Business Case: Recurrent - Data, Analytics and Intelligent Systems Refresh

2025-30 Regulatory Proposal

Supporting document [5.12.8]

January 2024

SA Power Networks

Empowering South Australia

Contents

Glossary

Acronym / term	Definition
AI	Artificial intelligence
AER	Australian Energy Regulator
Capex	Capital expenditure
CER	Customer energy resources
DER	Distributed energy resources
DNSP	Distribution Network Service Provider
EDP	Enterprise data platform
ERP	Enterprise Resource Planning
GIS	Geographical information system
ICT	Information and communication technology
IT	Information technology
IoT	Internet of Things
NER	National Electricity Rules
NPV	Net present value
ODP	Operational data platform
Opex	Operating expenditure
RCP	Regulatory control period
Repex	Replacement expenditure
RIN	Regulatory Information Notice
SaaS	Software as a Service

1 About this document

1.1 Purpose

The purpose of this document is to provide the business case and justification for the ongoing recurrent refresh for SA Power Network's enterprise data management, analytics and intelligent systems for the 2025–30 Regulatory Control Period (**RCP**).

1.2 Expenditure category

- Non-network ICT Capex: Recurrent
- Non-network ICT Opex: Software as a service (**SaaS**) Base Year Adjustment

1.3 Related documents

Table 1: Related documents

Title	Author	Version / date
5.12.1 - IT Investment Plan 2025-30	SA Power Networks	Jan 2024
Digital and Data Strategy	SA Power Networks	Jan 2024
IT Asset Management Plan	SA Power Networks	Jan 2024
5.12.11 - Enterprise Data Warehouse Replacement & Consolidation Business Case	SA Power Networks	Jan 2024

2 Executive summary

This business case details the justification for the recurrent Information and Communication Technology (**ICT**) expenditure required to ensure that our enterprise data, analytics and intelligent systems and services are maintained and secure with the current acceptable levels of risk. These systems have been developed and expanded during the 2020–25 RCP, resulting in an uplift in the required expenditure levels compared to the current RCP expenditure.

Approximately $36 million in programs and operational demand has directly and indirectly implemented and progressively expanded these systems and services over the last five years. The key drivers for this expansion have been:

- Increasing demand for quality, integrated data to enable improved network asset related decision-making, forecasting and planning. Programs have increased both the volumes of asset data that is being collected and the sophistication of the analytical models used to improve our electricity network asset replacement forecasting, to optimise the efficiency of the customer dollar being spent.
- Enabling the energy transition through more effective decision-making and modelling for a constantly changing electricity grid, using near real-time data from smart meters and inverters.
- Rearchitecting of how we perform our reporting, driven by the implementation of replacement and upgrades across our key systems.
- Increasing cyber security and privacy requirements, driven by the *Security of Critical Infrastructure Act*, meant that we implemented new systems to govern and manage customer and network data.

This business case recommends a continuation of the current program to proactively refresh our systems using the current refresh rates across the expanded environment. The **2025–30 RCP forecast of $14.8 million**[1] recurrent expenditure for the program includes **$11.9 million in recurrent capital and $2.9 million of recurrent opex** (Table 2). This represents an increase of $3.4 million compared to the current five-year expenditure for these services as a result of the drivers detailed above. The opex component reflects an effective capex-opex substitution, to be handled as base year adjustment, as systems have shifted to cloud SaaS. Taking into consideration the avoided costs of risk, avoiding a gradual reduction of decision-making accuracy and efficiency, and avoiding a gradual return to more manual processes, the recommended option provides a net present value (**NPV**) of $4.6 million (10-year NPV)[2].

Another option considered was:

- **Investing at the current levels of recurrent expenditure:** While this level of investment does manage some risk (compared to no investment), it will result in increasing risk and costs over time, as our cyber risk increases and our data quality and decision-making capability decreases. The lower NPV of $1.5 million (10-year NPV) and higher overall risk profile reflects these lower customer outcomes.

The preferred option was selected because it:

- maintains our existing systems and services at the current acceptable levels of risk;
- secures our cloud-based data through appropriate levels of updates and patching;
- enables the required level of funding to respond to the market and business changes and to ensure customer service levels are maintained in a rapidly evolving environment;

[1] Unless otherwise specified, all financial figures in this business case are in real June 2022 dollars.
[2] Normally we do not expect a positive NPV for ICT Recurrent expenditure given the difficulty associated with monetising risk across a very large range of services and systems. However, given the contained scope and focus of these data systems and the relative recency of the investment then we can essentially model the gradual unwinding of this created value without ongoing investment.

- retains the value created by the non-recurrent programs; and
- facilitates good network and asset decision-making by facilitating the increasing need for quality-controlled and secured data.

Table 2: Options assessment summary, $million, June 2022[3]

	2025–30 costs			10-year estimates		Residual risk rating[4]
Option	**Capex**	**Opex**	**Total**	**Benefits**	**NPV[5]**	
Investing at current levels of expenditure (Base case)	8.2	2.9	11.1	25.1	1.5	**Medium**
Maintain existing levels of service with prudent expenditure (Preferred)	11.9	2.9	14.8	36.8	4.6	**Low**

[3] Note: Totals presented in tables throughout this document may not exactly match the sums of individual figures due to rounding.
[4] The overall risk level for each option after the proposed option implemented. Refer to Appendix C – Risk assessment for details.
[5] NPV of the proposal over 10-year cash flow period from 1 July 2025 to 30 June 2035, based on discount rate of 4.05%.

3 Background

1.1 The scope of this business case

The costs in this business case are those recurrent costs associated with managing risk and maintaining services that will be in place at 30 June 2025. This includes the costs of:

- security updates and patching;
- minor updates to maintain existing functionality and investment value;
- small upgrades where required to maintain system supportability; and
- minor enhancements to optimise our existing investments and keep pace with change (this includes changes to data models and reports).

As at June 2025, the data environment will consist of a set of applications, services and capabilities that govern data quality and security through the data lifecycle and then bring together the data from different systems for reporting, analytics and intelligent decision-making. Hence the primary focus of this business case is for systems and capabilities that govern, centralise and share, analyse, visualise and report data. The systems are divided into a number of functional groups.

Data governance and data lifecycle management systems

The focus of data governance is three-fold:

1. Ensuring our data is secure and meets our cyber security and privacy obligations as a Security of Critical Infrastructure provider.
2. Retaining the value we create when we do projects involving data.
3. Ensuring the future changes to data are targeted and deliver the most value for our customers and our services.

Our data cataloguing and data quality tools enable our data to be governed, controlled and appropriately shared. Lifecycle management also includes the systems that archive data securely.

Centralised database and content management

Some applications require individual data stores to enable specific business functions. Centralising the management of these databases allows improved management of the reliability and security of the data, as well as consolidating datasets where possible to reduce costs.

Enterprise data platform (EDP)

Data is generally created and stored within an individual application, where it is used for a particular function. However, understanding the full end-to-end customer service requires integrating selected data from applications into an enterprise data platform that allows data to be accessed and consumed across the organisation via tightly managed data models. For example, customer consumption data is matched to network operational data to build our network forecast models. These models are continually evolving due to both the large individual project changes and the continually evolving nature of our day-to-day decision-making in a rapidly changing environment.[6]

[6] There is a separate business case '5.12.11 Non-Network ICT Non-Recurrent: Enterprise Data Warehouse Replacement & Consolidation' which is concerned with significantly expanding the EDP by consolidating other systems into it. That business case assumes the capabilities and costs in this business case are already in place.

Operational data platform (ODP)

The management of large volumes of distribution-grid-based customer energy resources (**CER**) necessitated significant uplifts in our understanding of those resources on the grid, as well as our ability to model their impact and facilitate real-time decision-making regarding the operational network. Due to our cyber security requirements, this operational network data is kept separate from the rest of the data in the enterprise data platform, although summary versions are integrated into the EDP for holistic analysis purposes.

Data analysis, reporting and visualisation systems

These systems are designed to enable users to analyse the data in different ways (eg, statistical analysis) and visualise it via different means, such as in tables or as a layer on a Geographical information system (**GIS**) map. There are thousands of reports that get used across the organisation on a daily basis to assist in making the most appropriate decisions. These reports need regular updating and minor modifications as situations change and decision-making requirements continue to evolve.

Intelligent systems

This is a suite of systems that are primarily focused on machine learning and artificial intelligence (**AI**). These capabilities can be applied to our datasets to facilitate improved and/or more automated decision-making. For example, identifying asset faults from thousands of pictures of assets or from drone video is more efficiently done by a machine algorithm than a human. This will be an area of significant growth in the future as we seek to manage a much more complex network environment within the constraints of our regulatory allowance.

Out of scope

This business case does not include costs associated with:

1. major upgrades, large compliance changes or new or expanded capabilities
2. data systems that are specifically designated as a distributed energy resource (**DER**) under the AER definition of DER for Regulated Information Notification (**RIN**) reporting purposes.

1.2 Our principles for managing our data and related systems.

Our principles for managing expenditure for systems in this area are as follows:

- Having single sources of truth for all data, to maintain trust and integrity.
- Ensuring all our data is appropriately secured and managed in line with our Security of Critical Infrastructure and privacy legislated requirements.
- Integrating data into the shared central systems where it proves valuable to do so.
- Integrating data such that it is ‘store once, use multiple times’ – minimising our storage costs while maximising the value of the data.
- Given the fast-moving nature of analytics and AI systems, we engage in proofs of concept before committing to any systems, to more fully understand the capabilities, costs and benefits.
- While we have limited choice in the timing of upgrades and updates for some systems (eg, SaaS systems or for high-critically security patching), when we do have choice, we seek to implement a number of updates or upgrades together to minimise our testing and change costs.

3.3 Our performance to date

Table 3 summarises the key changes undertaken during the 2020–25 RCP.
Overall, our enterprise data systems increased significantly in terms of number and capability – essentially, from a couple of standalone legacy databases with limited usage to more modern integrated cloud capabilities that are used extensively across the whole business and will continue to be augmented and expanded into the future.

Table 3: Changes during the 2020–25 RCP

Data related applications functional groups	2020–25 RCP changes
Data governance and lifecycle management systems	Implemented an enterprise data governance capability, including a formal executive governance group to make effective decisions regarding data and data value. By 2025, the legacy data governance tools will be replaced with a single cloud-based solution.
Centralised database and content management	Commenced consolidation of the database and content management.
Enterprise data platform (data integration and sharing systems)	Implemented and iteratively built a new centralised enterprise data platform, including an enterprise data warehouse and data lake capability. Commenced integrating datasets related to customers, financial, assets, network operations and internet of things (**IoT**) data.
Operational data platform	Implemented a separate, highly secure data platform to analyse increased volumes of electricity network related data for near-real-time operational decision making.
Data analysis, reporting and visualisation systems	Replaced our legacy reporting tools and implemented enterprise reporting and visualisation systems. During 2020–25, these systems were migrated to the SaaS-based Microsoft Power BI platform. This created much greater capability for business personnel to access curated data and manage their own reports.
Intelligent systems	Commenced the implementation of machine learning and artificial intelligence systems, which are increasingly used for operational and strategic decision-making for electricity network assets.

3.4 Our 2020–25 RCP financial performance

Table 4 summaries the actuals/forecast for the 2020–25 RCP. The forecast expenditure is 11.4 million.

Table 4: Actuals/forecast for the 2020–25 RCP, $m, $ June 2022

Cost type	2020–21	2021–22	2022–23	2023–24 FC	2024–25 FC	Total 2020–25
Actual/forecast (FC)	1.2	2.4	3.4	2.3	2.1	**11.4**

The allowance was originally a component of the overall IT Applications Refresh Business Case for the 2020-25 RCP but was separated out from the general applications refresh given the increasing strategic importance of these systems. Associated downward adjustments were made in the IT Applications Refresh business case.

3.5 Drivers for change

Reliable quality and, increasingly, real-time data is fundamental to effectively and efficiently managing and running the modern electricity network, as well as to assisting customer energy management decision-making. Data is now managed as an 'asset', with customer, business, privacy and cyber security requirements driving more formal data-lifecycle management standards and approaches. This in turn enables:

- the significant increase in demand for reliable data to improve network asset management decision-making, particularly regarding which assets need to be fixed or replaced and when
- increasing the use of data to facilitate operational network and asset management decision-making, particularly relating to the impact and management of DER on the network
- increasing the reliance on IT systems and more automated decision-making to assist with the rapidly increasing complexity on the electricity network, and
- the increased demand for data to facilitate reporting across all business and customer functions, as we strive to deliver services in a more financially constrained environment.

During the 2020–25 RCP, data has become more central to the delivery of electricity services. As the energy transformation gathers pace, the use of data has been identified as a central enabler to both managing the grid and ensuring an effective and efficient energy transformation for our customers. Data will flow in parallel with the electricity to ensure the best outcome is achieved for the end customers. For SA Power Networks, this has meant not just collecting more data regarding assets to ensure the cost-effective planning and delivery of asset management services, but also starting to expose the functioning of the grid to key customers, for example, virtual power plants, to enable more informed energy management decisions. We expect much more of this in the future.

A number of the large programs that have driven change in this space are summarised below. The net effect of all of these changes was the fundamental redesign of our data landscape and particularly, implementation of the EDP and ODP. Our existing tools (eg, SAP BW data warehouse) proved wholly inadequate for the expanding requirements – particularly, being able to cost-effectively integrate multiple sources of data and delivering on the advanced analytical toolsets required. Hence, after a number of proofs of concept and cost analysis, a Microsoft-Azure-based data warehouse was implemented as the basis for the enterprise data capabilities.

Driving better network investment decisions

This program improved our ability to make better network investment decisions – particularly, replacement expenditure (**repex**) – using improved risk modelling and customer-value measures, and our ability to embed this in our day-to-day decision-making processes. As part of these activities, we needed to improve which data we collected at each stage of the asset-management lifecycle and to enable it to flow down the process to the next stage. This work will continue into the 2025–30 RCP.

Operational network management

Managing large volumes of distribution-grid-based DER necessitated significant uplifts in our understanding of those resources on the grid, as well as in our ability to model their impact and facilitate near-real-time decision-making regarding the operational network. Our DER Management program successfully developed world-leading flexible tariffs to enable customers to effectively participate in the energy transition. This relies on being able to integrate information from multiple sources including smart meters, inverters and the operational network to make the flexible tariff arrangements work. At the same time, there is a need to maintain a reliable and stable grid. Leveraging the increasing availability of smart meter and inverter data is part of the solution to that. Therefore, a secure ODP was created to integrate these multiple sources of

data and supply the information for both customer DER management and general operational network management.

Billing replacement

The Billing Replacement program replaced a large number of disparate legacy billing and market systems with modern software platforms, including updated national market data integration, data storage, data lake and analytical systems. These changes coincided with a significant increase in the demand for integrating the customer information with network-related information to help customers and the organisation manage the energy transition. The centralised data capabilities became a fundamental component of delivering our day-to-day services.

SAP ERP upgrade

The ERP upgrade to SAP S4 required us to reconsider and redesign our approach to financial analytics and reporting. Again, the shift was from legacy systems and approaches to more modern cloud-based systems.

3.6 Industry practice

The energy transition is driving an increased focus on the value of, and focus on, data as an asset for all utilities. Hence data-related proposals have been an increasing component of many submissions to the Australian Energy Regulator (**AER**). An example is Ausgrid's 2024–29 Regulatory Submission[7], which details the implementation, during the 2019–24 RCP, of their Big Insights Platform, which has an architecture very similar to our own. Likewise, the Essential Energy 2024–29 Submission details the commencement of a similar journey to create a data platform[8] to move towards near-real-time analytics and reporting.

The Australian Energy Security Board Data Strategy 2021[9] documents the critical and central role that data will play for all stakeholders and customers in enabling the energy transition. A number of programs of initiatives are being worked though, focused on the required capabilities at a national market level, which we have been working to enable internally – data governance, accessibility, sharing, visibility and delivering long-term value[10].

Internationally, data is also seen as a fundamental enabler of the energy transition. The United Kingdom initiated a national energy data taskforce, which resulted in a national Energy Digitalisation Strategy in 2022[11]. This strategy has become a key requirement for UK utility regulatory submissions.[12]
Distribution utilities have lagged other sectors in adopting and using data systems and practices. Hence the systems and processes have been rapidly evolving based on the reasonable practices and toolsets from other sectors. Our current practices and systems are in line with these approaches and entirely consistent with other distribution network service providers (**DNSPs**) in Australia. These will continue to evolve over time.

[7] Ausgrid – Att. 5.9.f – Data & analytics program – 31 Jan 2023 – Public.pdf (aer.gov.au)
[8] Essential Proposal | Australian Energy Regulator (aer.gov.au)
[9] Energy Security Board: Data Strategy Final Recommendations July 2021
[10] ESB-data-services-delivery-model-consultation-paper-december–2022.pdf
[11] Energy Data Taskforce | A Modern Digitalised Energy System (catapult.org.uk)
[12] BEIS, Ofgem and Innovate UK Statement on the Energy Digitalisation Taskforce Report | Ofgem

4 The identified need

The underlying driver for investment action to be considered in this business case is the maintenance of our existing levels of service through the ongoing mitigation of risks associated with the failure or performance degradation of data related systems, due to being past their useful life, unsupported or not effectively secured from cyber threats. The risks occur at both the application level and with data models contained within those applications - meaning the data is no longer reliable, trusted nor effectively governed. In addition, we need to be able to continue to respond and adapt to ongoing small to medium changes required in providing information relevant to customer requests and changing needs.
Consequences of these risks include:

- Being unable to correctly identify life-support customers impacted by network changes.
- Ineffective network operational decisions leading to network outages.
- Ineffective network asset decisions leading to increased costs to customers.
- Being unable to supply customer information requests.
- Unauthorised customer data sharing.
- Loss of trust in the data resulting in increased costs due to workarounds.
- Loss of long-term investment value in our systems.

In considering potential responses to this driver, we 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 this refresh program is as follows:

a. To respond to customers' concerns[13], identified through our consumer and stakeholder engagement process, regarding their explicit service level recommendations that we:
   - maintain reliability service performance – driven by a desire to not see outages
   - maintain safety service performance – driven by a desire to not see vulnerable customers impacted by changes
   - ensure customer data is kept safe and effectively governed
   - ensure our network asset decisions are data driven and as efficient as possible.

b. To ensure that our services are able to continue to be delivered for the lowest possible long-term cost – through prudent, systematic, and timely refresh of assets suffering breakage or degradation in performance. This includes extending useful life beyond recommended refresh cycles, where prudent and appropriate to do so.

[13] This is pursuant to Clause 6.5.7(c)(5A) of the NER, which requires regard to be had to the extent to which forecast expenditure seeks to address the concerns of distribution service end users identified by the distributor's engagement process.

5 Comparison of options

5.1 The options considered

Table 5 summarises the options considered and costed for this investment.

Table 5: Summary of options considered

Option	Description
Option 1 – Maintain existing levels of expenditure	This option involves maintaining our recurrent expenditure levels at the actual/forecast levels for the 2020–25 RCP. In effect, this option does not take into account that new or expanded capabilities have been implemented during the RCP and so this option will result in an increasing risk profile over time. This option assumes a changed nature of expenditure – from capex to opex - for the applications that have been shifted to the SaaS systems.
Option 2 – Maintain existing levels of service with a prudent level of expenditure	This option involves maintaining our existing service levels and risk by investing at an increased level (compared to the current RCP) but one that reflects the prudent management of the larger number of data-related systems and capabilities that have been implemented during the RCP. This option also assumes a changed nature of expenditure – from capex to opex - for the applications that have been shifted to the SaaS systems.

5.2 Options investigated but deemed non-credible

The Do-Nothing Option was considered but deemed non-credible because:

- the services would become unusable during the RCP as the changing technical environment causes some systems to stop functioning without ongoing updates and upgrades
- the chances of a cyber security incident would increase dramatically over time due to the lack of security patching on the systems.

Although it was not a credible option, for risk monetisation purposes we did cost a ‘Do Nothing’ base case option to enable easier comparison between the different ‘Do something’ options.

5.3 Analysis summary and recommended option

Options assessment results

Table 6 summarises the costs, benefits and risks for the options considered.

Table 6: Costs, benefits and risks of alternative options relative to the base case over the 2025–30 RCP, $m, June 2022

Option	10-year program costs			2025–30 program costs			10-year risk monetised benefits[14]	10-year NPV[15]	Overall risk rating[16]	Ranking
	Capex	Opex	Total	Capex	Opex	Total				
Option 1 – Maintain existing levels of expenditure	17.5	6.0	23.5	8.2	2.9	11.1	25.1	1.5	Medium	2
Option 2 – Maintain existing levels of service and risk with a prudent level of expenditure	25.4	5.9	31.4	11.9	2.9	14.8	36.8	4.6	Low	1

Assumptions

Both options assume $2.9 million of opex, to be handled as a base year adjustment. Both options assert that this shift is necessary due to the fact that the reporting and governance are now SaaS cloud based and hence require opex to manage updates and refreshes.

5.4 Recommended option

Option 2 is the recommended option, with a total expenditure of $14.8 million, being $11.9 million of capital and $2.9 million of opex (as a base year adjustment). Option 2 has a higher cost but has a better NPV when risk reduction benefits are taken into account, as well as much lower residual risk.

This option is the only option that secures and enables the new capabilities that have been implemented during the 2020–25 RCP.

- This option maintains our existing systems and services at the current acceptable levels of risk.
- It secures our cloud-based data systems through appropriate levels of updates and patching.
- It enables the required level of funding to respond to the market and business changes and to ensure customer service levels are maintained in a rapidly evolving environment.
- It retains the value created by projects by enabling ongoing data governance capabilities.
- It facilitates the increasing consumption and use of reliable data to drive evidence-based decision-making.

[14] Represents the total capital and operating risk reduction over the 10-year cash flow period from 1 July 2025 to 30 June 2035 expected across the organisation as a result of implementing the proposed option, when compared with Doing Nothing.
[15] NPV of the proposal over 10-year cash flow period from 1 July 2025 to 30 June 2035, based on discount rate of 4.05%.
[16] The overall risk level for each option after the proposed option implemented. Refer to Appendix C – Risk assessment for details.

5.4.1 Option 1 – Maintain existing levels of expenditure

Description

As detailed in the sections above, data has become an increasingly strategic asset, resulting in an increase in the number of systems required to manage, analyse and report on data.

This option considers the scenario that a similar level of total expenditure is carried forward into the 2025–30 RCP.

Under this scenario, the existing level of investment is divided across a larger number of applications, which means any given application is receiving less over time. This is also equivalent to the situation where the applications implemented during 2020–25 are receiving very limited or no investment.

5.4.2 Costs

Table 7 details the five-year costs for Option 1. A more detailed breakdown for each application subset is provided in the associated costing spreadsheet listed in Appendix A – Cost models.

The $11.1 million is equivalent to the current forecast for the 2020–25 RCP of $11.4 million (Table 7).

Table 7: Option 1 – Costs by cost type ($m June 2022)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Capex	1.1	2.0	1.9	1.6	1.6	8.2
Opex	0.6	0.6	0.5	0.6	0.6	2.9
Total	**1.7**	**2.6**	**2.3**	**2.2**	**2.2**	**11.1**

Additional detail on the opex base year adjustment is provided in Appendix B – Opex base year adjustment (Preferred option).

5.4.3 Advantages of Option 1

This is the lowest cost option.

The most critical activities will be undertaken to ensure a level of security and refresh across the applications.

5.4.4 Disadvantages of Option 1

- Over time our risks will increase, as we will be servicing an increased portfolio of systems with the same levels of investment. This will result in increased vulnerabilities – while high-priority cyber security patching and updates will be done, lower priority will likely not – which increases the overall security risk over time.
- The thinner spread of the existing investment will mean a large increase in 'firefighting' problem fixing, rather than focusing on the quality of the data, extracting the most customer value we can from the data we collect, and ensuring the most efficient ongoing consumption of that data. In effect, this is a significant opportunity cost associated with this option.
- Over time, we also expect an increase in costs due to the increase in manual workarounds needed as the data models become more unreliable and less trusted. One impact is an increase in reporting time,

as people engage in manual merging and calculations rather than relying on the central systems. Additionally, manual workarounds significantly increase the likelihood of incorrect data being used for business-critical purposes such as regulatory reporting, leading to potentially very large impacts to the business and the sector.

- As the data models are not maintained at the required levels, the decision-making effectiveness for electricity network assets will reduce over time.
- We will be unable to respond effectively to the continued rapid evolution of the data and data-services requirements. We expect continued growth in dependence on, and performance from, our enterprise data services, as the energy transition progresses and reliable real-time data becomes more critical to our network, business and customer decision-making.

5.4.5 Risks

The high-level risks of Option 1 are summarised in Table 8.

Overall, the highest risks are created because we are unable to effectively maintain the full portfolio of applications to the appropriate level. The principal risks are related to the following:

1. The financial opportunity cost associated with an expected reduction in decision-making effectiveness for network assets.
2. The increased costs associated with the manual workarounds and reporting.
3. The increased risk of cyber security breaches as the systems will not be secured to the same level.

Table 8: Option 1 – Risk assessment summary

Risk consequence category	Residual risk level – Option 1[17]	Residual risk level – Do nothing
Safety – Harm to a worker, contractor or member of the public	Medium	High
Performance and growth – Financial impact	Medium	High
Governance – Non-compliance with regulatory obligations	Low	Medium
Customers – Failure to deliver on customer expectations	Low	Medium
Network – Failure to transport electricity from source to load	Medium	High
Technology and data – Unauthorised access, modifications or control of systems	Medium	Medium
Technology and data – Unauthorised access or disclosure of information	Medium	Medium
Technology and data – Disruption of access to or use of systems	Medium	Medium
Overall risk level	Medium	High

Overall, the risk is rated as Medium as some risks are managed (compared to no expenditure) but only to a moderate level. These risks will systematically increase over time as our systems become less supported and more vulnerable, and the data less trusted.

The detailed option risk scenario analysis is provided in Appendix C – Risk assessment.

5.4.6 Risk reduction benefits

Table 9 summarises the estimated risk monetised cost avoidance benefits associated with Option 1. For modelling purposes, these benefits are set against an option of 'no expenditure' and hence reflect the benefits of this option compared to doing nothing.

[17] The level of risk post current controls (i.e. after considering what we currently do to mitigate the risk).

Providing a level of ongoing investment does deliver an ongoing level of risk management and retention of investment value, but these benefits are lower than that provided by Option 2.

Table 9: Option 1 – 10-year risk reduction benefits ($m June 2022)

Risk consequence category	Benefit/risk cost avoidance or reduction	10-year estimates
Safety	Avoided increase in chances of harm to a life-support customer	4.0
Performance and growth	Avoided reduction in investment efficiency	9.5
Performance and growth	Avoided reversion to manual processes	8.7
Performance and growth	Avoided inaccurate regulatory reporting	1.9
Technology and data	Avoided cost of data breach	1.1
	Total	**25.5**

The estimates reflect the following:

1. The EDP is fundamental to the management of life-support customers and network decision-making regarding life-support customers. Therefore, continuing to invest in the EDP assists in avoiding likely harm to life-support customers. We have assumed potential minor harm to a customer. The costs of the investigation and remediation usually end up being around $1 million per incident.
2. Reductions in our network investment efficiency – as the applications are not maintained and the quality of our data and systems reduces over time, this leads to ineffective and inefficient decision-making and asset delivery. We have assumed only a very conservative value (0.01% pa) increased inefficiency across a conservative estimate of $124 million in the Network Assets portfolio per annum. However, this inefficiency factor is expected to increase each year as the data becomes more inaccurate and the systems less trusted.
3. Increases in manual processing time, as our reporting systems and data models gradually degrade over time resulting in both loss of trust in the data and a gradual reversion to manual reporting processes across the organisation. Compared to a baseline of no expenditure, Option 1 is expected to result in some voidance of these costs as the core models are receiving some investment, but it will not be as effective as Option 2.
4. The EDP and ODP becoming sources of trusted information for regulatory reporting. Reducing investment over time means the reliability of the reporting goes down and the cost to report goes up. Given the expansive nature of the various reporting mechanisms and the numbers of people involved, we have put a value of about $180 thousand per annum on the reporting accuracy.
5. The avoided cost of a cyber security breach and associated recovery time. This option assumes a lower avoided cost than Option 2, assuming a cyber security breach happens once in five years vs once in every 15 years for Option 2. The costs include a short downtime for system users and are mainly those associated with systems recovery and the reverification of the data and associated reporting, estimated at $360 thousand per event.

5.5 Option 2 – Maintain existing levels of service with a prudent level of expenditure

5.5.1 Description

This option provides for an increased level of investment commensurate with the increased number and complexity of the applications delivering this capability.

This investment manages the risks across the systems, while allowing a level of evolution across the systems to continue to respond to the rapidly changing data requirements.

5.5.2 Costs

Table 10 summarises the investment required for the RCP, being $11.9 million of capex and $2.9 million of opex, totalling $14.8 million.

Table 10: Option 2 – Costs by cost type ($m June 2022)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Capex	1.7	3.0	2.7	2.2	2.4	11.9
Opex	0.6	0.6	0.5	0.6	0.6	2.9
Total	**2.3**	**3.6**	**3.2**	**2.8**	**3.0**	**14.8**

Additional detail on the operating expenditure base year adjustment is provided in Appendix B.

5.5.3 Advantages of Option 2

This option effectively deals with the risks detailed for Option 1, resulting in a lower overall residual risk profile.

5.5.4 Risks

Table 11 summaries the risks for Option 2. The residual risk level is determined to be Medium – reflecting the lower overall cyber security and safety-related risks, as well lower risks associated with data loss, data quality reductions and non-compliance.

Table 11: Option 2 – Risk assessment summary

Risk consequence category	Residual risk level – Option 2[18]	Residual risk level – Do nothing
Safety – Harm to a worker, contractor or member of the public	Low	High
Performance and growth – Financial impact	Low	High
Governance – Non-compliance with regulatory obligations	Low	Medium
Customers – Failure to deliver on customer expectations	Low	Medium
Network – Failure to transport electricity from source to load	Low	High
Technology and data – Unauthorised access, modifications or control of systems	Low	Medium
Technology and data – Unauthorised access or disclosure of information	Low	Medium
Technology and data – Disruption of access to or use of systems	Low	Medium
Overall risk level	Low	High

[18] The level of risk post current controls (i.e. after considering what we currently do to mitigate the risk).

The detailed option risk scenario analysis is provided in Appendix C.

5.5.5 Risk reduction benefits

Table 12 summarises the estimated cost-avoidance benefits associated with Option 2.

Table 12: Option 2 – 10-year risk reduction benefits ($m June 2022)

Risk consequence category	Benefit/risk cost avoidance or reduction	10-year estimates
Safety	Avoided increase in chances of harm to a life-support customer	4.0
Performance and growth	Avoided reduction in investment efficiency	11.7
Performance and growth	Avoided reversion to manual processes	17.1
Performance and growth	Avoided inaccurate regulatory reporting	2.6
Technology and data	Avoided cost of data breach	1.5
	Total	**36.8**

The estimates reflect the following:

1. The EDP is fundamental to the management of life-support customers and network decision-making regarding life-support customers. Therefore, continuing to invest in the EDP assists in avoiding likely harm to life-support customers. We have assumed potential minor harm to a customer. The costs of the investigation and remediation historically end up being around $1 million per incident.
2. Reductions in our network investment efficiency – as the applications are not maintained and the quality of our data and systems reduces over time, this leads to ineffective and inefficient decision-making and asset delivery. In this option, we have assumed there is no inefficiency factor creeping in because the data and systems are effectively maintained going forward.
3. Reliable, trusted data sources mean more automated and trusted reporting – hence an avoidance of manual processing time. We assumed two different levels of report users – basic and advanced – with advanced users tending to spend a lot more time manual processing data if they do not trust it. We assumed basic users would waste about 15 minutes per month to start with (a very conservative number) and this would increase by an additional 15 minutes per month each year going forward, as they trust the data less. For advanced users, we assumed they would waste about three hours per month, with increases each year as well. Compared to a baseline, Option 2 has more avoidance benefits.
4. The EDP and ODP are becoming sources of trusted information for regulatory reporting. Reducing investment over time means the reliability of the reporting goes down and the cost to report goes up. Give the expansive nature of the various reporting mechanisms and the numbers of people involved, we have put a value of about $180 thousand per annum on the reporting accuracy.
5. The avoided cost of a cyber security breach and associated recovery time. The costs include a short downtime for system users and are mainly those associated with systems recovery and the reverification of data and associated reporting, estimated at $360 thousand per event. For Option 2, we assumed the breach happens once every 15 years versus once every five years for Option 1.

6 Deliverability of recommended option

This IT Recurrent Business Case represents an incremental increase on the current levels of expenditure, with the majority of this expenditure already being incurred. The existing teams will ramp up and down to reflect the variations in work on a year-to-year basis. There are no anticipated barriers to deliverability.

This expenditure reflects the base expenditure to refresh these services. Larger program and projects assume this expenditure is in place.

7 How the recommended option aligns with our engagement.

From a customer engagement perspective, Option 2 – 'Maintain existing levels of service with a prudent level of expenditure' was included as the preferred option in 'Scenario 1: Basic' for all our costing models. There was no specific discussion on this business case, consistent with all IT recurrent expenditure business cases.

8 Alignment with our vision and strategy

Our Digital & Data Strategy outlines the long-term strategic direction for ICT. The focus of the strategy is on the provision of efficient and reliable core systems, and a range of digitisation that ensures our workforce has appropriate skills for the technology implemented. A high-level view of our Digital & Data Strategy is depicted in Figure 1.

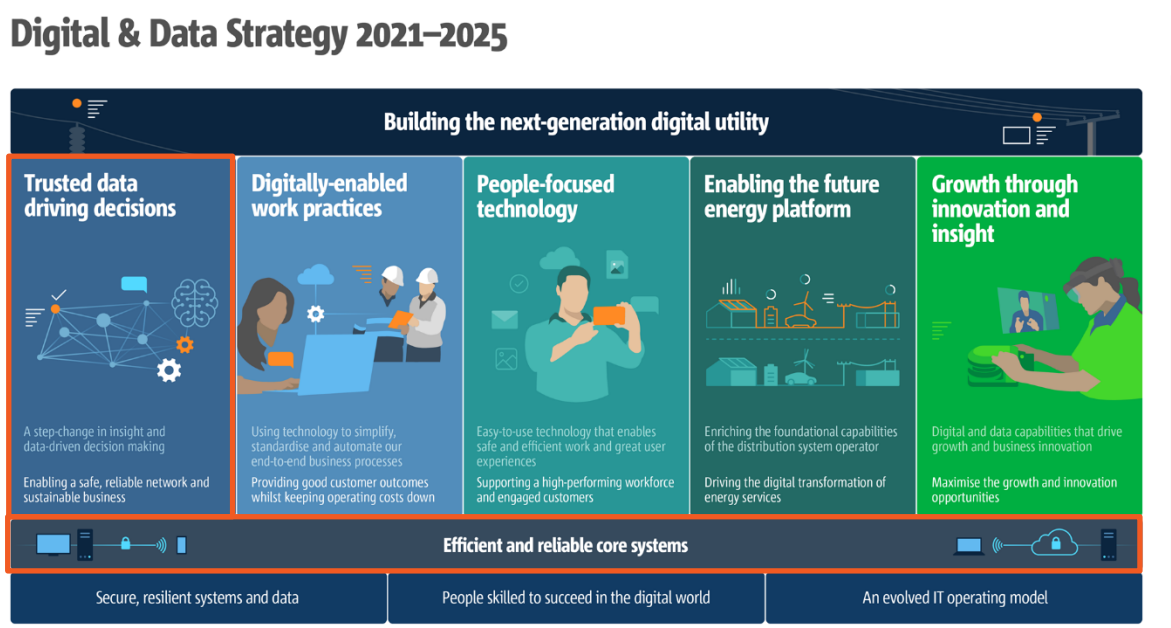

Figure 1: Digital & Data Strategy 2021–2025

The importance of the strategic role that data has in the ongoing delivery of network and customer service services is highlighted by:

1. Our key information technology strategy is now called the Digital & *Data* Strategy.
2. The role of trusted, governed and cost-effective data in customer services is our primary objective for the Digital & Data Strategy 2021–2025. '*Trusted data driving decisions*' aims to deliver a step-change in data-driven decision-making. This objective underpins all other objectives on the strategy.

The investment in this document is to enable the capabilities implemented as part of this objective to be sustainably managed, secured '*Efficient and reliable core systems*'.

9 Reasonableness of input assumptions and cost estimates

The costs are based on:

1. the list of systems that we have already implemented or are currently working to implement by 1 July 2025 and which will need some level of security updates and refresh during the 2025–30 RCP;
2. the levels of activity to refresh and enable these systems, based on past experience of those systems, as well as estimates based on systems with similar complexity to those newer systems; and
3. the frequency of updates and refreshes, based on the principles laid out in our IT Asset Management Plan, which includes factors such as the degree of cyber security exposure, the criticality of the system to our business services, and the frequency of the refresh rates mandated by suppliers to maintain required levels of ongoing support.

A. Appendix A – Cost models

- Data Analytics and Intelligent Systems estimate - Option 1 (Maintain existing spend).xlsm
- Data Analytics and Intelligent Systems estimate - Option 2 Preferred (Maintain existing risk).xlsm

B. Appendix B – Opex base year adjustment (Preferred option)

Table 13: Opex Base Year Adjustment ($m June 2022)

Category	Application function	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Base Year Adjustment	Analytics, reporting and visualisation systems	0.5	0.5	0.4	0.5	0.5	2.3
	Data governance systems	0.1	0.1	0.1	0.1	0.1	0.5
	Total opex base year adjustment	**0.6**	**0.6**	**0.5**	**0.6**	**0.6**	**2.9**

Table 14: Capex – Opex substitution

Topic	Detail
Background	During the 2020–25 RCP, key reporting capabilities migrated from onsite to SaaS cloud-based services. This includes Microsoft Power BI and part of SAP reporting (to SAP Analytics Cloud) and the Informatica data governance tool. Based on the accounting rule changes, the activities undertaken to refresh these systems, manage the data models and provide small refreshes on the reports are classified as opex.
Request	An opex base year adjustment of $2.9 million.

C. Appendix C – Risk assessment

				Residual risk (Do nothing)			Residual risk (Option 1)			Residual risk (Option 2		
ID	**Risk scenario**	**Consequence description**	**Consequence category**	**Consequence**	**Likelihood**	**Risk level**	**Consequence**	**Likelihood**	**Risk level**	**Consequence**	**Likelihood**	**Risk level**
1	Inaccurate or inconsistent data and reports lead to incorrect or inefficient investment decisions, or to information reported to external stakeholders being incorrect or unavailable. The enterprise data systems form the core components of the organisational risk cost modelling capability – allowing the integration of data from different sources to target all of the electricity network asset investments based on risk and customer benefit.	Relatively quick degradation in quality of the data will impact work prioritisation, planning and scheduling. This will lead to loss of trust in the data, with staff engaging in workarounds to validate the data so they can trust it, as well reverting to significant manual reporting efforts to generate the required reports on a daily, weekly or monthly basis. Significantly reduced business efficiency as staff increase the time spend on sourcing, compiling and reporting on data.	**Performance and growth –** Financial impact	3	5	**High (8)**	3	3	**Medium (6)**	3	2	**Low (5)**
		Quality of the investment decisions will reduce: assets will be replaced when they shouldn't have been, outages will be created by assets that should have been replaced but weren't.	**Performance and growth –** Financial impact	3	5	**High (8)**	3	3	**Medium (6)**	3	2	**Low (5)**

		Network – Failure to transport electricity from source to load	3	5	High (8)	3	3	Medium (8)	3	2	Low (5)
	Network outage management teams unable to identify, notify and maintain reliability of supply to critical and life-support customers. There are potentially catastrophic consequences associated with not being able to identify critical and life-support customers.	**Safety –** Harm to worker, contractor or member of the public	4	3	High (7)	4	2	Medium (6)	3	2	Low (5)
	SA Power Networks unable to manage electric-shock reporting and impacts leading to potentially catastrophic safety consequences, complaints, penalties from regulators and aggrieved party legal actions.	**Financial impact –** Litigation and/or penalties	3	3	Medium (6)	3	2	Low (5)	3	2	Low (5)
		Customers – Failure to deliver on customer expectations	3	3	Medium (6)	3	2	Low (5)	3	2	Low (5)
		Safety – Harm to worker, contractor or member of the public	4	3	High (7)	4	2	Low (5)	4	2	Low (5)

		Potential compromise of ability to generate accurate regulatory and reliability reporting, which is heavily dependent on enterprise data systems.	**Customers –** Failure to deliver on customer expectations	3	3	Medium (6)	3	2	Low (5)	3	2	Low (5)
			Financial impact – Litigation and/or penalties	3	3	Medium (6)	3	2	Low (5)	3	2	Low (5)
			Governance – Non-compliance with regulatory obligations	3	3	Medium (6)	3	2	Low (5)	3	2	Low (5)
2	Data systems are hacked due to unpatched cloud-based systems. The vulnerability of cloud systems to security breaches is related to its security configuration and encryption levels, and whether regular security patching is being applied regularly. Part of the nature of cloud systems is that suppliers add features or update configurations on a regular basis and it is up to the user to test that the changes do not create vulnerabilities.	A successful cyberattack could result in staff locked out of systems and a ramson demanded for release. This could compromise critical operational control systems, impacting reliability of supply. It could also result in theft of confidential customer and network data, resulting in the publication or sale of that information on the dark web. SA Power Networks could also expect financial loss from fines, as well as loss of reputation and adverse media, along with Regulator and aggrieved party legal actions.	**Technology and data** – Disruption of access to, or use of, systems	3	3	Medium (6)	3	3	Medium (6)	3	2	Low (5)
			Performance and growth – Litigation and/or penalties	3	3	Medium (6)	3	3	Medium (6)	3	2	Low (5)
			Safety – Harm to worker, contractor or member of the public	3	3	Medium (6)	3	3	Medium (6)	3	2	Low (5)

			Technology and data – Unauthorised access, modifications or control of systems	3	3	Medium (6)	3	3	Medium (6)	3	2	Low (5)
			Technology and data – Unauthorised access or disclosure of information	3	3	Medium (6)	3	3	Medium (6)	3	2	Low (5)
			Overall risk level[19]			High			Medium			Low

[19] For each option, the overall risk level is the highest of the individual risk levels.