IDEAS | PEOPLE | TRUST

Review of ICT Cyber Expenditure Treatment for 2025-2030 Regulatory Control Period

SA Power Network

Supporting document 5.12.24

18 January 2024

Table of contents

Introduction

BDO have been engaged by SA Power Networks to undertake a review of its proposal to re-classify existing and classify newly proposed ICT cyber expenditure in the next five-year Regulatory Control Period (RCP), 2025-30, commencing 1 July 2025. This report documents the scope, agreed approach and our findings.

Scope and Scope Limitations

The assignment is a consulting engagement as outlined in the 'Framework for Assurance Engagements', issued by the Auditing and Assurances Standards Board, Section 10. Consulting engagements employ an assurance practitioner's technical skills, education, observations, experiences and knowledge of the consulting process. The consulting process is an analytical process that typically involves some combination of activities relating to: objective-setting, fact-finding, definition of problems or opportunities, evaluation of alternatives, development of recommendations including actions, communication of results, and sometimes implementation and follow-up.

The nature and scope of work has been determined by agreement between BDO and SA Power Networks. This consulting engagement does not meet the definition of an assurance engagement, as such we are not proposing an audit in accordance with generally accepted auditing standards.

Except as otherwise noted in this report, we have not performed any testing on the information provided to confirm its completeness and accuracy.

Our report is prepared solely for the use of SA Power Networks and its regulatory proposal to the Australian Energy Regulator (AER) which we understand may be published on the AER website. No responsibility to any third party shall be accepted, as our report has not been prepared, and is not intended, for any other purpose.

This report is based on the latest information made available to us as at the date of this report and we accept no responsibility to update it for events that take place after the date of its issue.

The following items have been excluded from the scope of this review:

1. Except as otherwise noted, we will not perform any testing on the information provided to confirm its completeness and accuracy.
2. In performing our procedures, we will rely upon certain representations made by SA Power Networks and their representatives. We will not perform procedures to verify the accuracy or completeness of such representations.

Approach

To address the objectives of this assignment, the following procedures were determined, agreed and undertaken:

Phase 1: Business Understanding

In this phase, BDO engaged with SA Power Network project managers and key business representatives to understand the nature of the activities undertaken in the programs under review, as referred to in Table 1 below.

SA Power Networks is the monopoly electricity distribution and retail business servicing South Australia. The distribution network system comprises approximately 87,000 kilometres of power lines serving over 820,000 customers across 178,000 square kilometres.

SA Power Networks are preparing their regulated revenue submission to the Australian Energy Regulator (AER) for the 2025-30 Regulatory Control Period (RCP) (1 July 2025 to 30 June 2030). Draft business cases have been prepared to provide options, costs, benefits and timelines to support the submission.

Opinion is being sought regarding relevant accounting classification of ICT Cyber Security costs to operating expenditure (Opex) and capital expenditure (Capex).

Existing **'Cyber Security Refresh'** business case outlays of $13.5[1] million currently classified as capital expenditure (Capex) in the current 2020-25 RCP are proposed as operating expenditure (Opex) of $15.3 million for the 2025-30 RCP. Cyber Refresh business case outlays of approximately $7 million currently classified as operating expenditure (Opex) in the 2020-2025 RCP remain unchanged in total expenditure and Opex classification for the 2025-30 RCP. Operational Technology outlays (currently $4.1 million Capex) remain classified as Capex and are therefore excluded from the classification review.
Refer Table 1.

New outlays of $44.7 million relating to **'Cyber Security Uplift'** are proposed in a separate business case for the 2025-30 RCP and are also considered regarding relevant accounting classification as Opex or Capex. Refer Table 2.

The following tables summarise the investment considerations:

[1] All figures in this document are in real June 2022 dollars.

Table 1: SA Power Networks – Recurrent Cyber Business Case – Summary of Investment

Capability	Purpose	2020-25 Forecast Outlay $m	2025-30 Proposed Outlay $m
Operations	Understand cyber threats, proactive threat management, enhanced response and recovery strategies.	~ $7m Opex ~ $13.5m Capex	~ $7m Opex ~ $15.3m Opex Classification change from Capex to Opex
Digital Identity	Management of the complete identity lifecycle of employees and devices across all platforms, including on-premises, cloud, and mobile devices.		
Cyber Risk and IT Resilience	Documenting, mitigating and overseeing cyber security risk.		
Operational Technology	Visibility of operational technology assets, with thorough monitoring and tightly managed network controls.	~ $4.1m Capex	~ $3.1m Capex

Table 2: SA Power Networks – Cyber Uplift Business Case – Summary of Investment

Capability	Purpose	2025-30 Proposed Non-Recurrent $m	2025-30 Proposed Recurrent $m
Role based user access	User access and permission restrictions. Costs are mainly labour.	$4.2m labour	$3.9m software / $0.3m labour
Application control	To reduce attack surface by restricting how software is executed.	$0.7m labour	$1.3m software
Zero trust architecture	To increase granularity and further restrict permissions / access of users.	$4.1m labour $0.6m software	$1.3m software
Security Operations	To expand Security Operations Team	$5.3m labour	$3.8m software / $0.9m labour
IT resiliency lifecycle	Resources to continuously plan, prepare and test business continuity.	$1.6m labour	$Nil
Secure software development lifecycle	Create sustainable programme, standards, training, education and guidelines to embed security into our entire software development.	$0.7m labour	$0.6m software / $0.5m labour
Third-party security	Resources to conduct risk exposure monitoring of third-party providers and software purchases.	$0.2m labour	$0.4m software
Operational Technology	Embedded Operational Technology security team.	$3.9m labour	$0.9m labour
Information protection	Improved management of information by increased automation and targeted controls.	$2.1m labour	$0.6m software
Tools of trade devices	Update controls associated with tools of trade devices	$1.4m labour	$Nil

Capability	Purpose	2025-30 Proposed Non-Recurrent $m	2025-30 Proposed Recurrent $m
BYOD cyber strategy	Mitigate risks associated with employee personal devices	$1.0m labour	$1.1m software
Network detection and response (NDR)	Implement an NDR solution to enhance network visibility and monitoring capabilities.	$0.8m labour	$0.2m software
Cyber awareness	Education programme	$1.5m labour	$Nil
MyID	Improved identity management.	$0.6m labour	$Nil
TOTAL (Rounded)		**$28.2m labour $0.6m software $28.8m total**	**$13.3m software $2.7m labour $15.9m total**

Phase 2: Business Information Analysis

In this phase, we conducted a review of the information obtained as part of phase 1.

Work completed:

- Reviewed and considered relevant extracts provided by SA Power Networks from the following business cases, including the activities associated with each program:
  - 5.12.9 SAPN 2025-30 RESET Cyber Security Uplift Business Case
  - 5.12.6 SAPN 2025-30 RESET Cyber Security Refresh Business Case
- Reviewed publicly available information relating to the regulatory accounting treatment of outlays
- Considered the reasonableness of expensing the costs associated with these programs for regulatory purposes considering accounting standards and regulatory practice in Australia. Further information in relation to guidance drawn from accounting standards and other relevant Australian Accounting Standards Board (AASB) pronouncements, is provided in Appendix 1.

Phase 3: Report Findings

This report documents a summary of our findings ('Key Findings') and a detailed explanation of our findings (provided in Appendix 2).

Summary of Key Findings

Recurrent Cyber Business Case

Based on the information provided we consider SA Power Networks proposal to classify Cyber Security Refresh (Operations, Digital Identity, and Cyber Risk and IT Resilience) outlays as Opex expenditure is reasonable and we consider consistent with Accounting Standards. Outlays of $13.5 million currently classified as Capex in the 2020-25 RCP, are proposed to increase to $15.3 million in the 2025-30 RCP, with the proposed outlay to change classification from Capex to Opex. Existing recurrent Opex outlays approximating $7 million across Operations, Digital Identity, and Cyber Risk and IT Resilience remain unchanged with respect to accounting classification. Ongoing hardware and installation costs for Operational Technology requirements will remain as Capex.

The classification change from Capex to Opex relating to the Recurrent Cyber business case is considered reasonable with the relevant key points being as follows:

- These outlays meet the Australian Accounting Standard Board's (AASB) Framework (Framework) for the Preparation and Presentation of Financial Statements[2] definition of 'expense,' which in paragraph 70 (b) defines an expense as *'decreases in economic benefits during the accounting period in the form of outflows or depletions of assets or incurrences of liabilities that result in decreases in equity, other than those relating to distributions to equity participants.'* Further at paragraph 78 it is stated to *'encompass losses as well as those expenses that arise in the course of the ordinary activities of the entity'*.
- Paragraph 69(b) of the AASB Framework also provides clarity regarding 'expenses'. Paragraph 97 goes on to state *'An expense is recognised immediately in the income statement when an expenditure produces no further economic benefits or when, and to the extent that, future economic benefits do not qualify, or cease to qualify, for recognition in the balance sheet as an asset.'*
- AASB Standard 138 Intangible Assets[3] scope definitions also provide the following guidance at Paragraph 4:

  'in determining whether an asset that incorporates both intangible and tangible elements should be treated under AASB 116 Property, Plant and Equipment or as an intangible asset under this standard, an entity uses judgement to assess which element is more significant.'

- The treatment of these outlays as Opex is also supported by the AASB Framework in that these activities do not materially add to the value of existing assets by extending their life or increasing their capacity. As such, we believe the expenditure associated with these overhead activities should be treated as operating expenditure.
- Further, given the activities and programs are all integral to SA Power Networks ongoing business of earning operating revenues from the use of these assets, we believe the expenditure should be recognised at the time incurred in accordance with paragraphs 94 and 95 of *the* Framework:
  - Paragraph 94 states that *'Expenses are recognised in the income statement when a decrease in future economic benefits related to a decrease in an asset or an increase of a liability has arisen that can be measured reliably.'*
  - Paragraph 95 states that *'Expenses are recognised in the income statement on the basis of a direct association between the costs incurred and the earning of specific items of income. This process, commonly referred to as the matching of costs with revenues, involves the simultaneous or combined recognition of revenues and expenses that result directly and jointly from the same transactions or other events.'*
- SA Power Networks Cost Allocation Method does not require any change.

[2] Australian Accounting Standards Board – Framework for the Preparation and Presentation of Financial Statements – prepared on 29 October 2021, for application to annual reporting periods beginning on or after 1 July 2021.

[3] Australian Accounting Standards Board (AASB) 138 – Intangible Assets – Compilation no. 5 31 December 2022.

Cyber Uplift Business Case

New costs of $44.7 million relating to the Cyber Uplift business case relate to mitigating cyber security risk across a range of areas. The 2025-30 Regulatory Control Period outlays comprise Non-Recurrent outlays of $28.2 million labour, and $0.6 million software, and Recurrent outlays of $2.7 million labour and $13.3 million software.

The classification as Opex relating to the Cyber Uplift business case is considered reasonable and we consider consistent with Accounting Standards, with the relevant key points being as follows:

- The definition of an expense as provided in paragraphs 69(b) and 97 of the AASB Framework for the Preparation and Presentation of Financial Statements supports the treatment of these non-recurrent costs as Opex. The basis of this opinion is the operational nature of this activity and that it is not materially extending the useful life or increasing the capacity of SA Power Networks in a measurable way.
- AASB's *Framework for the Preparation and Presentation of Financial Statements*, BDO considers this outlay does not meet the future economic benefit requirement to be classified as an asset, and that the expenditure meets the definition of an expense and that it should be recognised as operating expenditure at the time incurred. These outlays are considered as Opex.
- BDO believe that the costs associated with the additional recurrent Cyber Security outlays are of an ongoing operational nature. This is supported / underpinned by the AASB 'Framework' in that the activities do not materially add to the value of existing assets by extending their life or increasing their capacity, but rather this expenditure should be classified as operating expenditure.
- $2.6 million of non-recurrent outlays relating to predominantly integration components of SaaS are classified as Capex in accordance with Framework guidance.

Having assessed the underlying objective and outcomes from these activities, with the exception of the $2.6 million relating to predominantly integration components of SaaS, which are classified as Capex, BDO considers it is reasonable for the non-recurrent expenditure outlays to be treated as Opex from 2025.

Based on the information provided we consider it reasonable and appropriate that SA Power Networks classify the proposed items in Recurrent Cyber business case and Cyber Uplift business case outlays as operating expenditure (Opex).

Appendix 1 - Guidance in Accounting Standards, AASB pronouncements and internal policies.

Overarching context

Australian Accounting Standards, the Australian Accounting Standards Board 'Framework for the Preparation and Presentation of Financial Statements', and SA Power Networks Cost Allocation Method (i.e. their Accounting Principles and Policies) provide guidance in determining the treatment of capital (Capex) and operating (Opex) outlays.

The Australian Accounting Standards Board (AASB) is an Australian Government agency constituted under Part 12 of the *Australian Securities and Investments Commission Act 2001 (ASIC Act)*. The functions of the AASB, as reflected in section 227 of the ASIC Act, include the development and maintenance of high-quality accounting standards for all sectors of the Australian economy.

Under the ASIC Act, the statutory functions of the AASB are:

- to develop a **conceptual framework** for the purpose of evaluating proposed standards;
- to make **accounting standards** under section 334 of the *Corporations Act 2001*;
- to formulate accounting standards for other purposes;
- to participate in and contribute to the development of a single set of accounting standards for worldwide use;
- and to advance and promote the main objects of Part 12 of the ASIC Act, which include reducing the cost of capital, enabling Australian entities to compete effectively overseas and maintaining investor confidence in the Australian economy.

The **AASB Conceptual Framework** provides the foundation for the AASB Standards that 'contribute to transparency by enhancing the international comparability and quality of financial information, enabling investors to make informed economic decisions' [4]

AASB standards are known as **Australian Accounting Standards** and include Australian equivalents to International Financial Reporting Standards (IFRS). The Australian Accounting Standards prescribe the accounting treatment.

The AASB **Framework for the Preparation and Presentation of Financial Statements (Framework)** 'sets out the concepts that underlie the preparation and presentation of financial statements for external users.'[5] The Framework provides guidance where there is no specific Accounting Standard applicable.

The Framework provides definitions for the elements of financial statements (assets, liabilities, equity, income and expenses), and further guidance in relation to the timing of recognition of expenditure.

- Paragraph 49 defines an **asset** as:

  'A resource controlled by the entity as a result of past events and from which future economic benefits are expected to flow to the entity.'
- Paragraph 70 (b) defines an **expense** as:

  'decreases in economic benefits during the accounting period in the form of outflows or depletions of assets or incurrences of liabilities that result in decreases in equity, other than those relating to distributions to equity participants.'

[4] Australian Accounting Standards Board – Conceptual Framework for Financial Reporting, 7 April 2022. AASB Status and Purpose of the Conceptual Framework, SP1.5 (a)

[5] Australian Accounting Standards Board – Framework for the Preparation and Presentation of Financial Statements – prepared on 29 October 2021, for application to annual reporting periods beginning on or after 1 July 2021.

- Paragraph 78 further defines **expenses** that:

  'encompass losses as well as those expenses that arise in the course of the ordinary activities of the entity. Expenses that arise in the course of the entity include, for example, cost of sales, wages and depreciation.'

The Framework also provides further guidance in relation to the timing of recognition for expenditure.

- Paragraph 94 states:

  'Expenses are recognised in the income statement when a decrease in future economic benefits related to a decrease in an asset or an increase of a liability has arisen that can be measured reliably.'

- Paragraph 95 states:

  'Expenses are recognised in the income statement on the basis of a direct association between the costs incurred and the earning of specific items of income. This process, commonly referred to as the matching of costs with revenues, involves the simultaneous or combined recognition of revenues and expenses that result directly and jointly from the same transactions or other events.'

- Paragraph 97 goes on to state:

  'An expense is recognised immediately in the income statement when an expenditure produces no further economic benefits or when, and to the extent that, future economic benefits do not qualify, or cease to qualify, for recognition in the balance sheet as an asset.'

AASB Standard 138 Intangible Assets[6] scope definitions provide the following guidance:

- Paragraph 4:

  'in determining whether an asset that incorporates both intangible and tangible elements should be treated under AASB 116 Property, Plant and Equipment or as an intangible asset under this standard, an entity uses judgement to assess which element is more significant. For example, computer software for a computer-controlled machine tool that cannot operate without that specific software is an integral part of the related hardware and it is treated as property, plant and equipment. The same applies to the operating system of a computer. When the software is not an integral part of the related hardware, computer software is treated as an intangible asset.'

- Further at Paragraph 8 – Fair Value is defined:

  'Fair value is the price that would be received to sell an asset or paid to transfer a liability in an orderly transaction between market participants at the measurement date. (See also AASB 13 Fair Value Measurement.)

The International Accounting Standards Board (IASB) through the IFRS Interpretations Committee (IFRSIC)[7] considered 'Climate-related and other Uncertainties in the Financial Statements' in their November 2023 meeting. This included discussion regarding:

a) *how entities reflect the potential for high variability in future cash flows over an extended time horizon when calculating the value in use of an asset; and*
b) *whether there is diversity in how entities understand and apply the requirements in International Accounting Standard (IAS) 36 Impairment of Assets in reflecting such variability in value in use calculations.*

The IASB resolved to consider this input at a future IASB meeting.

[6] Australian Accounting Standards Board (AASB) 138 – Intangible Assets – Compilation no. 5 31 December 2022.

[7] International Accounting Standards Board – IFRIC Update November 2023- Agenda Paper 3 – 'Climate-related and other Uncertainties in the Financial Statements'

SA Power Networks Cost Allocation Method (1 July 2020)[8] provide additional guidance regarding regulatory accounting and reporting adopted.

- Clause 6.15.4 of the National Electricity Rules (NER) require that:

  a) Each *Distribution Network Service Provider* (DSNP) must submit to the Australian Energy Regulator (AER) for its approval, a document setting out its proposed *Cost Allocation Method*.

  b) The *Cost Allocation Method* proposed by a DNSP must give effect to and be consistent with the *Cost Allocation Guideline* (CAG), each SA Power Networks'.

  SA Power Networks has a duty to comply with the approved Cost Allocation Method under clause 6.15 of the NER, which states at 6.15.1:

  "A DNSP must comply with the Cost allocation Method that has been approved in respect of that provider from time to time by the AER under this rule 6.15."

SA Power Networks Cost Allocation Method currently categorises Information Technology operating expenditure as Corporate costs that are allocated to standard control services, alternative control services, negotiated distribution services, unregulated distribution services or non-distribution services (refer Table 3 - Pg. 20). Information Technology capital expenditure is categorised as **Standard Control Capex** (Refer Table 2 - Pg. 12). Proposed changes from Capex to Opex for the 2025-30 RCP fall within the existing SA Power Network Cost Allocation Method classifications, and therefore do not require any change.

[8] SA Power Networks – Cost Allocation Method – Version 5 Updated 1 July 2020.

Appendix 2 - Detailed Findings

Detailed below are our findings and observations from the procedures that we performed.

1	Recurrent Cyber Business Case - Operations, Digital Identity, Cyber Risk and IT Resilience, Operational Technology.

Description of activities (as provided by SA Power Networks):

SA Power Networks proposes the existing Capex costs related to Operations, Digital Identity, Cyber Risk and IT Resilience ($13.5m) in the 2020-25 Regulatory Control Period (RCP) are reclassified to Operating Expenses (Opex) in the 2025-30 Regulatory Control Period.

SA Power Networks proposes expenditure of approximately $15.3m over the next 5-year Regulatory Control Period 2025-30.

Operational Technology costs of $4.1m in the 2020-25 Regulatory Control Period are currently classified as Capex. Outlays of $3.1m proposed for 2025-30 will remain classified as Capex.

We understand these outlays include:

Operations:

Providing SA Power Networks with an in-depth understanding of our cyber threats, and then supporting this with proactive threat management and enhanced response and recovery strategies. The core activities that are involved in this are:

- Security logging, monitoring and detection. Logging is the collection of the technical data automatically produced by information/digital assets (e.g., IT, OT and SCADA assets) that identifies the asset's low-level processes, tasks, actions and changes. Logging is the foundation that cyber security monitoring is built on. Monitoring is the activity that collects and analyses technical security data (such as logs) and presents it in a meaningful way to facilitate detection. Detection is the activity that correlates, analyses, contextualises, evaluates, identifies, alerts and escalates security information in response to detected cyber security occurrences, events and incidents.

Findings:

1) Having assessed the underlying objective and outcomes from these activities, BDO considers it is reasonable for this expenditure to be treated as Opex from 2025.

2) The basis of this opinion is the alignment with recognized Accounting Standard treatments.

3) Internal Accounting policies (SA Power Networks Cost Allocation Method) include Standard Control Opex costs for Information Technology, and therefore do not require any change to classification.

SA Power Networks propose $15.3m of Operations, Digital identity, and Cyber Risk and IT Resilience outlays to be expensed (Opex) over the next Regulatory Control Period, 2025-30.

Operating expenses are costs associated with running the day-to-day operations of a business, and they are incurred in the process of generating revenue.

This is supported / underpinned by the AASB 'Framework' (at para 97) 'an expense is recognised immediately in the income statement when an expenditure produces no future economic benefits or when, and to the extent that, future economic benefits do not qualify, or cease to qualify, for recognition in the balance sheet as an asset.' The expenses described by SA Power Networks are of an ongoing operational nature and are therefore, also operating expenditure. Whilst these outlays may also qualify as an Asset (as defined at para 53) in that 'the future economic benefit embodied in an asset is the potential to contribute, directly or indirectly, to the flow of cash or cash equivalents of the entity,' it is questionable whether these outlays materially add to the value of existing assets by extending their life or increasing their capacity. It is also guided by the personal judgement of SA Power Networks as preparers of the financial reports.

Asset classification / Capex is defined in the Framework (Para 49) as 'A resource controlled by the entity as a result of past events and from which future economic

1	Recurrent Cyber Business Case – Operations, Digital Identity, Cyber Risk and IT Resilience, Operational Technology.	
	• Incident response. Containing, mitigating, and remediating cyber security incidents in collaboration with internal stakeholders. • Vulnerability management. This is the proactive identification, assessment, prioritisation, remediation, and ongoing monitoring of cyber security vulnerabilities. This activity helps us understand our weaknesses and plan mitigation activities accordingly. • Threat intelligence and threat hunting. Threat intelligence is the activity of collecting, processing and analysing data to understand a threat actor's motives, targets and attack behaviours. Threat intelligence enables us to make faster, more-informed, data-backed security decisions. Threat hunting is a proactive activity that seeks out threat patterns that are not usually identified by cyber security technologies. This approach allows us to detect and mitigate cyber threats before they can cause disruption to our assets. **Digital Identity:** Management of the complete identity lifecycle of employees and devices across all SA Power Network platforms. Core activities include the following: • Internal and external platform enhancement – developing and enhancing all SA Power Network current digital repositories located internally and in SaaS solutions. • Risk Reduction – continued and increased risk-reduction controls to multi-factor authentication, conditional access policy, risky users and password policies. • Role based access – maintaining secure role-based access control mechanism and providing a framework for requestable and automatic role deployment, as well as supporting precise access for each individual. • Identify lifecycle monitoring – monitoring and protecting digital identities, including continuing to develop access and provisioning, and ensuring lifecycle management of user identity cube and subordinate accounts. Aim is to build fluid and frictionless fit for purpose access as the user account changes over time.	benefits are expected to flow to the entity.' An expense (Opex) is defined (para 70(b)) as 'decreases in economic benefits during the accounting period in the form of outflows or depletions of assets or incurrences of liabilities that result in decreases in equity, other than those relating to distributions to equity participants.' Further Para 78 defines expenses that 'encompass losses as well as those expenses that arise in the course of the ordinary activities of the entity. Expenses that arise in the course of the entity include, for example, cost of sales, wages and depreciation.' Para 97 goes on to state 'An expense is recognised immediately in the income statement when an expenditure produces no further economic benefits or when, and to the extent that, future economic benefits do not qualify, or cease to qualify, for recognition in the balance sheet as an asset.' Recurrent Cyber outlays include 'Operations' (security logging, monitoring and detection, incident response, vulnerability management, and threat intelligence and threat hunting), 'Digital Identity' (secure management of employee identity and devices lifecycle), 'Cyber Risk and IT Resilience' (documenting, mitigating and overseeing cyber security risk). These activities are performed across all SA Power Network platforms and are costs associated with running the day-to-day operations of a business, and they are incurred in the process of generating revenue. The definition criteria for intangible assets require that the asset is identifiable, that is, it can be separately sold, rented or exchanged, either individually or together with related assets or liabilities, or arises from contractual or other legal rights, and provides future economic benefits controlled by the entity. The AASB Framework and Policies therefore support the treatment of these costs as Opex. BDO believe that the costs associated with Operations, Digital identity, and Cyber Risk and IT Resilience as described by SA Power Networks are of an ongoing operational nature and are therefore, also operating expenditure. We suggest the forecast expenditure by SA Power Networks as part of undertaking all of these activities and programs in the next Regulatory Control Period as described to BDO, meets the definition of an expense as provided in paragraph 69(b) of the Framework for the Preparation and Presentation of Financial Statements ("the Framework").

1 Recurrent Cyber Business Case - Operations, Digital Identity, Cyber Risk and IT Resilience, Operational Technology.	
• User Experience (UX) collaboration – increase useability and user experience of the identity management system. Deliver efficiencies through user self-service. **Cyber Risk and IT Resilience:** Documenting, mitigating and overseeing cyber security risk, including: • managing the cyber security architectural resources for business projects • overseeing the IT Resilience function • providing a security awareness program.	
2 Cyber Uplift Business Case	
Description of activities (as provided by SA Power Networks): Cyber Uplift Capabilities including the following: Role based access, Application control, Zero trust architecture, Security Operations (SECOPS), IT resiliency lifecycle, Secure software development lifecycle, Third-party security, Operational Technology, Information protection, Tools of trade devices, BYOD cyber strategy, Network detection and response (NDR), Cyber awareness, MyID, Other Australian Energy Sector Cyber Security Framework (AESCSF) principles. $44.7m over the next Regulatory Control Period, 2025-30, comprised of $26.2m Non-Recurrent Opex, $15.9m Recurrent Opex and $2.6m Non-Recurrent Capex. No additional operational technology hardware outlays will be incurred.	**Findings:** **SA Power Networks** propose $44.7m of new costs related to mitigating cyber security risk across a range of areas. The 2025-30 Regulatory Control Period outlays comprise Non-Recurrent outlays of $28.2m labour, and $0.6m software, and Recurrent outlays of $2.7m labour and $13.3m software. The difference between the non-recurrent (once-off) and the Recurrent components ($15.9m) of the outlays in the Cyber Uplift business case is that the Non-Recurrent components ($28.8m) are typically developing the process capability to a level of maturity. Thereafter it becomes a recurrent outlay to maintain that maturity / capability moving forward. **Recurrent outlays** Cyber security expenses are typically considered to be an operating expense rather than a liability or an asset on an accounting sheet. Operating expenses are costs associated with running the day-to-day operations of a business, and they are incurred in the process of generating revenue. These expenses are usually listed on the income statement and are deducted from the company's revenue to calculate its net income. Liabilities and assets, on the other hand, represent the financial obligations and resources of a company, respectively. While cyber security investments may indirectly protect the value of a company's assets and reduce the risk of certain liabilities, the expenses themselves are generally categorized as operating expenses. Hardware purchased, however is normally classified as an asset (Capex) i.e. a firewall device. The cost of running a cyber security team / IT professionals would normally be classified as an

operational expense (Opex). In accordance with the AASB's *Framework for the Preparation and Presentation of Financial Statements*, BDO considers this outlay does not meet the future economic benefit requirement to be classified as an asset, and that the expenditure meets the definition of an expense and that it should be recognised as operating expenditure at the time incurred. These outlays are considered as Opex. Software costs can be capitalised if they are considered an asset.

BDO believe that the costs associated with the additional recurrent Cyber Security outlays are of an ongoing operational nature and are therefore operating expenditure. This is supported / underpinned by the AASB 'Framework' in that the activities do not materially add to the value of existing assets by extending their life or increasing their capacity, but rather this expenditure should be classified as operating expenditure.

Non-recurrent outlays

The process of deciding when to capitalise software or expense as it is incurred involves the GAAP (USA) IFRS (Aus) guidelines and the personal judgments of business leaders. Typically, capitalisation begins after the preliminary stage of software development when there's a sure source of funding for the project and a strong likelihood that the project could occur. It ends after the testing and completion of a software project. Consideration is required as to whether the once-off outlays meet the definition of an asset and, or materially extend the useful life of existing assets in a measurable way.

The definition of an expense as provided in paragraph 69(b) of the AASB Framework for the Preparation and Presentation of Financial Statements therefore supports the treatment of these non-recurrent costs as Opex. The basis of this opinion is the operational nature of this activity and that it is not materially extending the useful life or increasing the capacity of SA Power Networks in a measurable way.

Non-Recurrent outlays of $2.6m relating to predominantly integration components of SaaS are classified as Capex in accordance with the Framework guidance.

Consideration is required as to whether the once-off outlays meet the definition of an asset and, or materially extend the useful life of existing assets in a measurable way.

2 Cyber Uplift Business Case	
	Having assessed the underlying objective and outcomes from these activities, with the exception of the $2.6m relating to predominantly integration components of SaaS, which are classified as Capex, BDO considers it is reasonable for the non-recurrent expenditure outlays to be treated as Opex from 2025.

[1] All figures in this document are in real June 2022 dollars.

Disclaimer

This publication has been carefully prepared but is general commentary only. This publication is not legal or financial advice and should not be relied upon as such. The information in this publication is subject to change at any time and therefore we give no assurance or warranty that the information is current when read. The publication cannot be relied upon to cover any specific situation and you should not act, or refrain from acting, upon the information contained therein without obtaining specific professional advice. Please contact the BDO member firms in Australia to discuss these matters in the context of your particular circumstances.

BDO Australia Ltd and each BDO member firm in Australia, their partners and/or directors, employees and agents do not give any warranty as to the accuracy, reliability or completeness of information contained in this publication nor do they accept or assume any liability or duty of care for any loss arising from any action taken or not taken by anyone in reliance on the information in this publication or for any decision based on it, except in so far as any liability under statute cannot be excluded.

BDO Services Pty Ltd ABN 45 134 242 434 is a member of a national association of independent entities which are all members of BDO Australia Ltd ABN 77 050 110 275, an Australian company limited by guarantee. BDO Services Pty Ltd and BDO Australia Ltd are members of BDO International Ltd, a UK company limited by guarantee, and form part of the international BDO network of independent member firms. Liability limited by a scheme approved under Professional Standards Legislation.

BDO is the brand name for the BDO network and for each of the BDO member firms.

1300 138 991

www.bdo.com.au

AUDIT • TAX • ADVISORY

NEW SOUTH WALES
NORTHERN TERRITORY
QUEENSLAND
SOUTH AUSTRALIA
TASMANIA
VICTORIA
WESTERN AUSTRALIA