



Business case: ADMS Version Upgrade

2025-30 Regulatory Proposal

Supporting document 5.13.1

January 2024



Empowering South Australia

Contents

Glossary.....	3
1 About this document.....	4
1.1 Purpose.....	4
1.2 Expenditure category	4
1.3 Related documents.....	4
2 Executive summary	5
3 Background	6
3.1 The scope of this business case.....	6
3.2 Our performance to date.....	6
3.3 Drivers for change	7
3.4 Industry practice.....	8
4 The identified need	9
5 Comparison of options	10
5.1 The options considered	10
5.2 Options investigated but deemed non-credible	10
Replace the ADMS with a product from an alternative vendor	10
Cease to use an ADMS and fall back to manual processes	10
5.3 Analysis summary and recommended option	11
5.3.1 Options assessment results.....	11
5.3.2 Recommended option	11
5.4 Option 0 (base case) Do not upgrade the ADMS	11
5.4.1 Description	11
5.4.2 Costs.....	12
5.4.3 Risks	12
5.4.4 Disadvantages.....	12
5.4.5 Quantified benefits	13
5.4.6 Unquantified benefits	13
5.5 Option 1 Upgrade the ADMS.....	13
5.5.1 Description	13
5.5.2 Costs.....	13
5.5.3 Risks	14
5.5.4 Quantified benefits	14
5.5.5 Unquantified benefits	14
6 Deliverability of recommended option.....	15
7 How the recommended option aligns with our engagement	15
7.1 Alignment to customer expectations	15
7.2 Alignment to the views of other stakeholders.....	15
8 Alignment with our vision and strategy.....	15

9	Reasonableness of cost and benefit estimates	16
10	Reasonableness of input assumptions	16
A.	Appendix A – cost models	17
B.	Appendix B – Risk assessment	18

Glossary

Acronym / term	Definition
ACSC	Australian Cyber Security Centre
ADMS	Advanced Distribution Management System
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
ASD	Australian Signals Directorate
Capex	Capital expenditure
CSF	Cybersecurity Framework
DERMS	Distributed Energy Resource Management
LV	Low voltage
NIST	National Institute of Standards and Technology
NPV	Net present value
OMS	Outage Management System
Opex	Operating expenditure
RCP	Regulatory Control Period

1 About this document

1.1 Purpose

The purpose of this document is to provide the business case and justification for the ongoing investment in the Advanced Distribution Management System (ADMS) platform, [REDACTED]

1.2 Expenditure category

- Non-network capital expenditure (**capex**): other non-network

1.3 Related documents

Table 1: Related documents

Ref	Title	Author	Version / date
[1]	ADMS Business Case	SA Power Networks	10 December 2019, Supporting document 5.32, 2020-25 Revised Regulatory Proposal
[2]	LV Management Business case	SA Power Networks	25 January 2019, Supporting document 5.18, 2020-2025 Regulatory Proposal

2 Executive summary

This business case considers the investment options over the 2025-2030 regulatory control period (RCP) to maintain the capability [REDACTED], enabled by our Advanced Distribution Management System (ADMS). The preferred option is to continue our recurrent program of investment in the ADMS to maintain vendor support [REDACTED] and alignment with industry recommended cyber security practices.

We have been investing in our ADMS and increasing its capabilities and functionality to maintain service outcomes for customers despite an increasing amount of complexity surrounding the operation of the electricity distribution network.

[REDACTED]

One of the most effective defence mechanisms against cyber security threats is the regular updating and patching of application software, as this reduces vulnerabilities and therefore the likelihood of a security breach. [REDACTED]

[REDACTED]

The Australian Government through the Australian Signals Directorate's (ASD), Australian Cyber Security Centre (ACSC) and the Security of Critical Infrastructure Act, as well as good electricity industry practice, dictate that to manage the risk of cyber security attacks [REDACTED], vendor support should be current and in place for all systems and underlying platforms.

This business case recommends a continuation of the current program to proactively refresh our systems using the current refresh rates across the operational systems environment. The 2025-2030 RCP forecast of **\$28.0 million²** in capex represents an uplift of \$3.3m compared to the actual spend in the 2020-2025 RCP due to the additional functionality that was implemented in the 2020-25 RCP to support the Customer Energy Resources (CER) integration [REDACTED]

This option was selected because it:

- ensures our systems align with industry recommended cyber security practices;
- [REDACTED]; and
- maintains vendor support for critical applications and hardware.

We compared this option against the 'do nothing' baseline, ie not upgrading the ADMS after the extended vendor support ceases in 2027. The 'do nothing' option was deemed non-credible due to the unacceptable cyber security risk and lack of vendor support.

Other options considered were replacing the ADMS with a product from an alternative vendor and ceasing to use an ADMS and falling back to manual processes. These options were dismissed due to prohibitive costs and the lack of business benefits.

² Unless otherwise specified, all financial figures in this business case are in real June 2022 dollars

3 Background

3.1 The scope of this business case

The ADMS is a software platform [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

[REDACTED]
[REDACTED]

A critical requirement in the management of the ADMS is to maintain secure operating environments and effective interfaces between the key operational components whilst integrating it to an evolving software and hardware technology environment.

The most pertinent challenges to this requirement include:

- maintaining the currency of the ADMS software to ensure ongoing vendor support; and
- maintaining the operating systems and database platforms within the bounds of extended vendor support to mitigate cyber security risks.

3.2 Our performance to date

The Australian Energy Regulator (**AER**) Final Determination for the 2020-2025 RCP provided \$12.3m capex for the upgrade of the ADMS environment to the latest supported version of the operating system, application and hardware, as proposed in our 2019 ADMS business case⁴. The upgrade [REDACTED] addressed all key objectives of the project.

Consistent with our long-term direction for scaling of the flexible exports capabilities and in response to customers seeking flexible connections, for both load and generation connections, [REDACTED] This extension to existing ADMS functionality will be implemented in 2024 and was funded from the Low Voltage (**LV**) Management Business case⁵, as approved for the 2020-2025 RCP.

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

⁴ SA Power Networks: *ADMS Business case*, 25 January 2019, Supporting document 5.32, 2020-25 Revised Regulatory Proposal, 10 December 2019

⁵ SA Power Networks, *LV Management Business case*, Supporting document 5.18, 2020-2025 Regulatory Proposal, 25 January 2019

[REDACTED]

Subsequent to this, additional capabilities within the ADMS platform have been developed with further integrations with corporate systems to maintain customer outage notifications and reporting capabilities. This included the deployment of an Integrated Testing Environment as well as a dedicated Training Environment, both of which integrate to corporate test systems to allow end-to-end testing and regular operational training to occur for both office and field-based teams.

Whilst the implementation of these additional ADMS capabilities has not been included in our 2019 ADMS business case and the associated AER allowance, the recurrent spend required to maintain and refresh these capabilities has become part of the ongoing ADMS upgrade program and has therefore been included in this business case. [REDACTED]

[REDACTED] significant savings will be achieved by upgrading them as part of the ADMS, with a single implementation and data conversion effort.

The summary of our ADMS-related actual and forecast capex in the 2020-2025 RCP compared to the 2020-2025 AER allowance is presented in Table 2.

Table 2: ADMS-related actual/forecast capex compared to allowance for the 2020-2025 RCP, \$million, \$June 2022⁶

Program	Allowance	Actuals / Forecast
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

3.3 Drivers for change

The threats against critical infrastructure are increasing rapidly in Australia and worldwide. The ACSC 2022 Cyber Threat Report stated that 95 cyber security incidents occurred against critical infrastructure within the 2021-22 financial year. This threat is predicted to increase year on year, with Gartner predicting that by 2025, 30% of critical infrastructure worldwide will experience a breach that will result in the halting of either operations or mission critical cyber-physical systems⁷.

Maintaining vendor support for all components of the ADMS is critical to reduce the risk associated with cyber security threats within our operational systems.

In addition to this, since the initial implementation of the ADMS in 2014, the environment has continued to grow and expand as operational capability requirements have evolved. Additional modules, improved functionality and tightly integrated systems to deliver these capabilities have resulted in an increasingly complex environment. [REDACTED]

[REDACTED] This increase has resulted in the need for additional operational support and has resulted in more complex upgrade paths.

⁶ Note: Totals presented in tables throughout this document may not exactly match the sums of individual figures due to rounding

⁷ [Gartner Predicts 30% of Critical Infrastructure Organizations Will Experience a Security Breach by 2025](#)

It is also worth noting that our ADMS vendor has advised that our system support contract as it was negotiated and agreed for the 10-year period to 2024 included incorrect fees which, because of this error, were in the order of 25% lower than their normal support fees. The vendor has honoured the current contract at this lower rate but has advised the new contract to be agreed in 2024 will include current service fees which will result in a step change in our operational expenditure for annual system support costs. This additional cost will be absorbed within efficiency gains in the current operating expenditure allowance.

3.4 Industry practice

In August 2018 Australian Energy Market Operator (**AEMO**) in collaboration with industry and government stakeholders⁸ developed a cyber security capability framework and maturity model – the Australian Energy Sector Cyber Security Framework (AESCFS). This framework was designed to enable assessment of cyber security capability and maturity for Australian NEM participants. Legislation will be passed within the current RCP mandating that all high criticality energy businesses meet the first security profile within this framework – SP-1, while the 3rd maturity profile (SP-3) is expected to be legislated in the future. SA Power Networks has been assessed as a high criticality business under this framework in both 2022 and 2023.

[Redacted text block]

[Redacted text block]

⁸ including the Australian Energy Market Operator (AEMO), Australian Cyber Security Centre (ACSC), Cyber and Infrastructure Security Centre (CISC), and representatives from Australian energy organisations

4 The identified need

The driver for investment being considered in this business case is to address the issues associated with our business-critical technology capabilities. This includes addressing non-availability and security risks associated with applications or modules that have reached end-of-life by replacing or upgrading these, as well as implementation of any updates required to ensure that current capabilities can be maintained efficiently over time.

In considering potential responses to this driver, we engaged with our customers on their desired service level outcomes balanced against price outcomes and considered our regulatory requirements under the National Electricity Rules (NER), National Electricity Law and jurisdictional regulations. As a result of these considerations, the identified need for our ADMS lifecycle management is:

- a. to respond to customers' concerns^[1], identified through our consumer and stakeholder engagement process, regarding their explicit service level recommendations that we maintain reliability of service performance – driven by a desire to not see outages due to failed or insecure ADMS functions;
- b. to continue to comply with applicable regulatory obligations / requirements, in this case with specific reference to cyber security obligations and enhanced responsibilities for critical infrastructure providers;
- c. to maintain the safety of our distribution network and system, in relation to the risks of harm to workers, consumers and community – through the provision of easy to access and clear information for all customers when they need it, particularly during significant outage events; and
- d. to drive efficiency in our ADMS and related applications, ensuring continuity of essential services for the minimum possible long-term cost.

[REDACTED]

[REDACTED]

[REDACTED]

To meet these objectives and to pass vulnerability assessments our software systems must be maintained on supported versions. Unsupported and unpatched software does not meet the requirements for protection and may reduce the ability for a business to detect and respond to a cyber-attack.

Upgrade pathways and system supportability of the ADMS is determined by the software vendors. In this case, [REDACTED] will be discontinuing its support for the current installed versions of [REDACTED] and [REDACTED] follows a strict policy of removing extended support after the announced date.

5 Comparison of options

5.1 The options considered

Table 3: Summary of options considered

Option	Description
Option 0 (base case): Do not upgrade the ADMS	Continue using existing ADMS software and platform after Microsoft support for the operating systems is withdrawn.
Option 1: Upgrade the ADMS	Update the operating system to maintain vendor support which in turn necessitates updating the ADMS to the latest version.

5.2 Options investigated but deemed non-credible

The following options were identified but not considered in detail due to their non-feasibility.

Replace the ADMS with a product from an alternative vendor

This option has been rejected because the cost would be very high due to the need to establish a new system from scratch and retrain all staff. There are no known benefits that an alternative vendor could provide to SA Power Networks that could justify the additional expense.

Cease to use an ADMS and fall back to manual processes

This option has been rejected because the ADMS has resulted in significant business efficiencies. SA Power Networks would require a large increase in operating and capital expenditure to maintain current service levels without an ADMS.

The ADMS is embedded into many systems and business processes so calculating the additional expenditure required to operate the network without the ADMS would be a significant undertaking. Therefore, this option has not been considered for further investigation.

5.3 Analysis summary and recommended option

5.3.1 Options assessment results

Table 4: Costs, benefits and risks of alternative options relative to the base case over the 5-year period, \$m, \$ June 2022 real

	Costs		Benefits ⁹		NPV ¹⁰	Rank
	Capex ¹²	Opex ¹³	Capex	Opex		
Option 0 (base case): Do not upgrade the ADMS	-	-	-	-	-	Non-credible
Option 1: Upgrade the ADMS	28.0	-	-	-	-25.9	1

5.3.2 Recommended option

The preferred option is Option 1: Upgrade the ADMS. Under Option 1, we would update the operating systems and consequently update the ADMS to the latest version.

This option **will maintain the existing ADMS capabilities and cyber security posture at the lowest viable cost** by maintaining operating systems in software support with regular vendor security updates to meet cyber security requirements.

It is therefore recommended that approval be given to proceed with Option 1: Upgrade the ADMS.

5.4 Option 0 (base case) Do not upgrade the ADMS

5.4.1 Description

This option maintains the current ADMS software version after the extended support for the underlying operating system ceases at the end of 2027. This will result in an inability to update the operating systems to the latest versions of Windows Server or Windows operating system.

This option is not credible because continuing to use the Windows operating systems after vendor support is withdrawn has an unacceptable level of cyber security risk for a mission critical system and is not in keeping with good electricity industry practice.

Additionally, our ability to enhance the ADMS will be significantly reduced due to the age of the application and the vendors ability to maintain resources skilled in older versions. Any development work will incur

⁹ Represents the total capital and operating benefits, including any quantified risk reductions compared to the risk of Option 0, over 5-year cash flow period from 1 July 2025 to 30 June 2030 expected across the organisation as a result of implementing the proposed option.

¹⁰ Net present value (NPV) of the proposal over 5-year cash flow period from 1 July 2025 to 30 June 2030, based on discount rate of 4.05%.

¹¹ [Redacted]

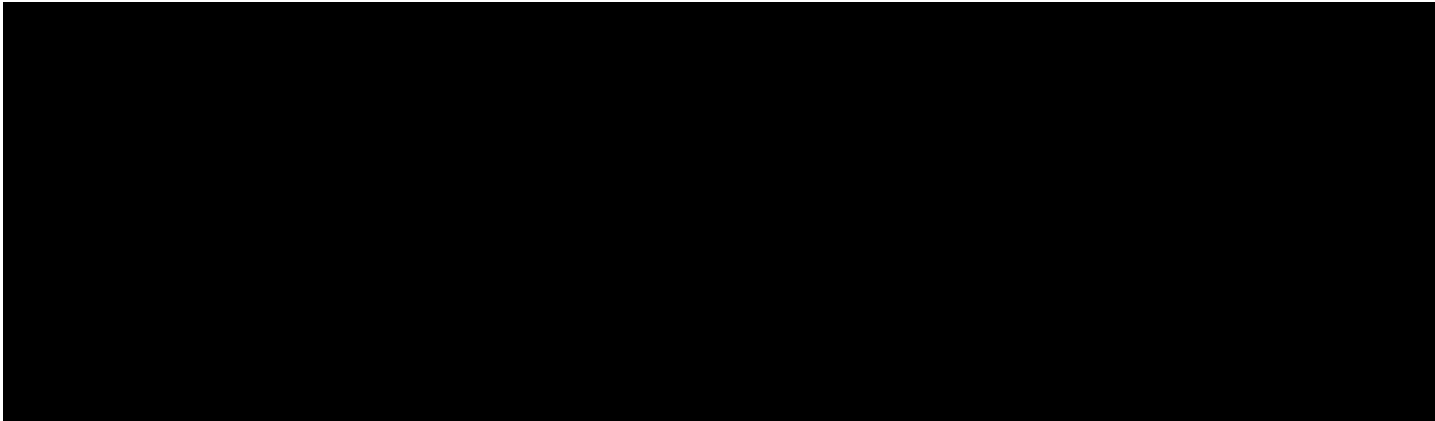
¹² Represents the total capex associated with the proposed option over the 5-year cash flow period from 1 July 2025 to 30 June 2030.

¹³ Represents the total opex increase associated with the proposed option above the current level of opex, over the 5-year cash flow period from 1 July 2025 to 30 June 2030.

additional cost as a result of the bespoke nature of the development and the increased risk of developing on older versions of code.

The matrix in Table 5 below shows the support status of each of the ADMS components during the 2025-30 period if this option is selected.

Table 5: ADMS Support Status (Option 0)

A large black rectangular redaction box covering the content of Table 5.

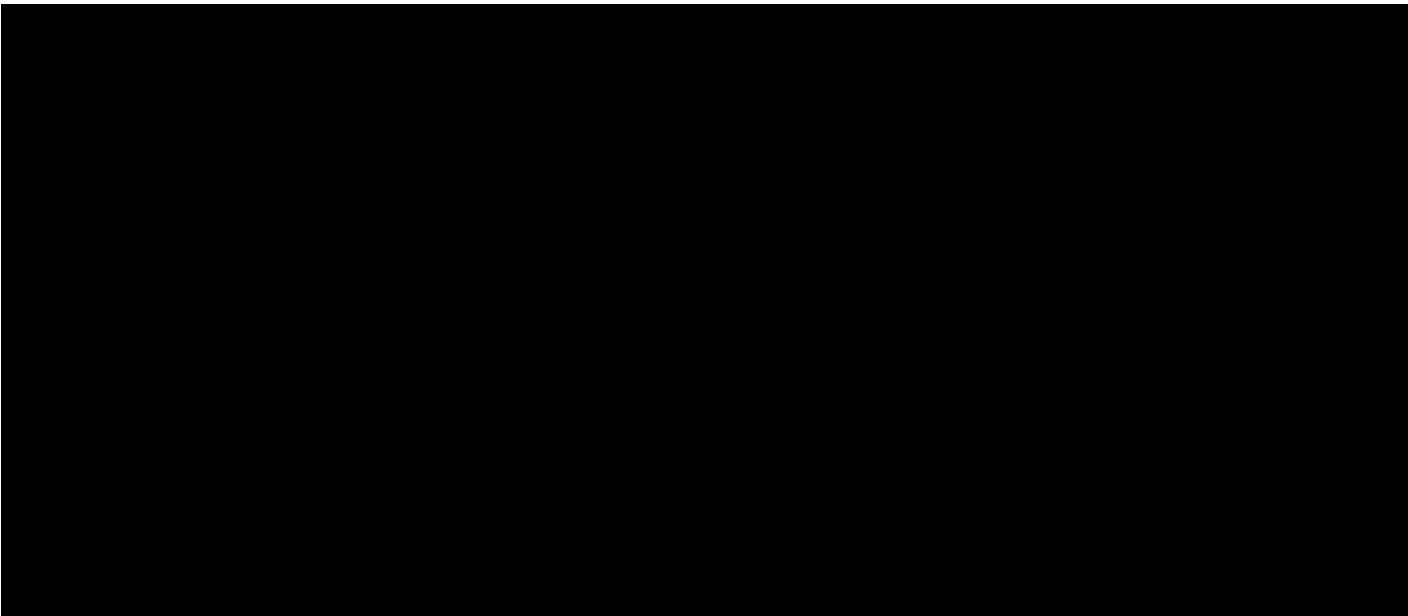
5.4.2 Costs

There is no capex associated with this option, however there is likely to be additional opex required to mitigate the increased risks associated with this option, which are summarised in Table 6.

5.4.3 Risks

Table 6 summarises the risks of not upgrading ADMS.

Table 6: Option 0 risk assessment summary

A large black rectangular redaction box covering the content of Table 6.

5.4.4 Disadvantages

SA Power Networks will be unable to take advantage of any product enhancements or new modules since it would be running an older version of the software which has ceased development. Any enhancements or development work would need to be funded at an increased cost and risk due to the age and supportability of an older version of the software.

5.4.5 Quantified benefits

Option 0 does not present any quantified benefits.

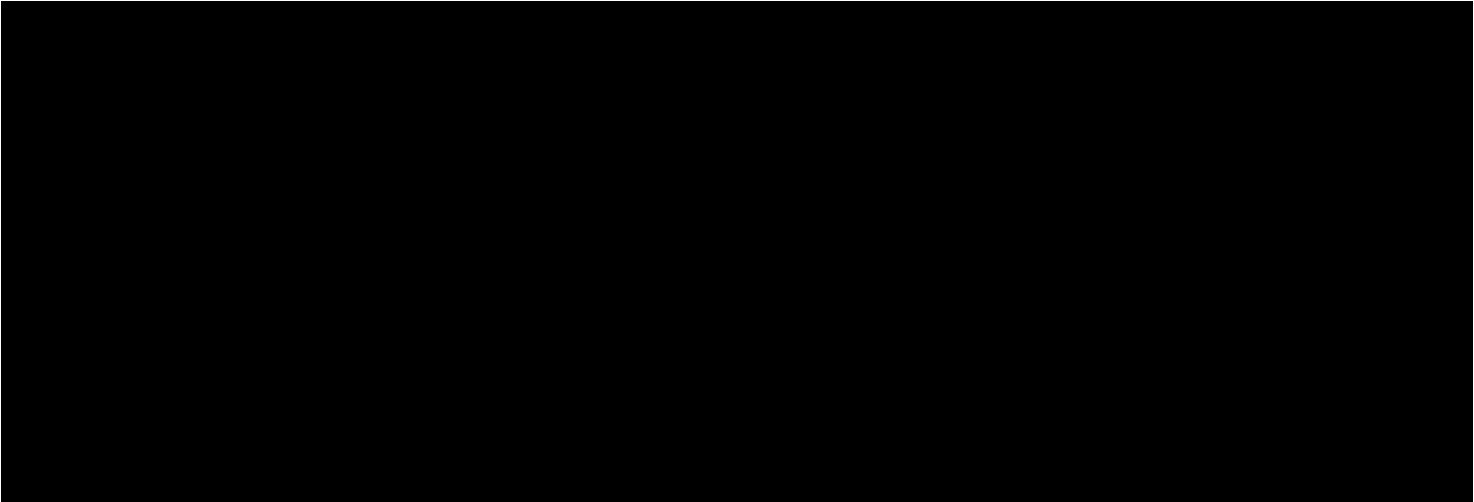
5.4.6 Unquantified benefits

Option 0 does not present any unqualified benefits. Under this option, SA Power Networks would be unable to take advantage of any product enhancements or new modules since it would be running an older version of the software which has ceased development.

5.5 Option 1 Upgrade the ADMS

5.5.1 Description

[Redacted text block]



5.5.2 Costs

Since we only recently implemented the ADMS and then added additional modules, our expenditure over the last two RCPs does not provide an accurate benchmark of the recurrent expenditure required to refresh the ADMS in the future. In view of this, we have estimated the upgrade costs bottom-up, based on our

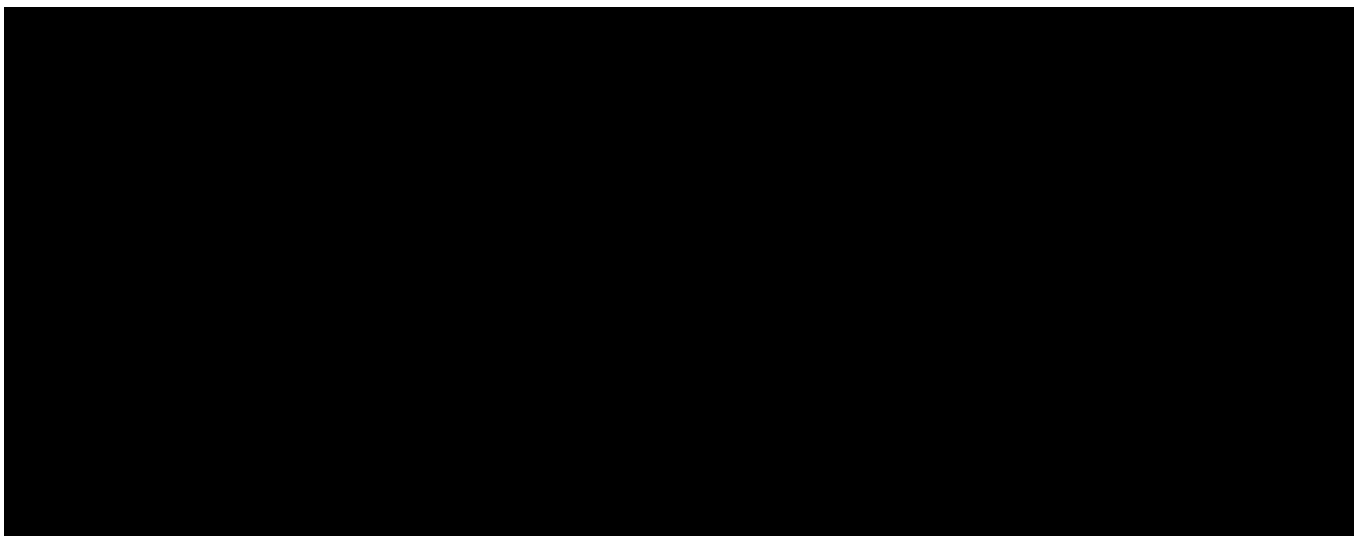
recent experience implementing the various ADMS components, and taking into account the efficiencies achieved through integration and consolidation of these components.

Table 8: Option 1 Total Cost by Cost Type (\$m Dec 2022 Real)

Cost Type	2025-26	2026-27	2027-28	2028-29	2029-30	Total 2025 - 30
Capex	2.82	12.37	11.07	0.87	0.87	28.00
Opex						
TOTAL COST	2.82	12.37	11.07	0.87	0.87	28.00

5.5.3 Risks

Table 9 summarises the residual risk after the ADMS is upgraded. Detailed risk assessment is provided in Appendix B.



5.5.4 Quantified benefits

Option 1 benefits have not been quantified.

5.5.5 Unquantified benefits

The driver for the update of the ADMS is to maintain existing capabilities and cyber security posture. This option will maintain existing capabilities and allow for future expansion of the system whilst maintaining vendor support.

The updated version of ADMS software may include capability enhancements that could provide a platform to support the implementation of the Future Network Strategy into the ADMS.

Incorporating the use of advanced modelling and forecasts can be used to identify network constraints that have the potential to adversely impact reliability, quality of supply and system security issues which are characteristics of multidirectional power flows.

6 Deliverability of recommended option

The proposed option (Option 1) is a continuation of the existing program of recurrent ADMS / OMS upgrades and replacements, which were successfully delivered in the 2020-2025 and earlier RCPs.

There is a stable ADMS support capability in place within SA Power Networks. Additional resources will be developed in-house through the recruitment and up-skilling of graduates working alongside experienced staff. We therefore do not foresee any issues with delivering this program of work over the 2025-30 RCP.

7 How the recommended option aligns with our engagement

7.1 Alignment to customer expectations

SA Power Networks is committed to ensuring that our business operations align with customer needs and priorities. By actively seeking input from stakeholders and customers, we ensure that decisions are informed by the needs and priorities of those they serve. This approach not only helps to improve customer satisfaction but also ensures that the company is well-positioned to adapt to changes in the energy landscape and emerging technologies.

7.2 Alignment to the views of other stakeholders

Customer engagement for the SA Power Networks 2025-2030 Reset largely consisted of a two part process. The first of these was a series of 'Focused Conversations' workshops with key stakeholders and customers, aimed at delving deeper into priority topics and gaining a better understanding customers' current needs and future priorities for electricity. The second component of the customer engagement program was a 'People's Panel' 2-day workshop. This was attended by a broad range of stakeholders providing a representation of the community, including businesses, renewables, youth, regional stakeholders, customer advocacy groups, local government representatives, and multicultural board members.

A significant focus of the Information and Communication Technology (ICT) component of these engagements was related to cyber security, with both panels recommending an uplift in investment relative to the current expenditure level. That the second engagement (People's Panel) outcome was to support a level of funding for SA Power Networks cybersecurity capability above expected legislated obligations in the 2025-30 RCP highlights the high importance that our customers attribute to cybersecurity health and mitigating these risks.

8 Alignment with our vision and strategy

SA Power Networks is a critical infrastructure provider and plays a vital role in powering South Australia. As the utilities model evolves and energy sources become more distributed, SA Power Networks is adapting to the changing landscape by incorporating new technologies and data-driven approaches to meet customer needs and optimize their operations. However, with the increasing reliance on technology comes the need for a strong cybersecurity posture to protect against cyber threats and ensure the safe and reliable operation of the electricity grid.

The SA Power Networks Digital and Data Strategy highlights a strong cyber security posture ('secure and resilient systems and data') as its critical enabler. With data being a core enabler across the business in achieving desired outcomes over the next regulatory horizons, the strategy acknowledges that a cybersecurity breach could have significant consequences not only for the company but also for the wider community.

9 Reasonableness of cost and benefit estimates

Cost and benefit estimates are derived from historical data from two RCPs from 2015 to 2025 and associated history.

10 Reasonableness of input assumptions

The main input assumptions used for this estimate are based on historical cost over the last ten-year period in relation to labour, materials and services. It is assumed that any changes in labour costs relative to historical levels are covered by input cost escalation.

Estimates also take into consideration the increased complexity and risk associated with the integration of the ADMS with external systems and the effort required to deploy and test against these integrations.

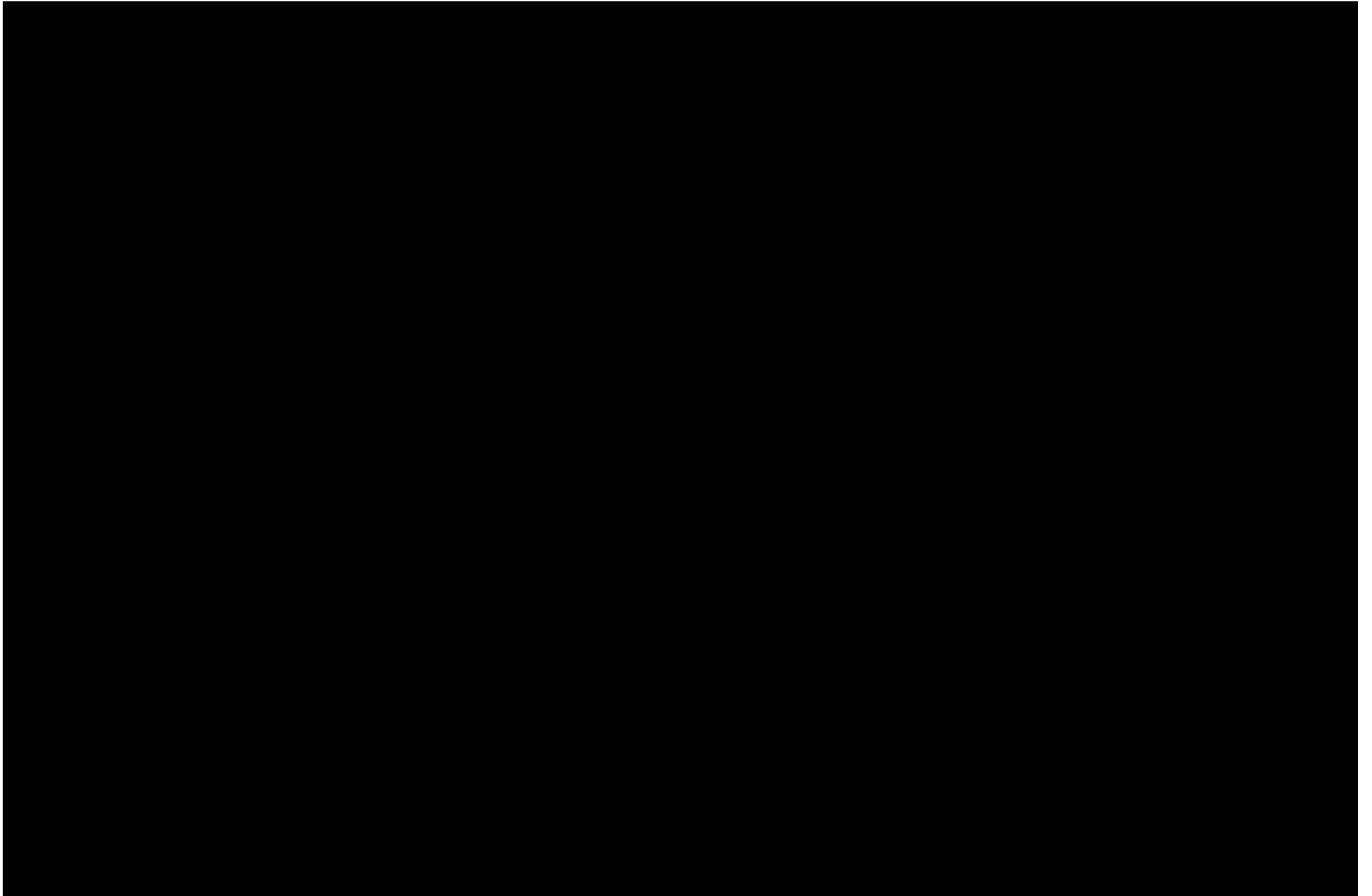
It is assumed that deployment of the ADMS solution will occur in a similar manner to previous deployments and will engage similar resource types.

A. Appendix A – cost models

High-level Options Analysis:

2025 - 30 Reset - Project-ADMS_Version_Upgrade-Option1.xlsm

2025 - 30 Reset - Project-ADMS_Version_Upgrade-Option2.xlsm





¹⁴ For each option, the overall risk level is the highest of the individual risk levels.