regulatory year, the HR department designed controls to monitor the completion of checklists where staff movements have occurred. These controls require HR staff to generate a report from SAP that identifies staff secondments and transfers to Enerven each month. HR staff are required to ensure that the hiring manager has prepared and signed a transfer or secondment checklist for the staff member. If a signed induction checklist is not completed, the HR team member contacts the hiring manager to ensure that a checklist is completed.</p> <p>The correct secondment checklist was not completed for the two staff members seconded to the Enerven [REDACTED] Project team. For one secondment, a checklist was completed however the correct checklist was not used and therefore the item to review IT system access was not included. The other secondment was from an internal Enerven distribution team to the Enerven [REDACTED] Project team. HR did not identify this during their monthly review. This indicates that controls to monitor the completion of secondment checklist were not appropriately designed and implemented during the year.</p>
Recommendation	<p>We recommend that:</p> <ul style="list-style-type: none"> All staff movements are recorded in SAP (including short term secondments and secondments between Enerven teams); A staff movement report is obtained from SAP at the end of each month to identify staff movements to an Enerven team; and Where staff movements have occurred, that IT consider the staff's access to any critical applications and restrict access where not permissible under the Guideline.
Management Response*	<p>A communication has been issued to all Enerven staff confirming the HR secondment and transfer process and reiterated the requirement for any staff secondment to involve the Enerven HR Talent Manager prior to commencement. The Talent Manager will ensure the correct HR secondment checklist is completed, and access restrictions are imposed prior to the commencement of any secondment.</p> <p>HR has implemented new digital checklists that have replaced the paper-based checklists with a new digital form. The checklists will be launched by a HR Officer at the earliest possible point in each recruitment process and will workflow to and between leaders and staff via emails, with instructions and links directly to the checklist.</p> <p>The 'Transferring Employee' induction checklist (which is now initiated by HR for all employee moves between business units – for secondments, permanent internal appointments, redeployment opportunities and realignment of roles and / or functions), contains a specific ring-fencing section in the 'pre-commencement' leader tasks section. If ring-fencing compliance actions apply to the employee move, both HR and the leader will ensure that all ring-fencing related tasks outlined in the checklist are completed <u>prior</u> to the employee commencing in their new position.</p> <p>All secondments and transfers (regardless of duration) will be actioned through the HR branch, and recorded in SAP.</p> <p>HR will monitor progress of the checklists weekly to ensure pre-commencement obligations are met.</p>
Rating	Exception
Protection of Confidential Information	
Guideline Reference	4.3.2 (a) (b)
Guideline Obligations	<p>A DNSP must:</p> <p>(a) keep confidential information confidential</p> <p>(b) only use confidential information for the purpose for which it was acquired or generated</p>
Observations	<p><i>SAP and IT application access restrictions</i></p> <p>In December 2017, the ring-fencing project management office ("PMO") identified 24 critical applications. Controls were designed to ensure that access to these critical applications was appropriately monitored and restricted.</p> <p>As outlined in our 30 June 2018 compliance report, when determining the list of critical applications, the PMO initially applied a definition of confidential information that was restricted to customer information that is not publicly available. Network and service information was not included in the definition of confidential information against which IT systems were assessed. Resultantly, IT applications that contain network and services information were not included in the list of critical applications.</p>

	<p>Per clause 4.3 of the Guideline, 'confidential information' means electricity information generated by a DNSP in connection with its provision of direct control services that is not already publicly available. Electricity information includes information about the electricity network, electricity customers or electricity services, but does not include non-customer financial information or non-customer performance information.</p> <p>The PMO also did not include SAP applications in the list of critical applications. As a result, the list of critical applications in the 6 months to 30 June 2018 was not complete.</p> <p>The list of critical applications is integral to the operation of key IT access controls such as the quarterly IT access review and the IT application access approval process.</p> <p>In July 2018, the IT team reassessed the list of critical applications by applying the guideline definition of confidential information. This assessment expanded the list to 35 critical applications.</p> <p>To test whether the revised list of critical applications is complete, Deloitte obtained a list of all IT applications at 30 June 2019 and assessed whether a sample of these IT applications contain confidential information that users are able to access.</p> <p>Our testing identified various SAP applications such as [REDACTED] and [REDACTED] that contain confidential information that are not included on the list of critical applications. Our testing did not identify any non-SAP applications that contained confidential information that were not included on the list of critical applications.</p> <p>Notwithstanding a number of mitigating controls such as extensive training and a quarterly management representations process, there is a risk that Enerven staff continue to have unrestricted access to SAP systems that contain confidential information.</p> <p>SAPN's ability to restrict SAP access for Enerven staff members is limited as separate company codes have not been established within SAP. The implementation of separate company codes in SAP is an extensive IT project with significant costs associated. These costs have been included in SA Power Networks' 2020-25 Regulatory Proposal.</p>
Recommendation	<p>We recommend that SAPN:</p> <ul style="list-style-type: none"> • Implement formal access restrictions in SAP by establishing a separate company code; • Undertake regular monitoring of access to confidential applications in SAP for ring-fencing compliance.
Management Response*	<p>Background</p> <p>SAP was implemented in 1997 and at that time the Construction and Maintenance Services (CAMS) Department, now known as Enerven, was set up together with joint procurement and financial operations as common services. Currently, SA Power Networks and Enerven are a single entity within SAP. The work to establish a separate company code in SAP for Enerven is highly complex and will require involvement of several business units across SA Power Networks and Enerven. It will include the review and modification of every SAP business process for Enerven (and several of SA Power Networks'), which is made more challenging by the current customisations in SAP that were created to suit SA Power Networks, and significant other IT projects currently underway. For these reasons, which are elaborated on below, it is not possible to commence implementation of a new SAP company code until after July 2020.</p> <p>Action Plan</p> <p>As is highlighted in our Regulatory Proposal for the 2020-25 Regulatory Control Period (RCP) Supporting Business Case "Ringfencing Compliance: Information Technology solution", the manual controls we have for SAP access are a risk-area. The business case driver for this IT project is the need to ensure ongoing ringfencing compliance by implementing improved compliance controls in the most efficient way (for regulated customers), being that Enerven continue to utilise SAPN's systems and is allocated its share of IT costs rather than Enerven have its own separate system(s) and regulated customers pay 100% of the costs. To minimise any ring-fencing non-compliance risk this project will implement stronger ex ante automated system controls, including the set up of a new company code in SAP to separate the regulated and unregulated entities, and also to implement more robust system-based information access controls for all applications that contain confidential information. Creation of a new company code in SAP will enable restricted access at transaction level between SA Power Networks information and Enerven information.</p>

	<p>We have reviewed options for interim controls and found that the only solution that will completely resolve the issue is implementation of a new company code in SAP as described above. An option we investigated was to use a separate SAP Purchasing Group for Enerven to restrict certain procurement information access between SA Power Networks and Enerven. The intention of this interim solution was that Enerven would have a separate Purchase Group (high level) code and would not be able to directly access or view SA Power Networks' purchase orders (low level), purchase requisitions and invoices. However, detailed user testing found that Enerven could still access the same information via other financial transactions, which could not be restricted using a Purchasing Group.</p> <p>Our proposed actions are therefore to reinforce existing controls (training, company-wide Directives and Policies, Quarterly Compliance Questionnaires, Audits, etc); and we are seeking funding in SA Power Networks' Regulatory Proposal for the 2020-2025 Regulatory period, for the IT ring-fencing project to create a separate company code for Enerven in SAP.</p>
Rating	Exception

*The management response does not form part of the auditor's opinion.

2. Independent Assurance Report to the Partners of SA Power Networks

Qualified Opinion

We have undertaken a reasonable assurance engagement on whether SA Power Network's Ring-Fencing Compliance Report has been prepared in compliance with 6.2.1a of the Ring-Fencing Guideline - Electricity Distribution (the "Guideline") as evaluated against 6.2.1b of the Guideline in all material respects for the period from 1 July 2018 to 30 June 2019. The Ring-Fencing Compliance Report will accompany our report, for the purpose of reporting to the Australian Energy Regulator ("AER").

In our opinion, except for the effects of the matters described in the Basis for Qualified Opinion paragraph, SA Power Networks has complied, in all material respects, with the NER Guideline as evaluated against the Obligations for the period from 1 July 2018 to 30 June 2019.

Basis for Qualified Opinion

We conducted our engagement in accordance with Standard on Assurance Engagements ASAE 3100 *Compliance Engagements* ("ASAE 3100") issued by the Auditing and Assurance Standards Board.

As explained in Section 3 of this report, SA Power Networks has not met guideline 3.1(b) relating to legal separation and guideline 4.3.2 (a) (b) relating to protection of confidential information.

Responsibilities of the Management of SA Power Networks

Management is responsible for:

- a) Providing a statement with respect to the outcome of the evaluation of the compliance activity against the requirements of the Guideline, which accompanies this independent assurance report.
- b) Identifying risks that threaten 6.2.1b of the Guideline identified above being met;
- c) Identifying suitable compliance requirements in the Guideline as required by the AER; and
- d) Identifying, designing and implementing controls to enable the requirements of the Guideline to be met and to monitor ongoing compliance.

Our Independence and Quality Control

We have complied with the independence and other relevant ethical requirements relating to assurance engagements, and apply Auditing Standard ASQC 1 *Quality Control for Firms that Perform Audits and Reviews of Financial Reports and Other Financial Information, and Other Assurance Engagements* in undertaking this assurance engagement.

Assurance Practitioner's Responsibilities

Our responsibility is to express an opinion on whether SA Power Networks' Ring-Fencing Compliance Report has been prepared in compliance with 6.2.1a of the Guideline as evaluated against 6.2.1b of the Guideline in all material respects for the period from 1 July 2018 to 30 June 2019. ASAE 3100 requires that we plan and perform our procedures to obtain reasonable assurance about whether SA Power Network's Ring-Fencing Compliance Report has been prepared in compliance with 6.2.1a of the Guideline as evaluated against 6.2.1b of the Guideline in all material respects for the period from 1 July 2018 to 30 June 2019.

An assurance engagement to report on SA Power Networks' Ring-Fencing Compliance Report involves performing procedures to obtain evidence about the compliance activity and controls implemented to meet the requirements of the Guideline. The procedures selected depend on our judgement, including the identification and assessment of risks of material misstatement in the Ring-Fencing Compliance Report, as evaluated against 6.2.1b of the Guideline.

Our procedures included, but were not limited to:

- Inquiring with SA Power Networks personnel about controls are in place to allow SA Power Networks to comply with the Obligations;
- On a sample basis, observing the control being performed, and/or inspecting documentation to evidence the design, implementation and effectiveness of the controls;
- Inquiring with management whether they are compliant with the Obligations and corroborating our inquiry with the results of our procedures.

- Inquiring with management whether they are compliant with the Obligations and corroborating our inquiry with the results of our procedures.

Inherent Limitations

Because of the inherent limitations of an assurance engagement, together with the internal control structure it is possible that fraud, error, or exception with compliance requirements may occur and not be detected.

A reasonable assurance engagement for the period from 1 July 2018 to 30 June 2019 does not provide assurance on whether compliance with the Guideline will continue in the future.


Restricted Use

This report has been prepared for use by the Partners of SA Power Networks for the purpose of meeting the reporting requirements to the AER. We disclaim any assumption of responsibility for any reliance on this report to any person other than SA Power Networks, or for any purpose other than that for which it was prepared. However, we understand that a copy of the report has been requested by AER. We agree that a copy of the report may be provided to AER for their information in connection with this purpose but, as will be made clear in the report, only on the basis that we accept no duty, responsibility or liability to any party, other than you, in connection with the report or this engagement.

It is our understanding that the AER may publish a copy of our report on their website. We accept no responsibility to any person or entity, apart from SA Power Networks that is provided with, or obtains a copy of our report, without our written agreement. No other person or entity is entitled to rely, in any manner, or for any purpose, on this report. We do not accept or assume responsibility to anyone other than the AER for our work, for this report, or for any reliance, which may be placed on this report by any party other than SA Power Networks.



DELOITTE TOUCHE TOHMATSU



Darren Hall

Partner

Chartered Accountant

30 October 2019, Adelaide

Liability limited by a scheme approved under Professional Standards Legislation.

Member of Deloitte Asia Pacific Limited and the Deloitte Network.

3. Detailed Findings

The descriptions of the tests of compliance that were performed, findings relating to the tests of compliance or particular aspects of the engagement, our recommendations and conclusion of whether there has been a breach of the requirements of the Guideline are described below.

The rating of each Obligation has been applied in accordance with *Section 1.2*.

Legal Separation	
Guideline Reference	3.1 (a)
Guideline Obligations	A DNSP must be a legal entity.
Testing	Key Control <ul style="list-style-type: none"> SAPN registered Australian Business Number (ABN) Test Performed <ul style="list-style-type: none"> We performed a search of the ASIC register for SAPN's ABN to verify that SAPN is a separate legal entity. We crosschecked the registered ABN against SAPN's Distribution Network Service Provider Licence.
Observations	Based on the testing performed we have not identified any matters of exception against the obligation.
Recommendation	NA
Management Response*	NA
Rating	No Exception
Legal Separation	
Guideline Reference	3.1 (b)
Guideline Obligations	A DNSP may provide distribution services and transmission services, but must not provide other services.
Testing	Key Control <ul style="list-style-type: none"> Central contract register Test Performed <ul style="list-style-type: none"> We selected a sample of SAPN revenue transactions to detect instances of other services being provided by the DNSP. We selected a sample of Enerven receivable balances and obtained the invoices to check that services are performed against the Enerven ABN. We tested the completeness of the contracts register by checking that a sample of contracts executed by Enerven are included on the contract register.
Observations	<p>Based on the testing performed we have identified the following exception:</p> <p>'Other services' contracts not included on waiver</p> <p>The AER granted SAPN a waiver from the obligation to comply with clause 3.1 of the Guideline from 18 December 2017 to 30 September 2018 so that it may continue to provide Other Services contracted under 20 construction and maintenance contracts.</p> <p>At the time of the initial waiver submission, [REDACTED]. In September 2018 when SAPN applied for an extension to the waiver it was discovered that 4 contracts were not included in the original waiver. SAPN identified these four contracts to the AER in the waiver extension, and reported them as a material breach. On 28 September 2018, the AER granted a waiver extension in relation to the Other Services contracts until the contract expiry in 2021.</p> <p>Subsequently, SAPN identified one contract that was not included on the initial waiver or the waiver extension. This contract was included on the material breach report to the AER. SAPN has rectified this breach by replacing the contract with a new contract with Enerven as the contracting party.</p> <p>The implication of this observation is that 5 SAPN contracts to provide Other Services were not covered by a valid waiver from the obligation to comply with clause 3.1 of the Guideline.</p>

	In the 2018/19 regulatory year the Enerven commercial team [REDACTED] [REDACTED] Intermittent testing on Enerven work-orders was performed by the Enerven Commercial team to identify other services performed under contracts that have not been novated to Enerven. No additional contracts were identified through this process. Any proposed amendments to the waived contracts are required to be discussed with the Regulation branch who will advise the AER of the proposed amendment, as required by the waiver notice.
Recommendation	We recommend that the Enerven commercial team establish preventative controls to ensure that a valid waiver is in place or by establishing a new contract with Enerven as the contracting party before any other services contract is fulfilled where SAPN is the contracting party
Management Response*	Enerven have conducted a review of existing contracts to ensure there are no more contracts where SAPN are the contracting party for other services that are not already on the existing AER-approved waiver. Preventative controls to ensure all Enerven contracts are raised with Enerven as the contracting party include central management of all contracts through the Enerven Commercial Team; providing training/advice to all relevant Enerven teams to ensure their understanding of this requirement; ongoing intermittent testing on Enerven work-order numbers.
Rating	Exception
Separate Accounts	
Guideline Reference	3.2.1 (a)
Guideline Obligations	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.
Testing	Key Control <ul style="list-style-type: none"> SAP accounting system which contains separate General Ledger accounts for recording transactions between SAPN and Enerven Test Performed <ul style="list-style-type: none"> We reviewed SAPN policies regarding maintaining separate accounts. We performed a walkthrough of SAPN's internal accounting procedures.
Observations	Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below: <ul style="list-style-type: none"> SAPN has internal accounting procedures in place that enable it to demonstrate the extent and nature of its transactions with Enerven.
Recommendation	NA
Management Response*	NA
Rating	No Exception
Cost Allocation and Attribution	
Guideline Reference	3.2.2 (a), (b)
Guideline Obligations	A DNSP must allocate or attribute costs to distribution services: <ul style="list-style-type: none"> 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. and must not allocate or attribute other costs to the distribution services it provides.
Testing	Key Control <ul style="list-style-type: none"> Cost Allocation Methodology ("CAM") approved by the AER Cost Allocation Calculation Test Performed <ul style="list-style-type: none"> We reviewed the CAM to confirm that it addresses the allocation of costs between SAPN and Enerven. We reviewed the cost allocation calculation and checked that it is consistent with the AER approved CAM.
Observations	Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below: <ul style="list-style-type: none"> The AER approved CAM addresses the allocation of costs to SAPN and Enerven. SAPN's cost allocation calculation is consistent with the AER approved CAM.

Recommendation	NA
Management Response*	NA
Rating	No Exception
Cost Allocation and Attribution	
Guideline Reference	3.2.2 (c)
Guideline Obligations	A DNSP must establish, maintain and keep records that demonstrate how it meets cost allocation and attribution obligations.
Testing	<p>Key Control</p> <ul style="list-style-type: none"> CAM approved by the AER Cost Allocation Calculation <p>Test Performed</p> <ul style="list-style-type: none"> We obtained and reviewed SAPN's cost allocation calculation, which is consistent with the AER approved CAM.
Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> SAPN maintains cost allocation calculations that are consistent with the AER approved CAM. These demonstrate how SAPN meets its cost allocation and attribution obligations.
Recommendation	NA
Management Response*	NA
Rating	No Exception
Obligation not to Discriminate	
Guideline Reference	4.1(b)
Guideline Obligations	<p>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> <p>i. direct control services by the DNSP (whether to itself or to any other legal entity); and / or</p> <p>ii. contestable electricity services by any other legal entity</p>
Testing	<p>Key Control</p> <ul style="list-style-type: none"> Enerven Engagement Guideline process Service agreements between SAPN and Enerven outlining the basis on which services will be provided Ring-fencing training Call centre script <p>Test Performed</p> <ul style="list-style-type: none"> We inquired of management and reviewed procurement policies to gain an understanding of the processes in place where Enerven is a potential supplier in SAPN sourcing activity. We inquired of management whether Enerven tendered to provide services to SAPN during the audit period. We reviewed the signed service agreements between SAPN and Enerven for evidence that they establish the basis on which services are performed between the entities. We reviewed the online ring-fencing training module for evidence that the obligation not to discriminate is explained in clear terms. We obtained the training report indicating the employees who completed the training and the overall rate of completion. We reviewed SAPN call centre scripts to confirm that appropriate instructions are given in instances where a potential Enerven customer calls. We called SAPN customer services on 3 occasions and inquired about contestable services to confirm they do not recommend Enerven as a provider.

Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> • [REDACTED] • SAPN has established internal policies and procedures where Enerven is a potential supplier during sourcing activity. • SAPN has signed service agreements with Enerven to outline the basis on which services will be provided. • The ring-fencing training module explains the obligation not to discriminate in clear terms. At 30 June 2019 the ring-fencing training module has been completed by 97% of employees. • On the 3 occasions we called the customer services centre and inquired about contestable services, the customer relations representatives did not recommend Enerven as a provider of contestable electricity services. <p>Based on the testing performed we have made the following observations in regards to prior year findings:</p> <p><i>Call centre script refers to Enerven</i></p> <p>In our 30 June 2018 compliance report we reported that the call centre script suggests that a customer relations representative may state "For example, there is Enerven our sister company, who do provide renewable products" when a customer enquires about installing solar products. As a result, we identified a risk that call centre staff may breach the Guideline by recommending Enerven to a caller inquiring about contestable services.</p> <p>Deloitte obtained a copy of the call centre scripts at 30 June 2019 and note that the scripts were amended to remove all mention of Enerven. Deloitte called the call centre on three occasions during the compliance period and inquired about contestable services. On these occasions call centre staff did not recommend or refer to Enerven.</p> <p><i>Call quality monitoring consideration of ring-fencing compliance</i></p> <p>In our 30 June 2018 compliance report we identified that the call quality monitoring process did not consider compliance with the Guideline. As a result, we identified a risk that breaches to the Guideline by customer relations representatives would not be identified and rectified.</p> <p>From 1 July 2018, the Customer Relations Team Leader included ring-fencing compliance for consideration in the monthly call quality monitoring. Deloitte selected a sample of call quality monitoring during the 2018/19 regulatory year and obtained evidence that the Customer Relations Team Leader considered whether the call indicated any breaches of the Guideline.</p> <p>Based on the testing performed we have identified the following improvement opportunities:</p> <p><i>Procurement information access restrictions</i></p> <p>Procurement staff members are a corporate service and are shared by SAPN and Enerven, as permitted under clause 4.2.2(b)(i)(c) of the Guideline. To perform their shared function, procurement staff members have access to SAP and other IT systems that contain confidential information such as current contract files and agreements.</p> <p>When SAPN undertakes sourcing activity where Enerven is a potential supplier, a procurement team representative is appointed to support Enerven. The procurement team representative is required not to access confidential information during the sourcing activity, however there are no formal restrictions within SAP to prevent access to this information.</p> <p>There is a risk that procurement staff will obtain information that gives Enerven an advantage during sourcing activity.</p> <p>We note that in the 2018/19 regulatory year there was no SAPN sourcing activity where Enerven was a potential supplier.</p> <p>For SAP applications, the ability to restrict access between SAPN and Enerven is limited without having separate company codes. The implementation of separate company code in SAP is an extensive IT project with significant costs associated. These costs have been included in SA Power Networks' 2020-25 Regulatory Proposal.</p>
Recommendation	<p><i>Procurement information access restrictions</i></p> <p>We recommend that formal access restrictions are implemented to ensure that procurement representatives supporting Enerven are not able to access information that gives Enerven an advantage during sourcing activity.</p> <p>In the absence of SAP enabling this functionality, we recommend a retrospective review of the procurement team representative's system activity to identify any non-compliance.</p>

Management Response*	<p>Procurement information access restrictions</p> <p>We have provided the AER further information at their request, in relation to sharing of procurement staff. AER staff have provided feedback that they believe sharing of Procurement staff to be in breach of the Guideline due to the nature of the services they provide. AER staff consider that involvement in sourcing activities constitutes 'electricity services' and therefore Procurement staff cannot be shared between our regulated distribution business, and the contestable affiliate business.</p> <p>We do not agree that Procurement staff should be treated differently than other shared corporate services functions, and do not believe sharing these staff is in breach of the Guideline, specifically clauses 4.2.2 and 4.1 (and therefore no breach of clause 4.3).</p> <p><i>Role of Procurement staff</i></p> <p>The SA Power Networks Group Shared Services (Procurement) branch forms part of the Finance Department, which provides a corporate shared service. To the best of our knowledge, procurement functions operate as a 'shared service' within the structure of other DNSPs.</p> <p>At SA Power Networks and Enerven, the services performed by procurement staff are not electricity services. Procurement staff perform an administrative support function, an 'input' to other parts of our business that do provide electricity services (e.g. Network Management Department). Procurement staff gather supplier information, consolidate it, present that information to those other parts of the business for decision making and actioning. Procurement staff in the performance of their role do not:</p> <ul style="list-style-type: none"> • Make decisions about contestable electricity services. These staff do not make decisions in relation to the pricing of supplies, which supplier to engage or on what terms. Those decisions are made by key functional (service delivery) areas; • Put together upstream tenders for work for Enerven. Enerven business development staff are responsible for tenders in which Enerven participates; • Have visibility of who Enerven's competitors are; • Have access to project or tender information for which Enerven is competing and the usefulness or otherwise of any information that SA Power Networks holds in order to be able to identify SA Power Networks information that competitively advantages Enerven; • Perform electricity services; or • Provide Enerven staff with supplier information in relation to SA Power Networks procurement activities. <p>Therefore procurement staff cannot in performance of their roles, functions or duties, engage in discriminatory conduct contrary to 4.1 of the Guideline.</p>
Rating	No Exception
Offices, Staff, Branding and Promotions	
Guideline Reference	4.2.1(a)
Guideline Obligations	A DNSP must use offices that are separate from any offices from which a related electricity service provider provides contestable electricity services
Testing	<p>Key Control</p> <ul style="list-style-type: none"> • Separate offices for SAPN and Enerven • Quarterly office sharing analysis <p>Test Performed</p> <ul style="list-style-type: none"> • We performed a search of the SAPN and Enerven business addresses and visited each entity's offices to confirm that SAPN uses offices that are separate from the offices where Enerven provides contestable electricity services. • We reviewed SAPN's policies in relation to offices, staff, branding and promotions. • We reviewed the quarterly office-sharing analysis.
Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> • SAPN have separate offices from Enerven. • General building access [REDACTED] <p>[REDACTED]</p> <p>[REDACTED]</p> <p>[REDACTED]</p>

	<ul style="list-style-type: none"> In correspondence with SAPN dated 5 April 2019, Angela Bourke of the AER noted that "Your letter has helped us to better understand how SA Power Networks is meeting its obligations in regard to the physical separation of its staff from those of Enerven. I note that there is an ongoing level of risk of discrimination, albeit low."
Recommendation	NA
Management Response*	NA
Rating	No Exception
Staff Sharing	
Guideline Reference	4.2.2(a)
Guideline Obligations	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.
Testing	<p>Key Control</p> <ul style="list-style-type: none"> Quarterly staff sharing analysis <p>Test Performed</p> <ul style="list-style-type: none"> We reviewed SAPN's policies in relation to staff sharing. We reviewed the quarterly staff sharing analysis. We selected a sample of 5 staff that cannot be shared by SAPN and Enerven. We obtained their position descriptions to confirm that they are not performing work for both SAPN and Enerven.
Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> SAPN has established internal policies and procedures designed to prevent staff sharing in circumstances not allowed by the Guideline. Staff sharing analysis is performed quarterly to identify staff members that are not able to be shared. <p>Based on the testing performed we have made the following observations in regards to prior year findings:</p> <p>Informing staff who cannot be shared following review of staff sharing analysis</p> <p>In our 30 June 2018 compliance report, we reported that the regulation team did not review the quarterly staff sharing analysis and did not communicate ring-fencing obligations to staff who were identified as not able to be shared.</p> <p>As a result, we identified the risk that staff that not able to be shared would perform duties for both SAPN and Enerven as they are not aware of their obligations. Further, where reviews are not documented, it is not possible to monitor whether the control is operating effectively.</p> <p>From 1 July 2018, the regulatory analyst has documented their review of the quarterly staff sharing analysis and informed hiring managers of all staff who have been identified as being unable to be shared.</p>
Recommendation	NA
Management Response*	NA
Rating	No Exception
Branding and Cross-promotion	
Guideline Reference	4.2.3(a)
Guideline Obligations	<p>A DNSP:</p> <ul style="list-style-type: none"> 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. 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). iii) must not advertise or promote contestable electricity services provided by a related electricity service provider other than the DNSP itself.

Testing	<p>Key Control</p> <ul style="list-style-type: none"> • Social media and website approval process • Call centre scripts <p>Test Performed</p> <ul style="list-style-type: none"> • We reviewed SAPN's policies relating to branding and cross promotion. • We inspected the SAPN website and social media pages for graphics or posts that would lead a reasonable person to infer that SAPN and Enerven are related or that show cross-advertisement, cross-promotion, or promotion of Enerven services. • We selected a sample of 5 updates to the SAPN website a sample of 10 social media posts made in the audit period and checked that the appropriate approval was obtained. • We selected a sample of 5 customer complaints and queries and investigated for evidence of customer complaints regarding branding or cross-promotion. • We reviewed SAPN call centre scripts for evidence of promotion of contestable electricity services provided by Enerven. • We called SAPN customer services and inquire about contestable services for evidence that Enerven is not recommended as a provider.
Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> • Distinctly separate Enerven branding has been developed for use when performing contestable electricity services. • Website and social media approval controls are appropriately designed and operated effectively during the 2018-19 regulatory year. • SAPN does not promote its direct control services and its contestable electricity services that are not direct control services together. <p>Based on the testing performed we have identified the following improvement opportunity:</p> <p>Vehicle Branding</p> <p>Enerven vehicles contain the branding "Enerven an SA Power Networks company" are used when performing other non-electricity services, but not when performing contestable electricity services.</p> <p>SAPN has not designed and implemented controls to ensure that this branding is not used when performing contestable electricity services.</p> <p>There is a risk that a vehicle containing the branding "Enerven an SA Power Networks company" is used when performing contestable electricity services.</p>
Recommendation	We recommend that management design and implement formal controls and processes to prevent the branding "Enerven an SA Power Networks company" from being used when performing contestable electricity services.
Management Response*	The Regulatory Analyst will work with Field Services teams to develop and implement a formal process and controls in relation to the use of vehicles branded "Enerven an SA Power Networks company".
Rating	No Exception
Office and Staff Registers	
Guideline Reference	4.2.4 (a), (b)
Guideline Obligations	<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; and</p> <p>(b) the nature of the positions (including a description of the roles, functions and duties) of its members of staff and must make the register publicly available on its website.</p>
Testing	<p>Key Control</p> <ul style="list-style-type: none"> • Office and staff registers • Quarterly staff sharing analysis • Quarterly office sharing analysis <p>Test Performed</p> <ul style="list-style-type: none"> • We sighted that the office and staff register is publicly available on the SAPN website. • We crosschecked the office and staff register against the results of the office/location and staff sharing analysis to ensured that the office and staff registers are appropriately maintained and updated.

Observations	Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below: <ul style="list-style-type: none"> SAPN maintains an office and staff register, which is publically available on its website and updated quarterly based on the results of the office sharing analysis and staff sharing analysis.
Recommendation	NA
Management Response*	NA
Rating	No Exception
Protection of Confidential Information	
Guideline Reference	4.3.2 (a) (b)
Guideline Obligations	A DNSP must: (a) keep confidential information confidential (b) only use confidential information for the purpose for which it was acquired or generated
Testing	Key Control <ul style="list-style-type: none"> Information Classification and Handling Procedure IT access approval IT access review Test Performed <ul style="list-style-type: none"> We reviewed the SAPN Policies in regards to the protection of confidential information. We reviewed the customer complaints register for evidence of customer complaints that indicate the disclosure of confidential information. We reviewed the list of critical applications for completeness. We tested the design and operating effectiveness of IT access review controls. We tested the design and operating effectiveness of IT access approval controls
Observations	<p>Based on the testing performed we have made the following two observations that have been classified as exceptions:</p> <p><i>Enerven staff accessing critical applications</i></p> <p>Deloitte obtained access logs for IT applications containing confidential information ("critical applications") on a sample basis. We identified two staff members who were seconded to the Enerven [REDACTED] Program Management team who accessed critical applications in the period 1 July 2018 - 30 June 2019.</p> <p>One employee was seconded from the Enerven metering team to the Enerven [REDACTED] Program Management team on 9 March 2019. The staff member accessed the [REDACTED] system on 10 occasions and the [REDACTED] on 18 occasions in the period 9 March 2019 – 30 June 2019. The employee accessed these systems to obtain site data in preparation for [REDACTED] site visits.</p> <p>The second employee was seconded from SAPN to Enerven on 12 January 2019. The staff member accessed [REDACTED] on 2 May 2019. [REDACTED] is a customer billing system and contains confidential electricity customer information. [REDACTED] is a SAPN developed application for viewing and reporting on interval metered and CT-metered customers. [REDACTED] contains confidential electricity information in accordance with the clause 4.3 Guideline definition.</p> <p>These staff members' access to critical applications was not considered for ring-fencing compliance at the commencement of their secondments.</p> <p>Once it was identified that these staff members had retained their access to these critical applications, the IT team reviewed and restricted these staff's IT access.</p> <p>From 1 January 2018 SAPN had manual controls in place that were intended to ensure that IT access to critical applications is reviewed prior to staff movements to Enerven.</p>

	<p>The control required a transfer or secondment checklist to be completed and returned when staff members are transferred or seconded to Enerven for a period greater than 6 weeks. When completing the checklist, hiring managers are required to ensure that staff access to critical applications is restricted. The checklists require the hiring managers to sign off on the following items:</p> <ul style="list-style-type: none"> • "Ensure employee is familiar with their ring-fencing obligations (employee to retake ring-fencing training if required)"; and • "Does the employee have access to any of the following restricted systems/applications? (If so, remove access where no longer required, or if still required advise Regulation Branch of the employees new position)". <p>In our 30 June 2018 compliance report, we identified that in the 6 months to 30 June 2018 there was no process in place to monitor whether transfer or secondment checklists had been completed by hiring managers or whether hiring managers had appropriately restricted access to controlled applications. In our 30 June 2018 compliance report we recommended that:</p> <ul style="list-style-type: none"> • HR implement controls to monitor whether checklists are completed and returned; and • checklists be required for all secondments, regardless of their duration. <p>At the start of the 2018/19 regulatory year, the Human Resources department designed controls to monitor the completion of checklists where staff movements have occurred. These controls require HR staff to generate a report from SAP that identifies staff secondments and transfers to Enerven each month. HR staff are required to ensure that the hiring manager has prepared and signed a transfer or secondment checklist for the staff member. If a signed induction checklist is not completed, the HR team member contacts the hiring manager to ensure that a checklist is completed.</p> <p>The correct secondment checklist was not completed for the two staff members seconded to the Enerven [REDACTED] Project team. For one secondment, a checklist was completed however the correct checklist was not used and therefore the item to review IT system access was not included. The other secondment was from an internal Enerven distribution team to the Enerven [REDACTED] Project team. HR did not identify this during their monthly review. This indicates that controls to monitor the completion of secondment checklist were not appropriately designed and implemented during the year.</p> <p>SAP and IT application access restrictions</p> <p>In December 2017, the ring-fencing project management office ("PMO") identified 24 critical applications. Controls were designed to ensure that access to these critical applications was appropriately monitored and restricted.</p> <p>As outlined in our 30 June 2018 compliance report, when determining the list of critical applications, the PMO initially applied a definition of confidential information that was restricted to customer information that is not publicly available. Network and service information was not included in the definition of confidential information against which IT systems were assessed. Resultantly, IT applications that contain network and services information were not included in the list of critical applications.</p> <p>Per clause 4.3 of the Guideline, 'confidential information' means electricity information generated by a DNSP in connection with its provision of direct control services that is not already publicly available. Electricity information includes information about the electricity network, electricity customers or electricity services, but does not include non-customer financial information or non-customer performance information.</p> <p>The PMO also did not include SAP applications in the list of critical applications. As a result, the list of critical applications in the 6 months to 30 June 2018 was not complete.</p> <p>The list of critical applications is integral to the operation of key IT access controls such as the quarterly IT access review and the IT application access approval process.</p> <p>In July 2018, the IT team reassessed the list of critical applications by applying the guideline definition of confidential information. This assessment expanded the list to 35 critical applications.</p> <p>To test whether the revised list of critical applications is complete, Deloitte obtained a list of all IT applications at 30 June 2019 and assessed whether a sample of these IT applications contain confidential information that users are able to access.</p> <p>Our testing identified various SAP applications such as [REDACTED] and [REDACTED] that contain confidential information that are not included on the list of critical applications. Our testing did not identify any non-SAP applications that contained confidential information that were not included on the list of critical applications.</p> <p>Notwithstanding a number of mitigating controls such as extensive training and a quarterly management representations process, there is a risk that Enerven staff continue to have unrestricted access to SAP systems that contain confidential information.</p>
--	---

	<p>SAPN's ability to restrict SAP access for Enerven staff members is limited as separate company codes have not been established within SAP. The implementation of separate company codes in SAP is an extensive IT project with significant costs associated. These costs have been included in SA Power Networks' 2020-25 Regulatory Proposal.</p> <p>Based on the testing performed we have identified the following improvement opportunities:</p> <p>IT Access Approval</p> <p>In the 6 months to 30 June 2018 applications for Enerven staff to receive access to critical applications were assessed for ring-fencing compliance and approved by the ring-fencing project management office ("PMO"). As outlined in our 30 June 2018 compliance report, we were not able to obtain evidence that these applications were in all cases approved by the PMO.</p> <p>From July 2018 the IT service desk implemented a business process that requires Enerven staff to request access to critical applications through the [REDACTED] system. The application is reviewed for ring-fencing compliance and approved by the relevant business owner prior to access being granted.</p> <p>Deloitte obtained a list of all applications for Enerven staff to obtain access to critical applications that were lodged through the [REDACTED] system in the period 1 July 2018 – 30 June 2019. We selected a sample and identified 4 instances where Enerven staff sought and obtained access to critical applications where the approval to grant access to the critical application was not documented.</p> <p>Approval for these applications was retrospectively documented in June and July 2019 and these staff member's access to these critical applications is permissible under the Guideline. However, where the approval of access to critical IT applications is not documented, it is not possible to monitor whether the approval control is operating effectively.</p> <p>IT Access Review</p> <p>From 1 July 2018, the IT team performed a quarterly review of Enerven staff with access to critical applications. The review is performed with to identify any Enerven staff members who have access to a critical application without the appropriate approval or where access to the critical application is not permissible under the Guideline.</p> <p>We made the following observations in relation to the quarterly IT access review:</p> <ul style="list-style-type: none"> • The review is not documented for all critical applications; • The reviewer's considerations are not documented (i.e. there is no evidence of the assessment of whether an employee's access is permissible under the Guideline); • The review is performed by various IT teams and is not performed or documented consistently for all critical applications. <p>Where the quarterly review is not performed consistently it may not be effective in detecting instances where staff have access to critical applications without a valid exemption under the Guideline.</p> <p>Where the review is not documented it is not possible to monitor whether the control is operating effectively.</p>
Recommendation	<p>Enerven staff accessing critical applications</p> <p>We recommend that:</p> <ul style="list-style-type: none"> • All staff movements are recorded in SAP (including short term secondments and secondments between Enerven teams); • A staff movement report is obtained from SAP at the end of each month to identify staff movements to an Enerven team; and • Where staff movements have occurred, that IT consider the staff's access to any critical applications and restrict access where not permissible under the Guideline. <p>SAP and IT application access restrictions</p> <p>We recommend that SAPN:</p> <ul style="list-style-type: none"> • Implement formal access restrictions in SAP by establishing a separate company code; • Undertake regular monitoring of access to confidential applications in SAP for ring-fencing compliance. <p>IT Access Approval</p> <p>We recommend that approval of requests to access critical applications be formally documented, including the reason why access is permissible under the ring-fencing guideline.</p>

	<p>IT Access Review</p> <p>We recommend that IT:</p> <ul style="list-style-type: none"> • Document their review of all critical applications, including those where no Enerven staff are identified as having access to the critical application; • Document the variables considered while performing the review; and • Develop a consistent methodology for reviewing access to ensure that the review is performed and documented consistently across all critical applications.
Management Response*	<p>Enerven staff accessing critical applications</p> <p>A communication has been issued to all Enerven staff confirming the HR secondment and transfer process and reiterated the requirement for any staff secondment to involve the Enerven HR Talent Manager prior to commencement. The Talent Manager will ensure the correct HR secondment checklist is completed, and access restrictions are imposed prior to the commencement of any secondment.</p> <p>HR has implemented new digital checklists that have replaced the paper-based checklists with a new digital form. The checklists will be launched by a HR Officer at the earliest possible point in each recruitment process and will workflow to and between leaders and staff via emails, with instructions and links directly to the checklist.</p> <p>The 'Transferring Employee' induction checklist (which is now initiated by HR for all employee moves between business units – for secondments, permanent internal appointments, redeployment opportunities and realignment of roles and / or functions), contains a specific ring-fencing section in the 'pre-commencement' leader tasks section. If ring-fencing compliance actions apply to the employee move, both HR and the leader will ensure that all ring-fencing related tasks outlined in the checklist are completed <u>prior</u> to the employee commencing in their new position.</p> <p>All secondments and transfers (regardless of duration) will be actioned through the HR branch, and recorded in SAP. HR will monitor progress of the checklists weekly to ensure pre-commencement obligations are met.</p> <p>SAP and IT application access restrictions</p> <p><i>Background</i></p> <p>SAP was implemented in 1997 and at that time the Construction and Maintenance Services (CAMS) Department, now known as Enerven, was set up together with joint procurement and financial operations as common services. Currently, SA Power Networks and Enerven are a single entity within SAP. The work to establish a separate company code in SAP for Enerven is highly complex and will require involvement of several business units across SA Power Networks and Enerven. It will include the review and modification of every SAP business process for Enerven (and several of SA Power Networks'), which is made more challenging by the current customisations in SAP that were created to suit SA Power Networks, and significant other IT projects currently underway. For these reasons, which are elaborated on below, it is not possible to commence implementation of a new SAP company code until after July 2020.</p> <p><i>Action Plan</i></p> <p>As is highlighted in our Regulatory Proposal for the 2020-25 Regulatory Control Period (RCP) Supporting Business Case "Ringfencing Compliance: Information Technology solution", the manual controls we have for SAP access are a risk-area. The business case driver for this IT project is the need to ensure ongoing ringfencing compliance by implementing improved compliance controls in the most efficient way (for regulated customers), being that Enerven continue to utilise SAPN's systems and is allocated its share of IT costs rather than Enerven have its own separate system(s) and regulated customers pay 100% of the costs. To minimise any ring-fencing non-compliance risk this project will implement stronger ex ante automated system controls, including the set up of a new company code in SAP to separate the regulated and unregulated entities, and also to implement more robust system-based information access controls for all applications that contain confidential information. Creation of a new company code in SAP will enable restricted access at transaction level between SA Power Networks information and Enerven information.</p> <p>We have reviewed options for interim controls and found that the only solution that will completely resolve the issue is implementation of a new company code in SAP as described above. An option we investigated was to use a separate SAP Purchasing Group for Enerven to restrict certain procurement information access between SA Power Networks and Enerven. The intention of this interim solution was that Enerven would have a separate Purchase Group (high level) code and would not be able to directly access or view SA Power Networks' purchase orders (low level), purchase requisitions and invoices. However, detailed user testing found that Enerven could still access the same information via other financial transactions, which could not be restricted using a Purchasing Group.</p>

	<p>Our proposed actions are therefore to reinforce existing controls (training, company-wide Directives and Policies, Quarterly Compliance Questionnaires, Audits, etc); and we are seeking funding in SA Power Networks' Regulatory Proposal for the 2020-2025 Regulatory period, for the IT ring-fencing project to create a separate company code for Enerven in SAP.</p> <p>IT Access Approval</p> <p>While the approvals process and appropriate record of those approvals is detailed in the Application Access Work Instruction, there were instances identified in Deloitte's Independent Assessment where approvals had not been recorded.</p> <p>IT Teams have been reminded of the critical importance by IT Management of adhering to the Application Access Work Instruction (which includes the requirement to record all system access approvals including reasons). The approval for ANY Enerven staff requesting access to critical systems will be automated in the IT service request management tool () to remove opportunity for human error. The automated approval, which will be recorded, will incorporate the detailed ring-fencing specific approval templates, and will stop the subsequent access provision process if appropriate approval is not granted via the IT service request management () tool.</p> <p>An IT Ring-fencing Compliance Group has been established and meetings are now held monthly with key staff representing all IT teams, to ensure all new staff understand the IT Application Access Work Instruction and Quarterly system access review process requirements, and all IT staff are continually reminded of the importance of the process. Team-specific meetings (i.e. Service Desk and Applications teams) will also include ring-fencing as a standing Agenda item. The IT induction process for any new or transferring staff within IT now includes (in addition to the online ring-fencing training activity) a review of the IT Application Access Work Instruction and Quarterly system access review process</p> <p>IT Access Review</p> <p>The quarterly system access review process was implemented from September 2018. The requirement was communicated by email and verbally to all IT Applications Team Leaders, however the process was not formally documented, including reporting format requirements. In their Independent Assessment, Deloitte has identified some process improvement opportunities in relation to these regular system access reviews and as a result, the following interim activities have been undertaken to improve our controls in October 2019:</p> <p>1. The process has now been documented by the Applications Team Leader, and approved by the Applications Support Services Manager, Manager SAP Services, and Manager Digital and Mobile Solutions. The process includes:</p> <ul style="list-style-type: none"> • Reporting frequency and due dates • Applicable systems for reporting (and team leader responsible) • Reporting format • Level 3 Manager review and approval (with approval records maintained) of all quarterly system access review reports all recorded in central repository for future reference <p>2. The process has been provided and clearly communicated to all applicable team leaders and Level 4 managers.</p> <p>In our Regulatory Proposal for the 2020-2025 period, we have proposed funding to implement more robust system-based information access controls and associated audit reporting for all applications that contain confidential information.</p>
Rating	Exceptions in relation to staff transfers/secondments and procurement staff access in SAP
Disclosure of Information	
Guideline Reference	4.3.3 (a)-(g)
Guideline Obligations	<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 in response 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>

	(g) 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.
Testing	<p>Key Control</p> <ul style="list-style-type: none"> • Requests for Information Procedure • Information Classification and Handling and Management Directive • Requests for Information Procedure • Information Sharing Protocol • Information Sharing Web Form • Information Sharing Terms and Conditions • Information Register <p>Test Performed</p> <ul style="list-style-type: none"> • We reviewed SAPN's policies in relation to the disclosure of information. • We performed inquiries to determine whether SAPN has disclosed any confidential information in the audit period. • We reviewed the customer queries and complaints register for evidence of customer complaints that indicate the disclosure of confidential information.
Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> • SAPN has developed policies and procedures to ensure that confidential information is disclosed only where permitted under the Guideline. • SAPN has not disclosed confidential information in the audit period.
Recommendation	NA
Management Response*	NA
Rating	No Exception
Information Register	
Guideline Reference	4.3.5 (a) - (c)
Guideline Obligations	<p>(a) A DNSP must establish, maintain and keep a register of all:</p> <p>i. related electricity service providers;</p> <p>ii. other legal entities who provide contestable electricity services but who are not affiliates of the DNSP; 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> <p>i. identify the kind of information requested by the legal entity; and</p> <p>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> <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>
Testing	<p>Key Control</p> <ul style="list-style-type: none"> • Information Register <p>Test Performed</p> <ul style="list-style-type: none"> • We sighted that the information register is publicly available on SAPN's website. • We confirmed that there were no disclosures of confidential information in the audit period by sighting the results of the Information Sharing Web Form.
Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> • SAPN has established an information register that is publically available on the SAPN website. • SAPN has processes in place to maintain the information register.
Recommendation	NA

Management Response*	NA
Rating	No Exception
Conduct of Service Providers	
Guideline Reference	4.4.1 (a)
Guideline Obligations	A DNSP: (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: i. clauses 4.1, 4.2.1, 4.2.2 and 4.3.2 of this Guideline; and ii. clause 4.2.3 of this Guideline in relation to the brands of the DNSP; as if the service provider was the DNSP
Testing	Key Control <ul style="list-style-type: none">SAPN Standard Terms and Conditions Test Performed <ul style="list-style-type: none">We reviewed SAPN Standard Terms and Conditions and checked that it requires service providers to comply with clauses 4.1, 4.2.1, 4.2.2, 4.3.2 and 4.2.3 of the Guideline.We selected a sample of 5 suppliers with new contracts entered into in the period and confirmed that the Standard Terms and Conditions attached to the contract contained the requirement to comply with clauses 4.1, 4.2.1, 4.2.2, 4.3.2 and 4.2.3 of the Guideline.
Observations	Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below: <ul style="list-style-type: none">SAPN standard terms and conditions requires service providers to comply with clauses 4.1, 4.2.1, 4.2.2, 4.3.2 and 4.2.3 of the Guideline.
Recommendation	NA
Management Response*	NA
Rating	No Exception
Conduct of Service Providers	
Guideline Reference	4.4.1 (b)
Guideline Obligations	A DNSP: (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.
Testing	Key Control <ul style="list-style-type: none">SAPN Standard Terms and ConditionsSupplier Contract Amendment Letter Test Performed <ul style="list-style-type: none">We reviewed the SAPN Standard Terms and Conditions and checked that they do not directly or indirectly, encourage or incentivise service providers to engage in conduct, which, if the SAPN engaged in the conduct itself, would be contrary to the DNSP's obligations.We selected a sample of 5 suppliers with new contracts entered into in the period and confirmed that the revised Standard Terms and Conditions were attached.
Observations	Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below: <ul style="list-style-type: none">SAPN standard terms and conditions requires service providers to comply with clauses 4.1, 4.2.1, 4.2.2, 4.3.2 and 4.2.3 of the Guideline.
Recommendation	NA
Management Response*	NA
Rating	No Exception

Waiver Register	
Guideline Reference	5.7 (a)
Guideline Obligations	A DNSP must establish, maintain and keep a register of all waivers (including any variation of a waiver) and must make the register publicly available on its website
Testing	Key Control <ul style="list-style-type: none"> Waiver register Test Performed <ul style="list-style-type: none"> We sighted that the waiver register is publicly available on SAPN's website. We crosschecked the details contained on the waiver register against the waiver decisions published on the AER website.
Observations	Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below: <ul style="list-style-type: none"> The waiver register is publically available on the SAPN website. SAPN's waiver register is consistent with the AER waiver decisions.
Recommendation	NA
Management Response*	NA
Rating	No Exception
Waiver Register	
Guideline Reference	5.7 (b)
Guideline Obligations	The register established under clause 5.7(a) must include: <ol style="list-style-type: none"> the description of the conduct to which the waiver or interim waiver applies; and the terms and conditions of the waiver or interim waiver; 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.
Testing	Key Control <ul style="list-style-type: none"> Waiver register. Test Performed <ul style="list-style-type: none"> We crosschecked the details contained on the waiver register against the requirements of the Guideline.
Observations	Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below: <ul style="list-style-type: none"> The details contained on SAPN's waiver register are consistent with the requirements of the Guideline.
Recommendation	NA
Management Response*	NA
Rating	No Exception
Maintaining Compliance	
Guideline Reference	6.1
Guideline Obligations	A DNSP must establish and maintain appropriate internal procedures to ensure it complies with its obligations under this Guideline.
Testing	Discussions held with: <ul style="list-style-type: none"> Regulatory Analyst Learning and Development Manager Key Control <ul style="list-style-type: none"> Quarterly Internal Compliance Questionnaire Dedicated regulatory team

	<ul style="list-style-type: none"> • Ring-Fencing Training <p>Information Obtained</p> <ul style="list-style-type: none"> • Regulation Ring-Fencing Compliance Procedure • Ring-Fencing Training module and completion report <p>Test Performed</p> <ul style="list-style-type: none"> • We reviewed the Regulation Ring-Fencing Compliance Procedure. • We reviewed the responses to the Regulation Ring-Fencing Quarterly Internal Compliance Questionnaire. • We reviewed the online ring-fencing training module for evidence that the ring-fencing obligations are explained in clear terms. • We obtained the training report indicating the employees who completed the training and the overall rate of completion.
Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> • SAPN has developed policies and procedures to ensure that it complies with the obligations under the Guidelines. • The ring-fencing training module explains the Guideline obligations in clear terms. • At 30 June 2018 96% of staff had completed the mandatory ring-fencing training. <p>Based on the testing performed we have made the following observations in regards to prior year findings:</p> <p>Review of quarterly compliance questionnaire</p> <p>The regulation team obtains responses to the quarterly compliance questionnaire from managers who are held accountable for ring-fencing compliance in their area of the business.</p> <p>In our 30 June 2018 compliance report, we reported that we were not able to obtain evidence of the Head of Regulation's review of management's responses to the quarterly compliance questionnaire.</p> <p>Where reviews are not documented, management and the Board of Directors are unable to monitor whether the control is operating effectively.</p> <p>From 1 July 2018, the regulatory analyst obtains the responses to all completed quarterly compliance questionnaires and summarises the responses to the Head of Regulation via email. The Head of Regulation reviews the quarterly emails to identify any ring-fencing concerns or potential breaches to the Guideline. When potential breaches are identified, the regulatory team and the Ring-fencing Breach Committee assess the materiality of the breach and determines whether the breach should be reported to the AER. The regulatory team then works with the business to develop strategies to address the breach.</p> <p>Review of ring-fencing training attendance for new starters</p> <p>When new staff commence, it is the responsibility of the hiring manager to use the induction checklist to ensure that staff complete all mandatory training, including the ring-fencing training, within 3 months.</p> <p>In our 30 June 2018 compliance report we reported that the learning and development team do not monitor staff attendance of the training.</p> <p>During the 2018/19 regulatory year the learning and development team has, on a monthly basis, notified team leaders of any new starters whom they have hired who are yet to complete their mandatory ring-fencing training. The respective team leaders are required to follow-up with these new starters on completing their mandatory training.</p> <p>The HR induction checklist has also been modified to include the requirement for new hires to complete the mandatory ring-fencing training.</p> <p>Based on the testing performed we have identified the following improvement opportunities:</p> <p>Ring-fencing e-learning</p> <p>The current ring-fencing e-learning training does not include an assessment at the conclusion of the training.</p> <p>Staff are able to complete the e-learning without demonstrating an understanding of the Guideline.</p> <p>Training for level 3 managers and above</p> <p>Attendance of the level 3 managers and above at the informal ring-fencing training session during June 2019 was not monitored.</p> <p>Not all managers may have attended the training session, and thus may not have refreshed their understanding of the ring fencing obligations.</p>

Recommendation	<p>Ring-fencing e-learning We recommend that management require staff to complete an assessment at the conclusion of the ring-fencing e-learning training and attain a certain score to pass the assessment.</p> <p>Training for level 3 managers and above We recommend that management:</p> <ul style="list-style-type: none"> • provide a yearly ring-fencing refresher for level 3 managers and above; • monitor attendance at ring fencing training sessions; and • provide staff who are not able to attend the training session with the relevant resources to refresh their understanding of the ring-fencing obligations.
Management Response*	<p>Ring-fencing e-learning The Regulatory Analyst is developing a ring-fencing Refresher online training module in conjunction with the Learning and Development Branch, for all staff to complete annually. The training includes quiz components for various obligations and while not 'scored' the training must be completed and correct answers viewed prior to the 'complete' status being fulfilled. Training completion will be monitored by the Regulatory Analyst to ensure completion by each staff member annually. The refresher training module is expected to be live by January 2020.</p> <p>Training for level 3 managers and above The Regulatory Analyst is developing a ring-fencing refresher online training module in conjunction with the Learning and Development Branch, for all staff to complete annually. The training includes quiz components for various obligations and while not 'scored' the training must be completed and correct answers viewed prior to the 'complete' status being fulfilled. Training completion will be monitored by the Regulatory Analyst to ensure completion by each staff member annually. The refresher training module is expected to be live by January 2020.</p> <p>Level 3 Managers receive a quarterly questionnaire as a reminder of the obligations that apply to their area of responsibility. Where there are changes to team structure, any new Level 3 Manager is briefed on ring-fencing obligations for their area to ensure understanding.</p>
Rating	No Exception
Annual Compliance Report	
Guideline Reference	6.2.1 (a), (b)
Guideline Obligations	<p>A DNSP must prepare an annual ring-fencing compliance report each regulatory year.</p> <p>The annual compliance report must identify and describe, in respect of the regulatory year to which the report relates:</p> <ol style="list-style-type: none"> the measures the DNSP has taken to ensure compliance with its obligations under this Guideline; any breaches of this Guideline by the DNSP, or which otherwise relate to the DNSP; and all other services provided by the DNSP in accordance with clause 3.1; and the purpose of all transactions between the DNSP and an affiliated entity.
Testing	<p>Key Control</p> <ul style="list-style-type: none"> • Ring-fencing compliance report <p>Test Performed</p> <ul style="list-style-type: none"> • We reviewed the draft 2018-19 ring-fencing compliance report against the requirements of the AER Electricity Distribution Ring-Fencing Guideline – Compliance reporting best practice manual (version 2).
Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> • SAPN has prepared a compliance report that is consistent with the requirements of the AER Electricity Distribution Ring-Fencing Guideline – Compliance reporting best practice manual (version 2).
Recommendation	NA
Management Response*	NA
Rating	No Exception

Annual Compliance Report	
Guideline Reference	6.2.1 (c)
Guideline Obligations	The annual compliance report must be accompanied by an assessment of compliance by a suitably qualified independent authority.
Testing	<p>Key Control</p> <ul style="list-style-type: none"> Ring-fencing compliance report Deloitte has been engaged as the independent authority to assess SAPN's compliance with the Guideline. <p>Test Performed</p> <ul style="list-style-type: none"> We reviewed the draft annual ring-fencing compliance report for evidence that it is accompanied by an assessment of compliance by a suitably qualified independent authority.
Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> SAPN has prepared a compliance report that is consistent with the requirements of the AER Electricity Distribution Ring-Fencing Guideline – Compliance reporting best practice manual. The compliance report is accompanied by an assessment of compliance by a suitably qualified independent authority.
Recommendation	NA
Management Response*	NA
Rating	No Exception
Compliance Breaches	
Guideline Reference	6.3
Guideline Obligations	A DNSP must notify the AER in writing within 5 (five) business days of becoming aware of a material breach of its obligations under this Guideline.
Testing	<p>Key Control</p> <ul style="list-style-type: none"> Breach Management Governance Framework Ring-fencing training module <p>Test Performed</p> <ul style="list-style-type: none"> We reviewed the Breach Management Governance Framework and Breach Reporting Quick Reference Guide. We selected a sample of 5 customer complaints and queries to investigate for instances of non-compliance with the Guideline. We reviewed the online ring-fencing training module for evidence that employees are informed of the breach reporting process. We obtained the training report indicating the employees who completed the training and the overall rate of completion.
Observations	<p>Based on the testing performed we have not identified any matters of exception against the obligation, with key point(s) below:</p> <ul style="list-style-type: none"> SAPN has established processes to ensure material breaches are reported to the AER within 5 days. On 26 July 2019, Deloitte identified an exception regarding Enerven staff accessing IT applications that contain confidential information, as described in this report in the exception titled "Enerven staff accessing critical applications". The exception has been assessed as not material and is therefore not required to be reported to the AER within 5 days of being identified.
Recommendation	NA
Management Response*	NA
Rating	No Exception

*The management response does not form part of the auditor's opinion.