

EMC^a

energy market consulting associates

SAPN 2025/26 to 2029/30 Regulatory Proposals

REVIEW OF CYBER SECURITY AND ADMS EXPENDITURE FORECAST

Public Version



Report prepared for:
**AUSTRALIAN ENERGY
REGULATOR**
August 2024

Preface

This report has been prepared to assist the Australian Energy Regulator (AER) with its determination of the appropriate revenues to be allowed for the prescribed distribution services of SAPN from 1st July 2025 to 30th June 2030. The AER's determination is conducted in accordance with its responsibilities under the National Electricity Rules (NER).


This report covers a particular and limited scope as defined by the AER and should not be read as a comprehensive assessment of proposed expenditure that has been conducted making use of all available assessment methods nor all available inputs to the regulatory determination process. This report relies on information provided to EMCa by SAPN. EMCa disclaims liability for any errors or omissions, for the validity of information provided to EMCa by other parties, for the use of any information in this report by any party other than the AER and for the use of this report for any purpose other than the intended purpose. In particular, this report is not intended to be used to support business cases or business investment decisions nor is this report intended to be read as an interpretation of the application of the NER or other legal instruments.

EMCa's opinions in this report include considerations of materiality to the requirements of the AER and opinions stated or inferred in this report should be read in relation to this overarching purpose.

Except where specifically noted, this report was prepared based on information provided to us prior to 21st June 2024 and any information provided subsequent to this time may not have been taken into account. Some numbers in this report may differ from those shown in SA Power Network's regulatory submission or other documents due to rounding.

Enquiries about this report should be directed to:

Paul Sell

Managing Director


Prepared by

Mark de Laeter with input from Cesare Tizi, Scott Wallance and Paul Sell

Date saved

12/09/2024 2:41 PM

Version

Final v1

Energy Market Consulting associates

ABN 75 102 418 020

Sydney Office

L25, 100 Mount Street, North Sydney NSW 2060
PO Box 592, North Sydney NSW 2059
contact@emca.com.au
www.emca.com.au

Perth Office

contact@emca.com.au
www.emca.com.au

TABLE OF CONTENTS

ABBREVIATIONS	III
EXECUTIVE SUMMARY	IV
1 INTRODUCTION	1
1.1 Purpose of this report.....	1
1.2 Scope of requested work.....	1
1.3 Our review approach	1
1.4 This report.....	2
2 RELEVANT CONTEXT TO OUR ASSESSMENT – CYBER SECURITY	4
2.1 Cyber security threat in Australia	4
2.2 Critical infrastructure regulation	4
2.3 The Australian Energy Sector Cyber Security Framework (AESCFS)	6
2.4 AER Guidelines for non-network ICT assessment.....	8
2.5 Implications for our assessment.....	9
3 SA POWER NETWORK’S PROPOSED CYBER SECURITY EXPENDITURE	11
3.1 Overview and summary of proposed expenditure.....	11
3.2 Summary of the basis for SAPN’ proposed expenditure	12
3.3 Our Assessment	13
4 ADVANCED DISTRIBUTION MANAGEMENT SYSTEM (ADMS) UPGRADE	26
4.1 Overview	26
4.2 Assessment	27

LIST OF TABLES

Table 2.1: AESCSF Version 1 and Version 2 comparison – Security Profiles	7
Table 3.1: SAPN proposed ICT cyber security related expenditures (\$m, FY25).....	11
Table 3.2: EMCa sensitivity analysis of likelihood and impact on consequence.....	24
Table 4.1: SAPN’s proposed expenditure profile for the ADMS Upgrade (\$m FY25).....	26

LIST OF FIGURES

Figure 1.1: Scope of work covered by this report.....	1
Figure 2.1: AESCSF E-CAT criticality bands for electricity sector – DNSPs highlighted.....	7
Figure 3.1: SAPN cyber incidents over the last four years.....	12

Figure 3.2: SAPN’s historical and proposed cyber security expenditure (\$m FY22)..... 13

Figure 3.3: SAPN’s projected achievement of AESCSF V2 controls by the end of the current RCP 14

Figure 3.4: SAPN options considered in its Cyber Security Refresh (\$m, real 2022)..... 16

Figure 3.5: Recurrent cyber security investment trend over time (\$m, 2022)..... 17

Figure 3.6: SAPN’s options for cyber security uplift program - \$million real 2022 18

Figure 3.7: SAPN’s extrapolation of total number of incidents per month 20

Figure 3.8: Assumed P2, P3, P4 incident severity ratios..... 20

Figure 3.9: SAPN - reduction of breach severity over 2021-2023 due to increased cyber resilience 21

Figure 3.10: Benefits derivation for P1 operational network loss, \$million real 2022..... 22

Figure 3.11: Benefits derivation for P1 major IT system loss, \$million real 2022 23

Figure 3.12: Benefits derivation from avoided cost of P1 Major Data Loss 23

ABBREVIATIONS

ADMS	Advanced Distribution Management System
AESCSF	Australian Energy Sector Cyber Security Framework
AER	Australian Energy Regulator
ASCS	Australian Cyber Security Centre
ASD	Australian Signals Directorate
BC	Business case
CIRMP	Critical Infrastructure Risk Management Plan
Current RCP	2020-2025 regulatory control period
DNSP	Distribution network service provider
E-CAT	Electricity sector criticality assessment tool
ECSO	Enhanced cyber security obligations
EEMM	Essential eight maturity model
IFRS	International Financial Reporting Standards
IT	Information technology
MIL	Maturity Indicator Level
NER	National Electricity Rules
Next RCP	2025-30 regulatory control period
NSP	Network service provider
OT	Operational technology
P1, P2, P3, P4	Severity ratings with P1 being the highest (i.e. Priority 1)
RP	Regulatory proposal
RRP	Revised regulatory proposal
SAPN	South Australia Power Networks
SLACIP Act	Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
SP	Security Profile
SoCI Act	Security of Critical Infrastructure Act 2018
SoNS	System of National Significance

EXECUTIVE SUMMARY

Introduction and context

1. The AER has engaged EMCa to undertake a technical review of aspects of the expenditure that SA Power Networks (SAPN) has proposed in its regulatory proposal (RP) for 2025-30 Regulatory Control Period (next RCP). The scope of our review, covered by this report, comprises proposed projects to mitigate cyber security risks and the Advanced Distribution Management System (ADMS) upgrade.
2. The assessment contained in this report is intended to assist the AER in its own analysis of the proposed capex allowance as an input to its draft determination on SAPN's revenue requirements for the next RCP.

Our assessment

Cyber security program

SAPN proposes a significant uplift in cyber security expenditure for the next RCP

3. SAPN proposes \$71.4 million cyber security expenditure for the next RCP in two programs:
 - A cyber security 'refresh' program ('operationalising cyber security step change'), which is essentially based on maintaining throughout the next RCP the cyber security operations capability it expects to achieve by the end of the current RCP, and
 - An 'uplift' program which is based on adding depth and breadth of controls to offset the risk of cyber security breach from an expected increased cyber security threat landscape and SAPN's increasing attack surface area.
4. This proposed expenditure comprises \$6.4 million capex and an opex step change of \$65.0 million.

SAPN presents a compelling case for increased investment to offset the escalating cyber security threat landscape

5. SAPN has identified its regulatory compliance obligations and has presented its analysis of the current and future threat landscape, referencing available literature and from information on its own escalating cyber security attack threat events. The external analysis draws on recognised industry sources, including the Australian Signal Directorate's Cyber Threat Report 2023, which points to a relentless increase in cyber threats from increasingly sophisticated actors.
6. SAPN's internal analysis shows the effectiveness of its cyber security investments in the 2020-25 RCP (current RCP) in mitigating the severity of the attacks, but also shows the rapidly increasing frequency of low-level severity attacks. SAPN also highlights that as a critical infrastructure operator with a broad operational cyber-attack surface, it is a prime target for threat actors.


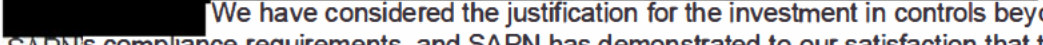
SAPN's strategy to manage cyber security risk escalation is to take a risk-based approach

7. Whilst it references the latest version of the Australian Energy Sector Cyber Security Framework (AESCSF), SAPN does not target a particular Security Profile (SP) under that framework. Rather, SAPN proposes to continue to meet its existing cyber security obligations through its 'refresh' program and to take a risk-based approach to mitigating the increasing cyber threat through its 'uplift' program.

SAPN's cyber security Refresh project is based on managing risks with fit-for-purpose controls

8. SAPN has compliance obligations arising from amendments to the Security of Critical Infrastructure Act 2018 (SOCIA Act) and the Privacy Act which it will more than satisfy by the end of the current RCP.
9. It is reasonable for SAPN to continue to incur its expected FY25 level of annual capex and opex over the course of the next RCP in order to maintain the underlying capability it has established. We consider that the proposed cyber security 'Refresh' capex and opex step change are likely to satisfy the National Electricity Rules (NER) expenditure criteria.
10. SAPN has adopted the International Financial Reporting Standards (IFRS) accounting treatment for the next RCP, which has led to the majority of expenditure for the refresh program being classified as (recurrent) opex, and which therefore requires an opex step change.

SAPN's cyber security Uplift project is based on managing increasing cyber risks with fit-for-purpose controls

11. 
 We have considered the justification for the investment in controls beyond SAPN's compliance requirements, and SAPN has demonstrated to our satisfaction that the proposed additional controls are warranted and represent a prudent approach to mitigate increasing cyber security risk.
12. SAPN's approach of creating a risk register, identification of gaps and controls to manage the exposures throughout the course of the next RCP, and costing the controls via a combination of vendor input and external advice to supplement its in-house expertise is a sound approach.

SAPN has selected a prudent option and the cost is reasonably derived

13. SAPN provided sufficient detail to support its proposed option, including the proposed breadth and depth of controls.
14. Whilst we consider that the avoided risk-cost benefits are likely to be significantly lower than SAPN has derived, due to what we view as overly pessimistic assumptions regarding the frequency of severe cyber security breaches in the next RCP, the net benefit is still likely to be positive.
15. SAPN's selected option is slightly less expensive than full achievement of the AESCSF V2 SP-3 practices and demonstrates a prudent outcome from the risk-cost approach that SAPN has taken.
16. We conclude that SAPN's proposed 'Uplift' capex and opex step change are likely to satisfy the NER expenditure criteria.

Proposed Advanced Distribution Management System Upgrade

SAPN's proposed ADMS upgrade is primarily driven by technical obsolescence

17. SAPN proposes \$32.4 million capex on upgrading its ADMS because the underlying operating and other systems which the ADMS needs will become unsupported from 2027. The current version of the ADMS will not operate on the upgraded operating system.
18. ADMS is a common operating system in the industry and is a critical operating system for DNSPs. It is essential for monitoring and managing the distribution network to help ensure operational security and reliability.

Upgrading the ADMS will provide improved cyber security resilience

19. SAPN has also identified that upgrading the ADMS will maintain secure operating environments and effective interfaces between the key operational components.
20. There is substantial evidence that critical infrastructure such as SAPN's distribution network are targets for cyber threat actors. The proposed ADMS upgrade will incorporate the latest available cyber security defences. The upgrade proposed will therefore bring an unquantified but substantial benefit to SAPN's cyber security resilience.

SAPN has selected a prudent option and its proposed cost is reasonably derived

21. SAPN provided sufficient detail to support its proposed option, with the least cost technically viable option selected.
22. The cost estimate is based on vendor advice combined with SAPN's relatively recent experience in installing its current version of the ADMS in the current regulatory control period. We consider the cost estimate has been reasonably derived.

Implications of our findings

23. SAPN proposes \$6.4 million capex plus \$65.0 million opex step changes for cyber security, and \$32.4 million capex for the ADMS upgrade. We consider that SAPN's proposed expenditure is reasonable.

1 INTRODUCTION

The AER has asked us to review and provide advice on SA Power Network's (SAPN) proposed allowances over the 2025-30 Regulatory Control Period (next RCP) relating to cyber security and the Advanced Distribution Management System (ADMS) upgrade. Our review is based on information that SAPN provided and on aspects of the National Electricity Rules (NER) relevant to assessment of expenditure allowances.

1.1 Purpose of this report

24. The purpose of this report is to provide the AER with a technical review of aspects of the expenditure that SAPN has proposed in its regulatory proposal (RP) for the next RCP.
25. The assessment contained in this report is intended to assist the AER in its own analysis of the proposed capex and opex allowances as an input to its draft determination on SAPN's revenue requirements for the next RCP.

1.2 Scope of requested work

26. Our scope of work, covered by this report, is as defined by the AER. Relevant aspects of this are as summarised in Figure 1.1.

Figure 1.1: Scope of work covered by this report



1.3 Our review approach

1.3.1 Approach overview

27. In conducting this review, we first reviewed the regulatory proposal (RP) documents that SAPN has submitted to the AER. This includes a range of appendices and attachments to SAPN's RP and certain Excel models which are relevant to our scope.

28. We next collated some information requests. The AER combined these with information request topics from its own review and sent these to SAPN.
29. In conjunction with AER staff, our review team met with SAPN at its offices on 23-24 May 2024. SAPN presented to our team on the scoped topics and we had the opportunity to engage with SAPN to consolidate our understanding of its proposal.
30. SAPN provided the AER with responses to information requests and, where these added relevant information, these responses are referenced within this review.
31. We have subjected the findings presented in this report to our peer review and Quality Assurance (QA) processes and we presented summaries of our findings to the AER prior to finalising this report.
32. The limited nature of our review does not extend to advising on all options and alternatives that may be reasonably considered by SAPN, or on all parts of the proposed forecast. We have included additional observations in some areas that we trust may assist the AER with its own assessment.

1.3.2 Technical review

33. Our assessments comprise a technical review. While we are aware of stakeholder inputs on aspects of what SAPN has proposed, our technical assessment framework is based on engineering / technical considerations and economics.
34. We have sought to assess SAPN's expenditure proposal based on SAPN's analysis and SAPN's own assessment of technical requirements and economics and the analysis that it has provided to support its proposal. Our findings are therefore based on this supporting information and, to the extent that SAPN may subsequently provide additional information or a varied proposal, our assessment may differ from the findings presented in the current report.
35. We have been provided with a range of reports, internal documents, responses to information requests and modelling in support of what SAPN has proposed, and our assessment takes account of this range of information provided. To the extent that we found discrepancies in this information, our default position is to revert to SAPN's regulatory submission documents as provided on its submission date, as the 'source of record' in respect of what we have assessed.

1.4 This report

1.4.1 Report structure

36. The scope of our assessment includes cyber security ex ante capex and opex and ADMS capex and is categorised as non-network ICT.
37. We have presented:
 - an overview of the proposed expenditure and a summary of SAPN's justification for that expenditure;
 - our assessment of the three projects (cyber security 'refresh', cyber security 'Uplift' and ADMS); and
 - our findings for the cyber security expenditure and the ADMS and the implications of these findings for the expenditure allowances determined by the AER in its draft regulatory determination.
38. We have taken as read the material and analysis that SAPN provided, and we have not sought to replicate this in our report except where we consider it to be directly relevant to our findings.

1.4.2 Information sources

39. We have examined relevant documents that SAPN has published and/or provided to the AER in support of the areas of focus and projects that the AER has designated for review. This included further information at onsite meetings and further documents in response to our information requests. These documents are referenced directly where they are relevant to our findings.
40. Except where specifically noted, this report was prepared based on information provided by AER staff prior to 21 June 2024 and any information provided subsequent to this time may not have been taken into account.
41. Unless otherwise stated, documents that we reference in this report are SAPN documents comprising its RP and including the various appendices and annexures to that proposal.
42. We also reference information responses, using the format IRXX being the reference numbering applied by the AER. Noting the wider scope of the AER's determination, the AER has provided us with IR documents that it considered to be relevant to our review.

1.4.3 Presentation of expenditure amounts

43. Expenditure is presented in this report in \$FY25 real terms, unless stated otherwise. In some cases, we have converted to this basis from information provided by SAPN in other terms.
44. While we have endeavoured to reconcile expenditure amounts presented in this report to source information, in some cases there may be discrepancies in source information provided to us and minor differences due to rounding. Any such discrepancies do not affect our findings.

2 RELEVANT CONTEXT TO OUR ASSESSMENT – CYBER SECURITY

We have conducted our review of SAPN's cyber security and ADMS projects in the context of increasing cyber security threats and a typically increasing threat surface, taking account of relevant regulatory compliance obligations and industry frameworks for assessing cyber risk criticality and risk mitigation maturity.

2.1 Cyber security threat in Australia

Increasing threat level is reported by the ACSC

45. The Australian Cyber Security Centre ('ACSC') monitors Australia's cyber threat landscape and among other things publishes an annual Cyber Threat Report. In its latest report (2022-23) it states that: *'The ACSC responded to over 1,100 cyber security incidents from Australian entities. Separately, nearly 94,000 reports were made to law enforcement through ReportCyber – around one every six minutes.'*¹

There is an increasing cyber threat against critical infrastructure

State actors are focussed on critical infrastructure worldwide

46. The Australian Signals Directorate (ASD) states:

*Globally, government and critical infrastructure networks were targeted by state cyber actors as part of ongoing information-gathering campaigns or disruption activities...Cyber operations are increasingly the preferred vector for state actors to conduct espionage and foreign interference.*²

47. In September 2022 and May 2023, the ASD and its international partners published advisory notices which strongly encouraged Australian entities to review their networks for signs of malicious activity.

Australian critical infrastructure has been targeted

48.

[REDACTED]

49. The 2023 Cyber Threat Report, notes that critical infrastructure can be targeted by the mass scanning of networks for old and new vulnerabilities, citing the example of an Italian energy and water provider that was affected by ransomware.

2.2 Critical infrastructure regulation

2.2.1 Amendments to the SOCI Act

50. The Security of Critical Infrastructure Act 2018 (SOCI Act) places obligations on specific entities in the electricity industry.

¹ ASD Cyber Threat Report 2022-23. Executive Summary.

² ASD Cyber Threat Report 2022-23. Executive Summary.

³ ASD Cyber Threat Report 2022-23. Executive Summary.

51. The Security Legislation Amendment (Critical Infrastructure) Act 2021 (SLACI Act) amended the SOCI Act to strengthen the security and resilience of critical infrastructure by expanding the sectors and asset classes the SOCI Act applies to, and to introduce new obligations.
52. The amendments were made to respond to *'the deteriorating threat environment related to cyber attacks'*.⁴ Electricity assets can be classed as critical infrastructure within the framework under the SoCI Act. The new 'Positive Security Obligations' that apply to certain sets of critical infrastructure assets are:
 - Register of Critical Infrastructure Assets: which requires reporting entities, who are either direct interest holders or the responsible entity of critical infrastructure assets, to provide to Government ownership, operational, interest and control information
 - Mandatory Cyber Incident Reporting: responsible entities for critical infrastructure assets are required to report critical and other cyber security incidents to the Australian Cyber Security Centre's online cyber incident reporting portal.
53. On 2 April 2022, additional amendments to the SOCI Act introduced the following:
 - A new obligation for responsible entities to create and maintain a critical infrastructure risk management program (CIRMP) with the obligation commencing on 17 February 2023⁵

• [REDACTED]

54. The CIRMP is a written program which requires a responsible entity for a critical infrastructure asset to (i) identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset, and so far as it is reasonably practicable to do so, (ii) minimise or eliminate any material risk of such a hazard occurring, and (iii) mitigate the relevant impact of such a hazard on the asset.⁷

55. [REDACTED]

2.2.2 CIRMP - AESCSF Security Profile 1 and Essential Eight Maturity Model

56. Under the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2023, a responsible entity must establish and maintain a process or system in the CIRMP to (a) comply with a framework contained in one of five documents referred to in the CIRMP, and (b) meet the corresponding condition for that document.⁹ The CIRMP must be in place within 18 months of the commencement of the instrument or within 18 months of the asset being designated a critical (electricity) infrastructure asset.¹⁰

⁴ [REDACTED]

⁶ [REDACTED]

⁷ Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 – explanatory statement.

⁸ [REDACTED]

⁹ Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023; subsection 8 (4).

¹⁰ Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023; subsection 4(2) and subsection 8(3).

57. The 2020-21 AESCSF Framework Core published by AEMO is one of the five documents referred to in the CIRMP instrument and the condition that is required to be met is SP-1. Therefore SP-1 is the legislative obligation that Network Service Providers (NSPs) must comply with if the NSP is defined as a responsible entity and selects the AESCSF as the cyber security framework.
58. Equally, the *Essential Eight Maturity Model* (EEMM) published by the Australian Signals Directorate is another referenced framework and the condition if it is adopted by an NSP is meeting Maturity Indicator Level one (MIL-1). Therefore MIL-1 is the legislative obligation to which NSPs must comply with if the NSP is defined as a responsible entity and the NSP selects the EEMM as its cyber security framework.

2.2.3 Privacy Act amendments 2022¹¹

59. The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 (the Bill) amends the Privacy Act 1988 to expand the Australian Information Commissioner's enforcement and information sharing powers, and to increase penalties for serious or repeated interferences with privacy.
60. The Bill increases the maximum penalty under section 13G of the Privacy Act for a body corporate to an amount not exceeding the greater of \$50 million, three times the value of the benefit obtained or, if the court cannot determine the value of the benefit, 30% of their adjusted turnover in the relevant period. The maximum penalty of \$50 million is an increase from the pre-existing maximum of \$2.2 million.
61. Within the Explanatory Memorandum to the Bill, it is stated that '[b]y strengthening penalties, Australia will be signalling its expectations that businesses undertake robust privacy and security practices.'¹²

2.3 The Australian Energy Sector Cyber Security Framework (AESCSF)

2.3.1 AESCSF V1

62. In response to the Finkel National Electricity Market Review recommendation 2.10 in 2018, the Australian Energy Market Operator (AEMO) collaborated with industry and government to develop the AESCSF. Among other markets, it covers Australia's electricity sector and is voluntary but has been adopted by NSPs.¹³ The AESCSF Version 1 (V1) is divided into 11 domains, ten C2M2¹⁴ domains, and the Australian Privacy Management Domain. There were minor revisions to the AESCSF in 2019, 2021, and 2022, with no significant changes in version 2022 compared to version 2021.¹⁵ AESCSF V1 encompasses the 2018 and subsequent iterations up to and including the 2022 revision.
63. The AESCSF V1 program includes the Electricity Criticality Assessment Tool (E-CAT), which is designed to assess the relative criticality of NSPs and other participants in the electricity sector.
64. The E-CAT allows assessment of the relative criticality of entities participating in the electricity and other energy sectors. The diagram below represents the criticality banding for the electricity sub-sector only, with DNSP criticality rating ranging between the High and Medium bands.

¹¹ https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r6940.

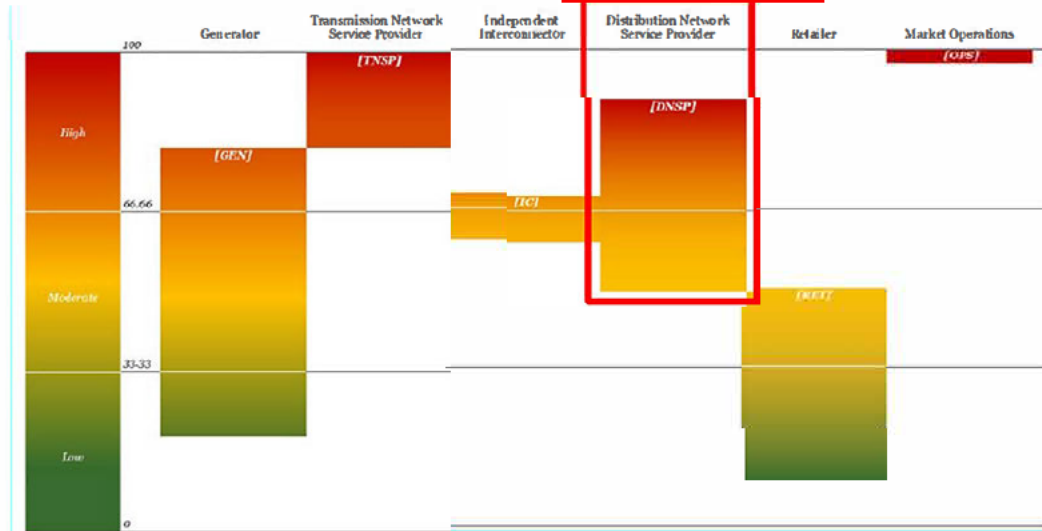
¹² Privacy Legislation Amendment (ENFORCEMENT and Other Measures) Bill 2022 EXPLANATORY MEMORANDUM, in reference to Section 13G – civil penalties (para 12).

¹³ AEMO, AESCSF Framework and Resources, AEMO website.

¹⁴ United States Department of Energy Cyber Security Capability Maturity Model.

¹⁵ AEMO AESCSF Framework Overview – 2022 Program. Page 1.

Figure 2.1: AESCSF E-CAT criticality bands for electricity sector – DNSPs highlighted



Source: AEMO, AESCSF Electricity Criticality Assessment Tool (E-CAT), per AESCSF V1

2.3.2 AESCSF Version 2 (V2)

- 65. In December 2022, Energy Ministers endorsed AESCSF V2, providing guidance about the continued role of the program to support energy sector cyber uplift and increasing cyber security requirements for the energy sector in line with escalating and evolving cyber threats.
- 66. The 2023 program intends to support AESCSF V2 assessment, AESCSF V1 (noting CIRMP minimum obligations), and a transition plan to ‘sunset’ AESCSF V1. AESCSF V2 was released in 2023. The update to AESCSF v2 has resulted in an additional 72 practices (i.e., 20% additional practices). A summary of the difference between AESCSF V1 and V2 is summarised in v2.1 and AESCSF v2 is provided in Table 2.1. AEMO has stated previously that ‘[t]he CAT should be treated as general guidance only. Results obtained from the CAT do not indicate that an entity has obligations under or is compliant with applicable Commonwealth (Cth) legislation.’¹⁶

Table 2.1: AESCSF Version 1 and Version 2 comparison – Security Profiles

Security Profile	Participant criticality	Total practices/anti-patterns required to achieve SP	
		AESCSF V1	AESCSF V2
SP-1	Low	88	123
SP-2	Medium	200 (88+112)	275 (123+152)
SP-3	High	282 (200+82)	354 (278+79)

Source: AEMO, AESCSF V2 Summary of Changes, page 4

- 67. To help organisations define roadmaps to improved cyber security maturity, the ACSC includes guidance on ‘Priority Practices’ within each SP. The Priority Practices are recommended for completion first as part of any uplift program.

¹⁶ AEMO AESCSF Framework Overview – 2022 Program. Page 3.

2.4 AER Guidelines for non-network ICT assessment

2.4.1 Assessment of non-network ICT capex

68. The scope of our assessment includes ex ante cyber security and ADMS capex, which are categorised as non-network ICT.
69. The AER's 2019 non-network ICT capex assessment approach guideline ('ICT assessment guideline') is relevant to SAPN's proposed cyber security capex. The proposed expenditure is also 'non-recurrent'.
70. The AER requires DNSPs to allocate their non-recurrent ICT expenditures into the three subcategories for which it applies different assessment approaches, as described below:¹⁷

Maintaining existing services, functionalities, capability and/or market benefits

71. The AER states that:

Given that these expenditures are related to maintaining existing service, we note that it will not always be the case that the investment will have a positive NPV. As such, it is reasonable to choose the least negative NPV option from a range of feasible options including the counterfactual.¹⁸ We consider that such investments should be justified on the basis of a business case, where the business case considers possible multiple timing and scope options of the investments (to demonstrate prudence) and options for alternative systems and service providers (to demonstrate efficiency). The assessment methodology would also give regard to the past expenditure in this subcategory.¹⁹

Complying with new / altered regulatory obligations / requirements

72. The AER states that:

It is likely that for such investments, the costs will exceed the measurable benefits and as such, the least cost option will likely be reasonably acceptable in regard to the NER expenditure criteria. Therefore the assessment of these expenditures is similar to subcategory one. Should there be options to achieve compliance through the use of external service providers [sic], the costs and merits of these should be compared.²⁰

New or expanded ICT capability, functions and services

73. The AER states that:

We consider that these expenditures require justification through demonstrating benefits exceed costs (positive NPV). We will make our assessment therefore through assessing the cost-benefit analysis. Where benefits exceed costs consideration should also be given to self-funding of the investment.

For each subcategory of non-recurrent expenditure, we note that there may be cases where the highest NPV option is not chosen. In these cases, where either the chosen option achieves benefits that are qualitative or intangible, we would expect evidence to support the qualitative assumptions. We consider the evidence provided must be commensurate with the cost difference between the chosen and highest NPV option.

¹⁷ In cases where programs/projects cover multiple categories of expenditure, the distributor is expected to apportion costs from individual components across multiple categories to reflect the nature of the work undertaken.

¹⁸ The only exception will be where the business can demonstrate that any unquantified/intangible benefits of an option can support the decision to not choose the highest NPV option.

¹⁹ AER, Non-network ICT capex assessment approach, November 2019. Page 11.

²⁰ AER, Non-network ICT capex assessment approach, November 2019. Page 11.

We also note that where non-recurrent projects either lead to or become recurrent expenditures in the future, this needs to be identified in the supporting business case and accounted for in any financial analysis undertaken to support the investment.²¹

2.4.2 Assessment of opex step changes

74. Our scope includes assessment of SAPN's proposed cyber security opex step changes. Section 2.2 of the AER's Expenditure Forecast Assessment Guideline for Electricity Distribution outlines its general approach for assessing opex step changes and which we have followed. In summary:
- The AER separately assesses the prudence and efficiency of forecast cost increases or decreases from new regulatory obligations and capex/opex trade-offs;
 - For capex/opex trade-off step changes, the emphasis is on establishing whether it is prudent and efficient to substitute opex for capex; and
 - For step changes arising from new regulatory obligations, the emphasis is on:
 - whether there is a binding change in regulatory obligations that affects the efficient forecast opex and when the change occurred, and
 - what options were considered and whether the selected option is an efficient option.²²

2.5 Implications for our assessment

Increasing threat landscape and attack surface mean cyber risk is increasing

75. The advice from government agencies is both that the cyber-attack landscape is worsening and that the cyber-attack surface presented by NSPs is increasing, leading to an increasingly higher risk of cyber-attack and potential breach.
76. In our assessment we have sought to understand how SAPN has incorporated the increasing threat landscape and attack surface issues into its risk analysis and, ultimately into its option selection and proposed expenditure profile.

Cyber security compliance obligations for NSPs are derived from the (amended) SOCI Act and from consideration of certain amendments to the Privacy Act

77. The minimum obligations for NSPs under the SOCI Act have been enhanced over the period FY22 and FY23 to include the following:
- Register of Critical Infrastructure Assets
 - Mandatory Cyber Incident Reporting
 - CIRMP, which requires completion of all the practices (and absence of anti-patterns) required to achieve SP-1 noting that SP-1 is the least onerous of the security profiles under the AESCSF.
78. [REDACTED]
79. Further the civil penalties for a breach(es) of the Privacy Act have been increased in 2022 from \$2.2 million to \$50.0 million (maximum) with the expectation from the Federal government via the amendment that organisations such as SAPN will act accordingly to undertake robust privacy and security practices which we interpret to include cyber security-related practices.

²¹ AER, Non-network ICT capex assessment approach, November 2019. Page 12.

²² AER, Expenditure Forecast Assessment Guideline for Electricity Distribution. Page 11.

80. We have assessed how SAPN has responded to its common and specific cyber security compliance obligations, cognisant of:
- the worsening threat landscape and attack surface issues; and
 - its expected cyber security compliance position at the end of the current RCP.
81. We have also considered whether SAPN has identified any other relevant obligations.
82. In addition to its minimum compliance obligations, we consider the controls SAPN has proposed (and the cost of them) to manage the increasing cyber security threat landscape. A useful reference is the SP practices expected to be in place by the end of the current RCP and the projected SP practices it is likely to achieve with the proposed investment by the end of the next RCP (if available).

3 SA POWER NETWORK’S PROPOSED CYBER SECURITY EXPENDITURE

SAPN has proposed a cyber security-related capex allowance of \$6.35 million and opex step changes totalling 65.0 million for the next RCP, being a total cost of \$71.35 million. This represents a significant uplift from the current RCP with the majority of the increase being for a proposed ‘uplift’ program with totex of \$50.65 million.

We consider that the proposed expenditure on maintaining its current cyber security practices and controls is a reasonable estimate of what is required throughout the next RCP. SAPN has classified the majority of its expenditure as opex and has sought a step change accordingly.

To develop its ‘uplift’ program, SAPN has taken a risk-based approach to developing its planned initiatives. This is an appropriate strategy in our view, and we consider that the proposed capex and opex step change for this program are reasonable.

We therefore consider that SAPN’s proposed cyber security capex and proposed opex step changes are likely to satisfy the NER’s expenditure criteria.

3.1 Overview and summary of proposed expenditure

3.1.1 What SAPN proposed in its RP

- 83. SAPN has proposed two cyber security programs for the next RCP, comprising a ‘refresh’ program and an ‘uplift’ program. The total proposed cyber security expenditure over the next RCP is \$71.35 million totex, a 130% increase from the expected totex in the current RCP.
- 84. The expenditure profile is shown in Table 3.1, and is comprised of two programs:
 - Refresh, and
 - Uplift.
- 85. SAPN has classified the bulk of its recurrent expenditure as opex and seeks a step change of \$17.4 million from its ‘Refresh’ program, together with \$3.35 million ongoing capex. SAPN proposes an additional \$47.6 million ongoing/recurrent opex from its ‘Uplift’ program as a step change, together with \$3.0 million capex.

Table 3.1: SAPN proposed ICT cyber security related expenditures (\$m, FY25)

Description	2025	2026	2027	2028	2029	Total	
Cyber security refresh program	Capex	0.60	0.60	0.96	0.60	0.60	3.35
	Opex step change	3.47	3.47	3.47	3.47	3.47	17.37
	Sub-total	4.07	4.07	4.43	4.07	4.07	20.72
Cyber security uplift program	Capex	0.07	0.60	0.97	0.93	0.44	3.00
	Opex step change	4.61	10.87	11.35	10.45	10.37	47.65
	Sub-total	4.68	11.47	12.32	11.38	10.81	50.65
Total	8.75	15.54	16.75	15.45	14.88	71.37	

Source: SAPN – 6.1 – Opex Model – January 2024 Public; SAPN – 5.1.1 – AER Standardised Capex model – January 2024 – Public

3.2 Summary of the basis for SAPN’ proposed expenditure

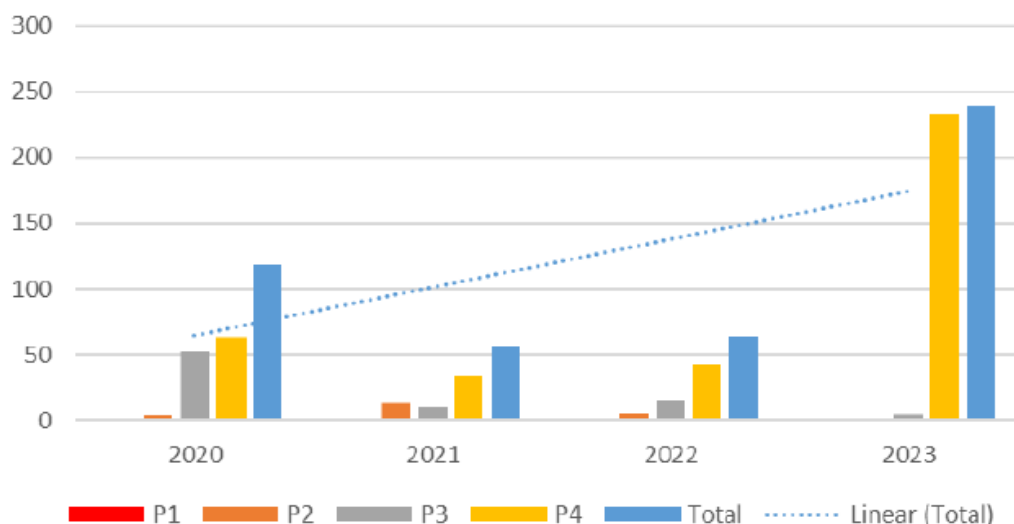
3.2.1 Documents supporting proposed cyber security program

86. SAPN has provided the following core documents to support its cyber security strategy, initiatives and investment:
- SAPN - 5.12.1 - IT Investment Plan 2025-30 - January 2024 - Public
 - SAPN - 5.12.6 - Cyber Security Refresh - January 2024 - SOCI Act Protected
 - SAPN - 5.12.9 - Cyber Security Uplift - January 2024 - SOCI Act Protected
 - SAPN - 5.12.6 Cyber Security (recurrent) estimate - Option 2 Preferred (Maintain current risk level) SOCI Act Protected
 - SAPN - 5.12.9 Cyber Uplift estimate - Option 2 Preferred (Risk-based) SOCI Act Protected.
87. These documents were supplemented by information provided in response to written information requests and from presentation material and discussions at an on-site meeting with SAPN representatives and representatives of the AER in May 2024.

3.2.2 Problem definition and risk assessment

88. The drivers for change enunciated in SAPN’s business cases are aligned to the ASD’s Cyber Security Threat Report 2023, stressing the increasing complexity, prevalence, and targeted nature of cyber security threats on its business. Figure 3.1 shows the increasing trend in cyber security incidents impacting SAPN over the last three years. It has had no P1 breaches (highest severity). The most numerous breaches are P4 (least severe), and the data shows a significant decline in the number of P2 incidents as SAPN’s cyber security investments have progressed.

Figure 3.1: SAPN cyber incidents over the last four years



Source: SAPN - 5.12.6 - Cyber Security Refresh - January 2024 - SOCI Act Protected

89. SAPN also provides an analysis of the changes to the SOCI Act, including the SLACIP Act.

3.2.3 SAPN’s cyber security strategy and objectives

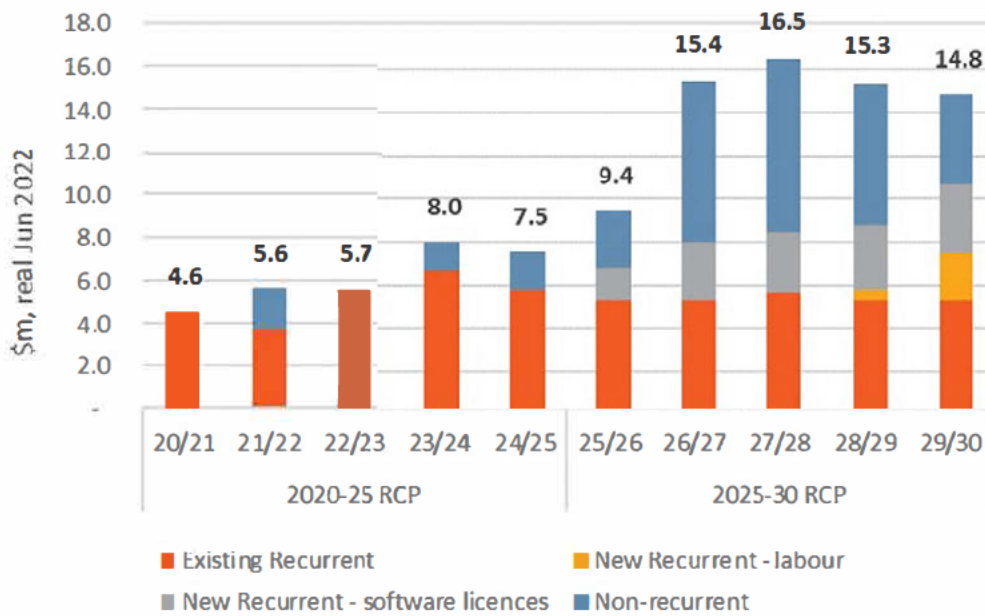
90. SAPN’s ICT cyber security strategy is based on compliance with the requirements of the SOCI Act and a risk-based approach to managing the increasing cyber security threat level and attack surface.

3.3 Our Assessment

3.3.1 Trend expenditure

91. In Figure 3.2, we show SAPN's forecast total expenditure on cyber security and its actual expenditure since 2020/21 (in \$FY22). As can be seen from this figure, SAPN's recurrent expenditure is relatively stable. The majority of the increase in the next RCP results from the increasing cost of software licences and from proposed non-recurrent capex, with a step increase in the latter commencing from 2026/27.

Figure 3.2: SAPN's historical and proposed cyber security expenditure (\$m FY22)



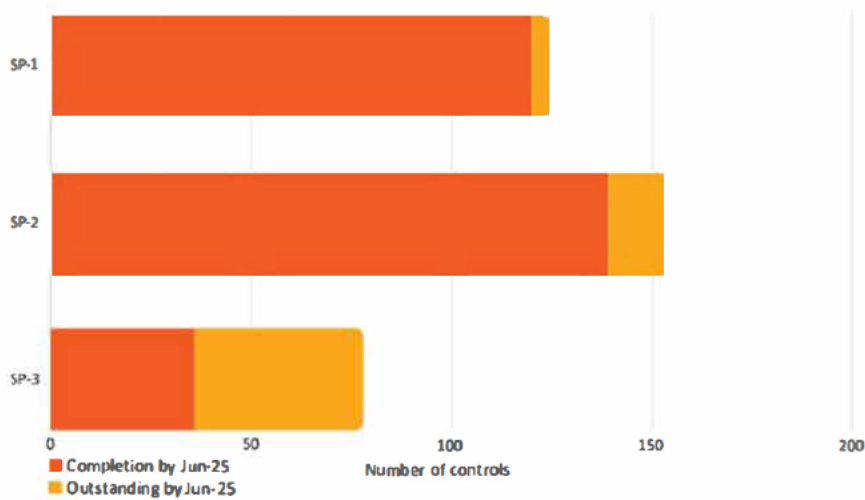
Source: SAPN, Day 2 ICT Cyber Security, [REDACTED]

3.3.2 SAPN's current state

SAPN's current cyber security program will place it well ahead of the minimum SP-1 obligation by the end of the current RCP

92. [REDACTED]

Figure 3.3: SAPN’s projected achievement of AESCSF V2 controls by the end of the current RCP



Source: SAPN Day 2 ICT Cyber Security, slide 8

- 93. SAPN has made substantial progress in implementing controls in the current RCP and the evidence would suggest that, whilst not eliminating all cyber security risk, those controls have been effective.
- 94. SAPN also notes that many of the implemented controls have been prioritised on the basis that they are ‘quick wins,’ and that remaining controls will on average be more complex, time-consuming and costly. We take this into account in our assessment of SAPN’s proposed 2025-30 expenditure.
- 95. SAPN advises that it will exceed the AER allowance of \$23.5 million (capex, \$2022) by \$7.6 million (+32%) due to:
 - The change from AESCSF V1 to V2, which has significantly increased the scope and cost of compliance with AESCSF; and
 - Its 2020-25 non-recurrent capex which is directed to an ‘uplift program of work’ to respond to increasing risk, with the cost likely to exceed the allowance because of a change in AESCSF requirements, more expensive personnel, and an increase in the real cost of software licensing.²³
- 96. We conclude that SAPN had (and still has) a reasonable basis for exceeding the allowance.

3.3.3 SAPN’s risk analysis

SAPN identifies its cyber security-related compliance obligations

- 97. [Redacted text]

²³ Day 2 ICT Cyber Security [Redacted text]

98. We are satisfied that SAPN has a good understanding of its compliance obligations, and we discuss SAPN's proposed expenditure to maintain compliance with those obligations in section 3.3.5.

SAPN has demonstrated an understanding of the threat landscape

99. Among other things, SAPN has identified that the underlying driver of its 'refresh' cyber security program is containment and mitigation of the existing risks associated with cyber security threats, which include:

the possibility of widespread network outages, physical harm to persons, large productivity losses, and non-compliance with regulatory and legal obligations.²⁴

100. SAPN has provided sufficient information in its business cases to enable us to conclude that:
- It has a good understanding of the form of risks it is exposed to both through operational technology (OT) and Information technology (IT) attack surfaces
 - It understands its obligations under the SOCI Act and has executed or will execute initiatives to implement cyber security controls in accordance with the AESCSF (i.e. including achievement of SP-1)
 - It understands the necessity to embed the capability to sustain the minimum compliance level of cyber security capability.

SAPN's risk profile at the commencement of the next RCP is self-assessed as 'High' despite considerable improvement over the course of the current RCP

101. SAPN has provided solid evidence that despite the substantial increase in cyber security incidents from 2022 to 2023, the controls it has introduced have been effective in reducing the severity of breaches (per Figure 3.1). While SAPN assesses that its risk profile will be 'high' at the commencement of the next RCP, this is considerably less than it would otherwise have been.
102. The escalation of incidents evident in Figure 3.3 is indicative of the increasing cyber security risk to SAPN and despite the improvement in its cyber security capability over the course of the current RCP it is reasonable for it to assess its cyber risk at the commencement of the next RCP as 'High'.²⁵
103. Furthermore, its assessment that it faces escalating risk over the course of the next RCP is consistent with advice from the information it has provided in its business cases and with ASD references we refer to in Section 2.
104. SAPN has presented its risk assessment for the next RCP in the absence of additional controls and we are satisfied that 'Extreme' is a reasonable representation of the projected qualitative risk by the end of the next RCP, as a counterfactual base case.²⁶ We therefore consider it reasonable for SAPN to consider investing in a further uplift in its cyber security controls (i.e. as an extension to the uplift program to be completed in the current RCP and while maintaining its proposed 'cyber security refresh' program, both of which we discuss below).
105. As discussed in our assessment of SAPN's options analysis, below, it has undertaken a cost-benefit analysis which derives the benefits from its proposed investments in enhanced cyber security controls based on probabilistic avoided costs. We comment on its assumptions regarding avoided risk as part of our assessment of the reasonableness of its proposed expenditure given that expenditure to reduce risk needs to be economically justified.

²⁴ SAPN - 5.12.6 - Cyber Security Refresh - January 2024 - SOCI Act Protected. Page 15.

²⁵ SAPN - 5.12.9 - Cyber Security Uplift - January 2024 - SOCI Act Protected, Page 22.

²⁶ Noting that this risk rating is not equivalent to the E-CAT criticality rating referred to in section 2.3

3.3.4 SAPN’s cyber-related objectives and strategy for the next RCP

SAPN has adopted a risk-based strategy which is appropriate

- 106. SAPN is pursuing a threat-based and risk-based approach to uplifting its cyber security capabilities to ‘*minimise and mitigate increasing cyber security risks.*’²⁷ This is consistent with what we consider to be good practice, with the proviso that the risk assessment identifies gaps and that controls are matched to those gaps, with implementation that is fit-for-purpose and implemented in a priority order to maximise risk mitigation.
- 107. We assess SAPN’s application of its risk-based approach in our assessment of SAPN’s proposed Cyber Security Uplift Program in section 3.3.6.

3.3.5 SAPN’s Cyber Security Refresh Program

- 108. We first assess the compliance of SAPN’s proposed refresh (or recurrent) cyber security expenditure, for which the objective is to maintain its existing cyber security and IT resilience capabilities.

Overview of options

- 109. SAPN presents only two options in its business case, as shown in Figure 3.4.

Figure 3.4: SAPN options considered in its Cyber Security Refresh (\$m, real 2022)

Option	10-year program costs			2025–30 program costs			10-year benefits ¹⁶	10-year NPV ¹⁷	Overall risk rating ¹⁸
	Capex	Opex	Total	Capex	Opex	Total			
Option 1 – Maintain current level of investment	8.3	27.1	35.4	4.1	13.5	17.7	n/a	-29.2	Extreme
Option 2 – Maintain current level of risk given existing threat levels	5.5	30.7	36.2	2.9	15.3	18.2	n/a	-29.9	Extreme

Source: SAPN - 5.12.6 - Cyber Security Refresh - January 2024 - SOCI Act Protected

Our assessment

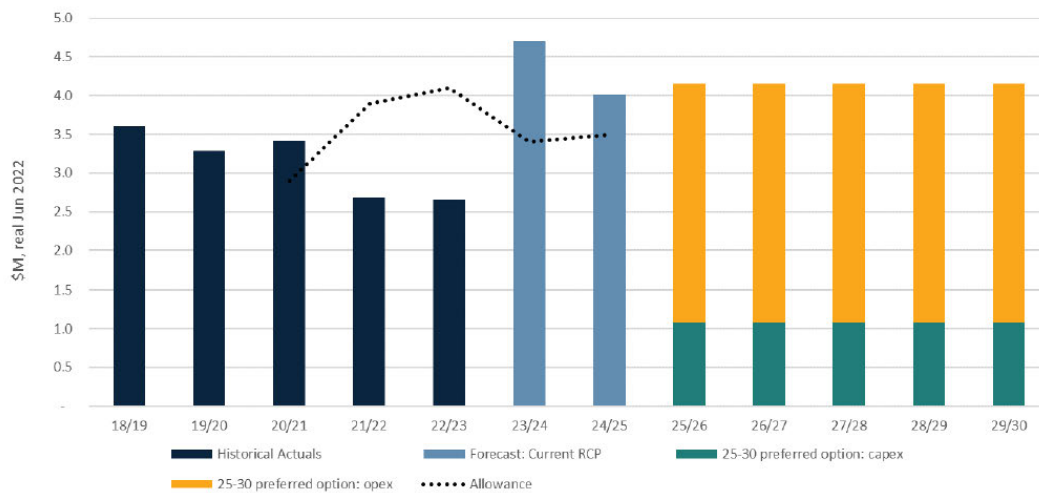
There is no material difference between the two options

- 110. SAPN has selected Option 2 after rejecting consideration of any option that reduces the level of expenditure to less than the current business-as-usual level.
- 111. Option 1 maintains the level of expenditure on cyber security over the next RCP at the same \$17.7 million (totex, \$FY22) as for the current RCP, noting that for both options there is a proposed reclassification of expenditure for operational IT cyber security activities from capex to opex, leading in turn to a proposed opex step change.
- 112. Option 2 includes the refresh of OT equipment coming to the end of its useful life plus a \$0.5 million (4%) increase to ‘*support the required increase in recurrent cyber security activity.*’²⁸ Refer to Figure 3.5.
- 113. SAPN states that pursuing its preferred Option 2 still renders it vulnerable to cyber-attack at an increasing rate, with the residual risk at the end of the next RCP rated by it as Extreme. Hence its proposed need for Uplift expenditure, discussed in Section 3.3.6.

²⁷ SAPN - 5.12.9 - Cyber Security Uplift - January 2024 - SOCI Act Protected. Page 6.

²⁸ SAPN - 5.12.6 - Cyber Security Refresh - January 2024 - SOCI Act Protected. Page 24.

Figure 3.5: Recurrent cyber security investment trend over time (\$m, 2022)



Source: SAPN - 5.12.6 - Cyber Security Refresh - January 2024 - SOCI Act Protected, Figure 4

SAPN identifies no quantifiable benefits for its preferred option

- 114. SAPN has presented a cost-benefit analysis for Options 1 and 2 but in the absence of benefits, it essentially presents the present cost of the options over a 10-year study period.
- 115. For expenditure to maintain capability, a positive CBA is not necessary under the AER’s guidance note.²⁹ We therefore consider only the costs, which we consider are reasonably derived (i.e. from extrapolation of its FY24/25 forecast).

The proposed expenditure is reasonable

- 116. We are satisfied that the proposed expenditure is likely to satisfy the AER expenditure criteria given that (i) SAPN has introduced a large number of controls during the current RCP as evidenced by its mapping of controls versus the AESCSF Security Profiles, and (ii) the proposed recurrent expenditure enables maintenance of current cyber security controls.
- 117. Therefore we consider that SAPN’s proposed capex and opex is reasonable.

3.3.6 SAPN’s Cyber Security Uplift Program

- 118. In addition to the \$20.7 million proposed for maintaining the current cyber security controls, SAPN proposes a further \$50.7 million to improve its capability over the course of the next RCP.

Overview of Options

- 119. Figure 3.6 shows the options considered by SAPN for its Uplift program. Option 2 is preferred, noting that the amounts shown in this figure are in \$2022.

²⁹ Refer to section 2.4.1.

Figure 3.6: SAPN’s options for cyber security uplift program - \$million real 2022

Option	10-year program/project costs			2025–30 Program/project costs			10-year benefits ⁴³	10-year NPV ⁴⁴	Overall risk rating ⁴⁵
	Capex	Opex	Total	Capex	Opex	Total			
Option 0 – Do nothing	-	-	-	-	-	-	-	-	Extreme
Option 1 – Basic controls	0.8	16.9	17.8	0.8	9.6	10.4	85.6	48.2	Extreme
Option 2 – Risk-based approach	2.6	68.9	71.4	2.6	42.1	44.7	225.7	107.0	Medium
Option 3 – Risk-based approach + Comply with SP-3	2.6	71.7	74.3	2.6	45.0	47.5	225.9	104.6	Medium

Source: SAPN - 5.12.9 - Cyber Security Uplift - January 2024 - SOCI Act Protected, Table 5

Our assessment

SAPN’s rational for uplifting its cyber security capability in the next RCP and adopting a risk-based approach is satisfactory

120. We are satisfied that the reasonable response to the cyber security risk assessment in section 2.1 and in SAPN’s business cases, is an uplift in risk mitigation capability over the course of the next RCP to ‘contain and mitigate’ the increasing threat level. This renders Option 0 as an imprudent approach.

Option 2 is the superior option of those considered

121. Option 1 would provide for \$10.4 million (\$2022) over the next RCP to implement ‘Application control’ and ‘Role-based access’ control to align with the ASD’s Essential 8 framework.³⁰ We accept SAPN’s assessment that achievement of the Essential 8 is not sufficient to address the cyber security risks in other areas of SAPN’s business.³¹
122. Option 2 is proposed by SAPN as it aligns with its risk-based approach to determining what controls it needs to mitigate its cyber security risk. We consider that a risk-based approach is appropriate and that SAPN has adequately sought to balance the cost of specific controls against the risk mitigation that can be achieved from those controls.
123. Option 3 would provide for achievement of all SP-3 controls for an additional \$2.8 million (\$2022) compared to its preferred Option 2. SAPN has not proposed it because it will achieve substantially the same benefits as Option 3 but at a slightly lower cost. SAPN notes that SP-3 is not a regulatory requirement,

SAPN effectively proposes going beyond the AESCSF in several control areas

124. SAPN claims that the AESCSF is deficient in that it ‘fails to account for some of the critical security controls identified in other internationally recognised cyber security frameworks.’³² SAPN has consequently included controls from its international research in its proposed Uplift program.
125. SAPN’s claim that the AESCSF V2 is somewhat deficient is surprising given the AESCSF has recently been updated with an extra 72 practices (between SP-1, SP-2 and SP-3) and in doing so it drew from internationally recognised frameworks, with NIST chief among them. Nonetheless, we assess SAPN’s proposed controls based on the merits of its assessment process. Its approach started with developing a risk register, drawing on its threat intelligence, then identifying gaps in its controls and appropriate control enhancements or new controls (drawing from international learnings). Finally, it advises that it has prioritised the implementation of the controls for maximum impact.

³⁰ SAPN - 5.12.9 - Cyber Security Uplift - January 2024 - SOCI Act Protected. Page 26.

³¹ SAPN - 5.12.9 - Cyber Security Uplift - January 2024 - SOCI Act Protected. Page 28 and Appendix B.

³² SAPN - 5.12.9 - Cyber Security Uplift - January 2024 - SOCI Act Protected. Page 31.

126. We consider this to be a transparent and appropriate approach to demonstrate the necessary controls to prudently manage the risks without being tied exactly to the ADESCSF, but nonetheless aligning to it. SAPN identifies 12 controls for implementation under Option 2 (i.e. in addition to the two Option 1 controls) and discusses the basis for each, explaining the current environment, the basis for its gap analyses (in several cases using alternative maturity frameworks), and describing the rationale for the selected solutions.
127. It is apparent from the relatively low maturity self-assessments against alternative maturity frameworks such as the CISA Zero Trust framework and the OWASP's SAMM V2 SSDLC³³ that SAPN is likely to exceed the level of cyber security resilience that would be achieved through satisfying the ADESCSF, at least in some areas.
128. It is evident that SAPN has undertaken a robust assessment and we consider that SAPN provides a reasonable basis for its assessment that its qualitative cyber risk level is likely to be reduced from a starting point of 'High' at the commencement of the next RCP (per the discussion in section 3.3.3) to 'Medium' by the end it. Later in our assessment, we consider SAPN's claim that the cost of the proposed capability uplift expenditure is more than offset by realistically determined benefits.

SAPN's cost estimation approach is satisfactory

129. SAPN describes a combination of a bottom-up and top-down approach to determining the cost estimation. Referring to the controls it identifies in its business case, it describes the following bottom-up steps:
- Estimate delivery team effort
 - Expenditure calculated using standard IT labour rates
 - Assess new software licensing requirements and cost.
130. SAPN states that it then subjected the bottom-up estimate to a peer review, benchmarking with other DNSPs, and other external entities to confirm the reasonableness of its estimate.
131. We observe that SAPN does not accurately represent the AER's draft decision regarding Ausgrid's cyber security totex that SAPN relies upon for a benchmark. SAPN cites \$70 million as a benchmark,³⁴ but this was proposed by us as a *maximum* justifiable amount in our report to the AER, based on the information that Ausgrid had provided.³⁵ Nonetheless, we have reviewed the costs for each control proposed by SAPN and consider them to be reasonable.

SAPN's net benefit is likely overstated but is still sufficient to justify the uplift project

132. SAPN's benefits assessment is based on two sources of monetised risk avoidance: (i) the avoided cost of P2-P4 events (i.e. less critical events, with P4 being the lowest impact), and (ii) the avoided cost of P1 events that would otherwise occur in the absence of further investment.
133. We assess SAPN's derivations of the two 'tranches' of benefits below.

SAPN's P2 P3, P4 probabilistic avoided recovery cost (benefit) is overstated

134. SAPN's first tranche of benefit is derived from assuming that by the end of FY30, the number of incidents per month increases as shown in Figure 3.7. While the increase in events in 2023 is significant, different interpretations of this for the future are possible. While SAPN has interpreted this increase as the beginning of a continuing trend increase leading to a tripling of such events by the end of the period, an alternative interpretation could be that the step increase in 2023 essentially represents a 'new normal' and that the number of future incidents could plateau at around this level. While we have no reason to favour one

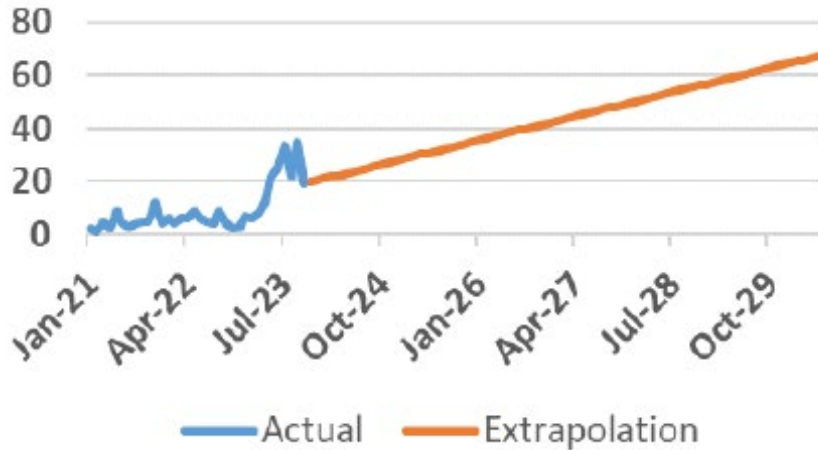
³³ Open Worldwide Application Security Project; Software Assurance Maturity Model; Secure Software Development Lifecycle.

³⁴ SAPN - 5.12.9 - Cyber Security Uplift - January 2024 - SOCI Act Protected. Page 18.

³⁵ EMCa, *Report to AER on Ausgrid's proposed expenditure on ICT cyber security 2024–29*, August 2023. Page 26.

interpretation over the other, we nevertheless consider that SAPN’s interpretation is more reasonably considered as an upper bound meaning that its forecast represents an overstatement of the ‘expected’ level of such incidents.

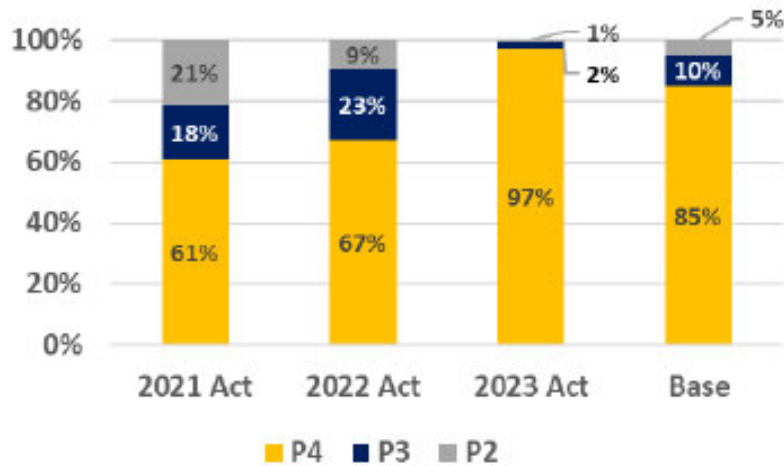
Figure 3.7: SAPN’s extrapolation of total number of incidents per month



Source: SAPN, Day 2 ICT Cyber Security, slide 18

- 135. Further, SAPN estimates the apportionment of P2, P3 and P4 events as shown in Figure 3.8, with 5% of incidents being P2 for the base case (i.e. the counterfactual against which the comparative benefits for Options 1, 2 and 3 are derived).
- 136. We focus here on P2 incidents as these incur the highest recovery cost and contribute the highest potential benefit, despite the higher assumed volumes of P3 and P4 incidents.

Figure 3.8: Assumed P2, P3, P4 incident severity ratios



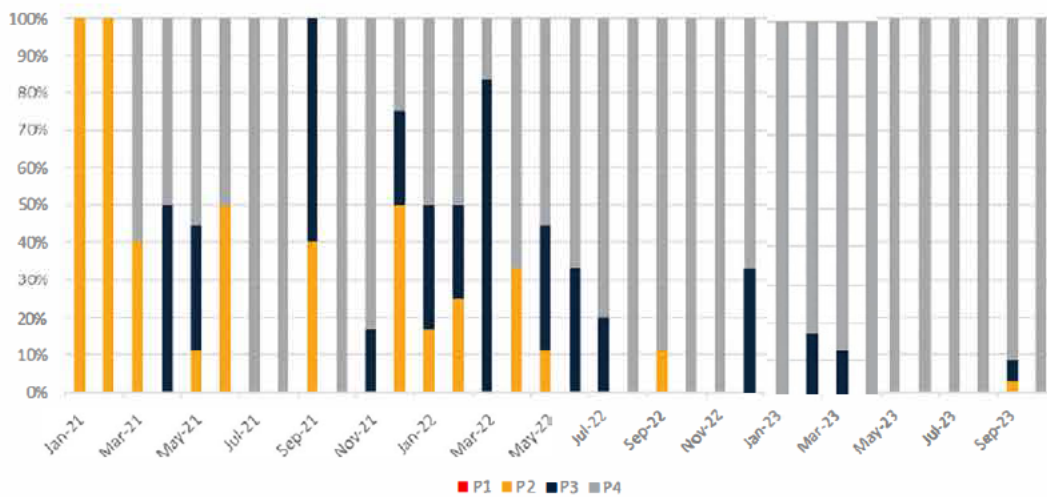
Source: Day 2 ICT Cyber Security - SOCI Act Protected, slide 18

- 137. The 5% assumption leads to an assumed 3.1 P2 incidents in FY25 and 39 P2 incidents p.a. by FY30 and 67 by 2035. We think this is likely to overestimate the number of P2 breaches for the following reasons:
 - There was a single P2 incident in FY23 (0.9% of the total incidents for the year), yet SAPN’s Base Case assumes 5% of incidents in 2025³⁶

³⁶ 5.12.9 Cyber Uplift estimate - Option 2 Preferred (Risk-based) SOCI Act Protected, incidents.

- SAPN is continuing to improve its cyber security resilience through to the end of the current RCP - it is reasonable to assume this will mitigate P2 incidents, as SAPN has successfully done over 2022 and 2023 (refer to Figure 3.9)
- SAPN has an extensive IT Investment Plan³⁷ for the next RCP with a common driver of cyber security resilience - the majority of the IT programs within the Plan result in upgrades or replacement of systems/apps/platforms to, among other things, improve cyber security against external attack,³⁸ and
- The ADMS will be upgraded in 2027 – again, SAPN cites cyber security resilience as a key reason for the upgrade of this critical operational technology.³⁹

Figure 3.9: SAPN - reduction of breach severity over 2021-2023 due to increased cyber resilience



Source: SAPN - 5.12.9 - Cyber Security Uplift - January 2024 - SOCI Act Protected, Figure 3

138. While the ADMS and IT upgrades are not a substitute for an uplift in cyber security along the lines proposed in the business case, in our view these should contribute to a lower proportion of P2 incidents across the next RCP.
139. SAPN has estimated the cost of P4 breaches [REDACTED] based on the estimated recovery costs, derived from SAPN's own experience. We consider this to be a sound approach to deriving the consequence values and therefore the amounts to also be reasonable for the purposes of the analysis. We discuss SAPN's sensitivity analysis which is based primarily on varying the avoided costs in a section below.
140. The benefit over the ten-year study period from adopting Option 2 and thereby avoiding the majority of P2, P3, and P4 incidents is determined by SAPN to be [REDACTED] (\$2022). We consider this to be an overestimate of the probabilistic avoided cost, and which we consider further as part of our sensitivity analysis, discussed below, after first assessing SAPN's P1 benefit analysis.

SAPN's P1 probabilistic avoided cost (benefit) is overstated

141. [REDACTED]

[REDACTED]

[REDACTED]

³⁷ SAPN - 5.12.1 - IT Investment Plan 2025-30 - January 2024 – Public.

³⁸ Regular refreshes and upgrades will continue to occur through to the end of the ten year study period of 2035, with commensurate upgraded cyber security patches and general resilience improvements.

³⁹ The ADMS upgrade is not included in the IT Investment Plan 2025-30; refer to Section 4 of this report.

- [REDACTED]
- [REDACTED]

- [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]

- [REDACTED]

- [REDACTED]

40

- [REDACTED]

[REDACTED]

[REDACTED]

SAPN's sensitivity analysis shows a positive NPV for the lowest impact scenario

147. SAPN developed two alternative scenarios to contrast with its 'Likely case' (i.e. its proposed Option 2):

- The Best case (lowest impact of cyber security events), and
- The Worst case (highest impact of cyber security events).

148. The benefits (avoided monetised risk) over 10 years were calculated by SAPN for the Best and Worst cases by varying [REDACTED]

[REDACTED] SAPN also varied the discount rate (Lower, Central, and High) to further test the robustness of the proposed investment. The result for the Best case under each of the discount rate assumptions is a marginally positive NPV even with the lowest benefits (i.e. the best case scenario).

149. We consider that SAPN's sensitivity analysis helps confirm that its Uplift investment is likely to be prudent. Nonetheless, because we are of the view that SAPN's likelihood of consequence assumptions are overstated, we also considered an alternative sensitivity study.

EMCa's sensitivity analysis of SAPN's assumed likelihood of occurrence of P1-P4 events

150. Our alternative sensitivity study is based on our view that SAPN may have overstated the likelihood of occurrence of the P1 and P2 events:

- For P1 incidents, SAPN has not provided compelling information to substantiate its proposed starting points or escalation rates for the frequency of P1 incidents leading to 2.2 P1 incidents p.a. in 2030 and increasing from that point to the end of the study period. We acknowledge that it is not possible to forecast accurately the number of P1 incidents over the next RCP and through to 2035 given the variables involved. Nonetheless, we consider SAPN's assumption to be representative of a 'High' case. As

shown in Table 3.2, we have varied the likelihood of two of the P1 events as part of hypothetical 'Central' and 'Low' cases.

- For P2 incidents, SAPN assumed 5% of its P2+P3+P4 incidents are P2 incidents. A P2 incident is the second-most significant cyber incident and is not justified by the historical information provided by SAPN described above. Again, we accept that it is not possible to forecast accurately the number of P2 events over the next RCP given the variables involved. Noting that we are of the view that SAPN's linear projection of P2+P3+P4 incidents appears to be overly pessimistic, we consider that 5% is more likely than not a 'High' case. As shown in Table 3.2, we have varied the likelihood of occurrence of P2 incidents to create Central and Low cases.
 - For P3-P4 incidents, we have not changed SAPN's assumed likelihood of occurrence because the impact on the outcome is not material.
 - We have not varied SAPN's assumed cost of consequence in our sensitivity study.
151. The resulting risk reductions compared to SAPN's Option 2 afforded by the Central and Low scenarios are 39% and 54% respectively, which are substantial but still result in positive NPVs.
152. We could also vary the cost of consequence assumptions as SAPN has done in its sensitivity analysis and a negative NPV would likely result, however, the point of the exercise was to test whether SAPN's proposed investment is likely to be prudent under less 'pessimistic' projections of incident frequency.

Table 3.2: EMCa sensitivity analysis of likelihood and impact on consequence

Event	Sensitivity 'cases'					
	SAPN 'Option 2'		EMCa 'Central'		EMCa 'Low'	
	2025	2030	2025	2030	2025	2030
Risk reduction (\$m FY21)	219.7		134.1		101.5	
Cost of risk reduction	0% (counterfactual)		-39%		-54%	
NPV (\$m FY22, 10 years)	107.0		42.6		18.2	

Source: EMCa analysis based on SAPN 5.12.9 Cyber Uplift estimate - Option 2 Preferred (Risk-based) SOCI Act Protected

SAPNs net benefit is likely to exceed the uplift cost

153. In aggregate SAPN has derived a benefit from the avoided cost and risk monetisation from implementing Option 2 compared to its counterfactual (base case) of \$225.7 million (\$2022, over the 10-year study period), equivalent to a PV of \$167 million. The NPV is calculated by SAPN to be \$107.0 million (\$2022) after deducting the PV of cost of \$60.0 million.⁴²
154. Whilst we consider that the benefit is likely to be overstated by between approximately 40% to 55%, the resultant NPV would still be positive for both Options 2 and 3, with the NPV being higher for Option 2 (as shown in Table 3.2), supporting selection of Option 2.

⁴² 5.12.9 Cyber Uplift estimate - Option 2 Preferred (Risk-based) SOCI Act Protected, NPV Analysis.

155. Similarly, SAPN's own sensitivity analysis indicates that the NPV will be positive with significantly lower consequence costs, adding weight to our conclusion that Option 2 represents a prudent path forward.

3.3.7 Findings and Implications

Summary of our findings

SAPN's cyber security Refresh project is reasonable, based on managing risks with fit-for-purpose controls

156. SAPN has compliance obligations arising from amendments to the SOCI Act and the Privacy Act which it will more than satisfy by the end of the current RCP. [REDACTED]

157. We consider it reasonable for SAPN to maintain its expected FY24/25 level of annual capex and opex over the course of the next RCP to maintain the underlying capability it has established. Therefore, we conclude that the proposed cyber security 'Refresh' capex and opex step change are likely to satisfy the NER expenditure criteria.

SAPN's cyber security Uplift project is reasonable, based on managing increasing cyber risks with risk-prioritised additional controls

158. We are satisfied that the combination of SAPN's risk register and the identification of gaps and controls to manage the exposures throughout the course of the next RCP is a sound approach. The detail it has provided to support its proposed Option 2, including the proposed breadth and depth of controls is sufficient justification for the scope of work.
159. SAPN has selected an option which is slightly lower cost than achieving full alignment with AESCSF V2 SP-3, but which substantially achieves the same level of benefits. We consider this to be a prudent approach.
160. We are satisfied that SAPN's cost forecasting methodology is a sound basis for estimating the cost required to deliver the Uplift project for the next RCP.
161. We therefore conclude that the proposed 'Uplift' capex and opex step change are likely to satisfy the NER expenditure criteria.

Implications of our findings for proposed expenditure

162. We propose no adjustment to SAPN's proposed capex for the next RCP nor to its proposed opex step change. Therefore, we consider that the capex and opex that SAPN has proposed, as shown in Table 3.1, is reasonable.

4 ADVANCED DISTRIBUTION MANAGEMENT SYSTEM (ADMS) UPGRADE

The ADMS provides automated outage detection, restoration, and performance optimisation of SAPN’s network.

Extended support for the Microsoft operating system and database used by key ADMS components ends in 2027, necessitating an update to the ADMS software at an estimated capital cost of \$32.4 million (and no opex). SAPN also cites compliance with the SOCI Act as a complementary driver.

We consider that SAPN has identified the prudent option and that the estimated cost is reasonably based, drawing from relatively recent experience with updating version [REDACTED] to the current version [REDACTED] and with implementing OMS and DERMS modules, among other functionality.

4.1 Overview

- 163. SAPN’s current version [REDACTED] of ADMS comprises the ADMS application, operating systems, physical and virtual workstations, and server hardware. It incorporates SCADA, Feeder Automation, Outage Management and Switching Management for management of planned and unplanned outages. It will also include a DERMS module before the end of the current RCP.⁴³
- 164. Table 4.1 shows SAPN’s proposed expenditure over the next RCP for the \$32.4 million project to replace its ADMS and the associated modules, systems, and database.

Table 4.1: SAPN’s proposed expenditure profile for the ADMS Upgrade (\$m FY25)

	FY26	FY27	FY28	FY29	FY30	TOTAL
ADMS Hardware Upgrade	0.6	4.2	0.4	0.0	0.0	5.1
ADMS Software Upgrade	1.7	9.1	11.4	0.0	0.0	22.2
Additional ADMS Functions	1.0	1.0	1.0	1.0	1.0	5.0
TOTAL	3.3	14.3	12.8	1.0	1.0	32.4

Source: EMCa table, from SAPN 5.1.1 standardised capex model

- 165. SAPN’s upgrade project is based on four drivers, all of which are related to version [REDACTED] of its ADMS indirectly becoming unsupported in late 2027:⁴⁴
 - To respond to customers’ requirement for SAPN to maintain reliability of service
 - To help comply with SOCI Act obligations – particularly pertaining to cyber security
 - To maintain the safety of the distribution network and system
 - To drive efficiency in the ADMS and related applications.

⁴³ SAPN - 5.13.1 - ADMS Version Upgrade - January 2024 - SOCI Act Protected. Page 6.

⁴⁴ SAPN - 5.13.1 - ADMS Version Upgrade - January 2024 - SOCI Act Protected. Page 9.

4.2 Assessment

SAPN's ADMS has grown over the course of the current RCP with more investment to come

166. SAPN's ADMS has undergone numerous upgrades and refreshes since it was first installed. The latest version [REDACTED] was installed in the current RCP at a cost of \$10.6 million (\$2022). The 2020-25 program also included retiring the standalone Outage Management System (OMS) and incorporating an OMS module within the ADMS (\$8.4 million, \$2022) and also adding a Distributed Energy Resource Management System (DERMS) module (\$3.5 million). The addition functionality (i.e. OMS and DERMS) was not included in the 2019 business case.
167. SAPN also invested \$2.3 million (\$2022) to deploy an Integrated Testing Environment and a dedicated Training Environment. In aggregate this led to an expected project expenditure in the current RCP of \$24.7 million (\$2022) capex, compared to the AER's FD allowance of \$16.3 million (\$2022).⁴⁵
168. This is relevant to the estimated cost of upgrading the ADMS again in the next RCP, with SAPN stating that the *'integration between the ADMS and corporate IT systems has increased from two integrations in 2014 to more than 40 in the ADMS version [REDACTED]*⁴⁶

SAPN needs to respond to looming technical obsolescence

169. SAPN's ADMS is a business-critical system, as are ADMSs in any DNSP. It is fundamental to maintaining the operational security and reliability of its distribution network,
170. It is reasonable for SAPN to conclude that the ADMS presents a significant target for cyber threat actors looking for avenues to disrupt SAPNs operations. The P1 operational network loss scenario discussed in section 3.3.6 could be realised through a successful breach of the ADMS, for example.
171. SAPN advises that Microsoft will discontinue support for its currently installed versions of Microsoft Server and Windows Operating systems [REDACTED] and Microsoft SQL database software in [REDACTED]. It further advises that:
- ADMS [REDACTED] software is not compatible with newer Microsoft operating systems and therefore a change to the Microsoft operating system necessitates an update to the ADMS software.
 - Microsoft follows a strict policy of removing extended support after the announced date.
172. Lastly, we consider that SAPN's statement that *'...regular updating and patching of application software, ...reduces vulnerabilities and therefore the likelihood of a security breach'* is a defensible statement.⁴⁷ We have taken this into account in our assessment of SAPN's benefit analysis in section 3.3.6.
173. We conclude that it is appropriate for SAPN to consider alternatives to manage the operational and cyber security risks inherent to an unsupported ADMS.

SAPN's options analysis was simple but the selected option is prudent

174. SAPN identifies four options in its ADMS business case. It dismisses two of them on the grounds of excessive cost, without compensating benefits:
- Cease using ADMS / rely on manual processes
 - Replace the ADMS with a product from an alternative vendor.
175. SAPN also dismisses a third option, to not upgrade ADMS [REDACTED] until the 2030-35 RCP, because it would lead to an 'Extreme' risk level by the end of the next RCP. SAPN has only

⁴⁵ SAPN - 5.13.1 - ADMS Version Upgrade - January 2024 - SOCI Act Protected. Pages 6-7.

⁴⁶ SAPN - 5.13.1 - ADMS Version Upgrade - January 2024 - SOCI Act Protected. Page 7.

⁴⁷ SAPN - 5.13.1 - ADMS Version Upgrade - January 2024 - SOCI Act Protected. Page 5.

presented a qualitative risk assessment, with a security breach assumed to result in severe disruption to services and high financial costs (recovery costs and penalties). However, it is a reasonable conclusion that not replacing the ADMS until the 2030-35 RCP would not be prudent, noting the project lifecycle is estimated by SAPN to be three years from start to finish.

176. This leaves its preferred option, upgrading the ADMS (with OMS and DERMS functionality), which will maintain vendor support with the latest available cyber security defence measures inbuilt.
177. Whilst the 'do nothing' option could be maintained for perhaps one to two years after the end of vendor support, the deferred costs of \$2-3 million in present value terms would be more than offset by the risk-cost of a breach, as discussed in section 3.
178. No quantified benefits are attributable to the preferred option. SAPN claims that integrating the OMS into the ADMS suite represents a cost saving on maintaining a stand-alone system, but this has not been quantified. Regardless, the decision to retire the then-current OMS has been made in the current RCP (with \$11.4 million of the total estimated OMS replacement cost of \$19.8 million to be spent in the current RCP).
179. Overall, we consider that upgrading the ADMS, including the OMS and DERMS modules, by late 2027 is the prudent path. It will maintain vendor support for all components of the ADMS, significantly reducing cyber security risk. The upgrade of the ADMS should be considered explicitly by SAPN as a key plank in its defences against cyber security breaches.

The cost estimate is reasonable

180. We note the following with respect to SAPN's cost estimate:
- SAPN's cost estimate is a bottom-up build with a modest work breakdown structure and hard coded numbers.⁴⁸
 - SAPN underspent its allowance by 13.5% in implementing the ADMS upgrade and DERMS module in the current RCP, which indicates that it may be prone to overestimating costs – however we consider that this possibility is largely offset by SAPN's claim to have based the estimate for the work in the next RCP on its experience with the current project.
 - SAPN attributes the \$5.0 million higher cost for the next RCP to the need to support the additional DERMS and OMS functionality – this is reasonable.
181. We conclude that SAPN's cost estimate is reasonable.

4.2.2 Findings and implications

Summary of our Findings

182. SAPN has provided sufficient information for us to conclude that upgrading its ADMS by 2027 is the prudent path due to the lack of vendor support from that time. The underpinning Microsoft operating system [REDACTED] server and database software reach the end of extended support in late 2027 and SAPN's current version of ADMS is not compatible with [REDACTED]
183. The upgrade proposed will bring an unquantified benefit to SAPN's cyber security resilience by including the latest defences against cyber-attacks of its primary operational technology system.

⁴⁸ 2025 - 30 Reset - Project-ADMS_Version_Upgrade-Option1_CONFIDENTIAL.

Implications of our findings

184. No capex adjustment is proposed, noting that SAPN is bearing the increased opex cost (higher licence fees) and has not proposed an opex step change. We therefore consider that the capex that SAPN has proposed, as shown in Table 4.1, is reasonable.