Business case: ICT Non-Recurrent - Integration Platform Replacement

2025-30 Regulatory Proposal

Supporting document 5.12.12

January 2024

SA Power Networks

Empowering South Australia

Contents

Glossary

Acronym / term	Definition
AEMO	Australian Energy Market Operator
Capex	Capital expenditure
DNSP	Distribution network service provider
GIS	Geographic information system
ICT	Information and communication technology
NEM	National Electricity Market
NPV	Net present value
NMI	National meter identifier
Opex	Operating expenditure
RCP	Regulatory control period
SAP PO	SAP Process orchestration
SMS	Short Message Service

1. About this document

1.1 Purpose

This document details the justification for non-recurrent Information and communication technology (**ICT**) expenditure to deliver a replacement of our core integration platform software, which will reach end of life in the 2025–30 Regulatory Control Period (**RCP**). This integration software provides business and network critical connectivity and data sharing capabilities, including third-party systems such as market systems managed by the Australian Energy Market Operator (**AEMO**).

1.2 Expenditure category

- Non-network ICT capital expenditure (**capex**): Non-recurrent – major replacements or upgrades.

1.3 Related documents

Table 1: Related documents

Title	Author	Version / date
5.12.1 - IT Investment Plan 2025-30 - Asset Plan	SA Power Networks	Jan 2024
Digital and Data Strategy	SA Power Networks	Jan 2024
IT Asset Management Plan	SA Power Networks	Jan 2024

2. Executive summary

This business case details the justification for non-recurrent ICT expenditure to deliver a replacement of our core integration platform software. This integration software provides connectivity and data-sharing capabilities between critical business systems, and therefore supports highly secure, real-time customer, market and business critical capabilities. This includes integration with the AEMO market systems, which enables SA Power Networks to fulfil our obligations within the National Electricity Market (**NEM**). Simply put – all of our customer, network billing and asset data flows through this platform. However, our current platform software is no longer being updated and will go out of mainstream support in December 2027, with support ceasing completely in 2030. This recommendation seeks to maintain our existing customer and business services and risk level by ensuring that our core integration platform is fit for purpose, secure and reliable.

Secure transfer of customer data is a key requirement of our integration platform. This includes connectivity between our operational and business systems for customer notifications, call-centre interactions, customer billing, outage management, and critical life-support information. Secure, reliable, real-time integration with no downtime is also critical to service delivery for many of our customer-facing services. This includes field crew appointments/availability/allocation; service orders, including customer meters (reading, connects, disconnects); banking; Short Message Service (**SMS**) outage notifications; Geographic information system (**GIS**) mapping services; and customer information used to log outages. This technology also ensures secure connectivity between SA Power Networks and third parties, such as local, state and federal governments.

Our integration platform is currently provided by SAP Process Orchestration (**SAP PO**) and SAP Data Services technology. We have been advised that standard vendor support for both of these products will stop as of December 2027. Extended support will be available between 2027 and 2030 at an additional cost; however, regular updates will cease, and security patching will be available only for critical issues. After 2030, no support will be available.

This business case recommends both migrating and replacing our current integration platform during the 2025–30 RCP. This includes migrating SAP PO to the SAP Integration Suite and replacing SAP Data Services with SAP Data Intelligence and Microsoft Azure Data Factory by December 2027. This solution supports services we use currently, while ensuring a long-term stable and secure environment. The total expenditure for this preferred option **is $13.0 million in capex.**[1] The overall residual risk rating is Medium.

Other options we considered are:

- Not replacing our Integration systems (i.e., 'Do nothing')
- Alternative vendor integration products
- Extended support until the end of 2030, and then negotiating alternative support arrangements beyond 2030.

The preferred option has been selected because it provides for the continued support and security of our core integration platform, as well as continuity of critical business services, at the lowest long-term cost to customers. It ensures we can continue to meet our Critical Infrastructure and Energy Market obligations. In addition:

- It provides the least risk option to migrating, as we can use existing tools to assist us with the transition, and we are already using them and are therefore familiar with the new integration products (SAP Integration Suite).
- It reduces complexity by minimising the number of integration products and customisation required.

[1] Unless otherwise specified, all financial figures in this business case are in real June 2022 dollars.

- It removes the potential implications of using extended/alternative support, including:
  - reduced real-time support of integrations for life-support processes;
  - reduced real-time support of integrations to externally facing NEM systems; and
  - significant support risk that would impact customer-facing services or customer data.

With the ongoing need for new, increasingly complex data sharing between disparate solutions, not replacing our integration platform will increase the risk of our critical business processes failing. This will likely result in some of our services and core functions becoming unavailable during the period. The chances of a cyber security incident will also increase dramatically over time due to the lack of security patching on the systems, with older style integrations not being supported.

Table 2: Non-recurrent expenditure options assessment summary relative to the Option 0 – Base case, $million, Jun 2022 real[2]

	Total program costs			2025–30 costs			Program or 10-year estimates		Residual risk rating[3]
Option	**Capex**	**Opex**	**Total**	**Capex**	**Opex**	**Total**	**Benefits**	**NPV[4]**	
Option 0 – Do nothing (Retain existing integration systems)[5]	-	-	-	-	-	-	-	-	**Extreme**
Option 1 – Staggered deployment of SAP solution in the 2025–30 RCP	13.0	-	13.0	13.0	-	13.0	27.4	10.0	**Medium**
Option 2 – Big-bang deployment of SAP solution in the 2025–30 RCP	12.6	2.6	15.2	12.6	2.6	15.2	27.4	7.4	**Medium**
Option 3 – Deployment of an alternative product solution for integration and data services	18.3	0.1	18.5	18.3	0.1	18.5	27.4	4.2	**High**
Option 4 – Defer integration platform replacement until 2030–35 RCP	19.5	2.6	22.1	5.1	-	5.1	10.2	-10.6	**Extreme**

[2] Note: Totals presented in tables throughout this document may not exactly match the sums of individual figures due to rounding.
[3] The overall risk level for each option after the proposed option implemented. Refer to Appendix B – risk assessment for details.
[4] Net present value (**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%.
[5] The costs and NPV of option 0 (base case) have been set to zero as the costs associated with this option have been included as benefits of other options as appropriate.

3. Background

Integration software provides connectivity and data-sharing capabilities between critical business systems, including third-party systems. For SA Power Networks, this includes:

- AEMO systems required to fulfil our NEM obligations;
- business-to-business communications to other market participants, sharing information such as customer and site (including life-support) details, meter data, one-way notifications (meter faults and planned interruptions), service orders (requests and responses), and network billing–invoice data;
- business-to-market connectivity to ensure that configuration data is kept in sync with AEMO's Market Settlement and Transfer Solution system for customer administration and transfer, and meter data management; and
- connectivity to local, state and federal governments.

Secure, reliable, real-time integration with no downtime is also critical to service delivery for many of our customer-facing services, such as:

- field crew scheduling appointments/availability/allocation;
- high-priority service-order processing, including meter reading/connects/disconnects/special-reads;
- provision of meter data to customers (regulatory requirement);
- banking;
- power outage notifications via SMS to customers;
- GIS mapping services for asset management; and
- customer website applications and information.

The integration platform (SAP PO and Data Services) was implemented in 2015 to fulfil the requirements for a system that was stable, secure, flexible and cost-effective, and met our business process, data and information needs.

Today, SAP PO continues to be our current integration system, providing highly secure and real-time customer, market and business-critical capabilities across a large number of customer and business services and systems.

A key component of our integration platform is the data transfer capability provided by SAP Data Services. This is an SAP Extract Transform Load solution that enables data integration and data conversion capabilities. This product is used to:

- migrate data from to data warehouses for analytics and reporting purposes;
- copy customer information to our operational network and supervisory control and data acquisition systems to enable real-time operation of the electricity grid;
- link customer, property and GIS location data for meter reading route sequencing;
- provide details of newly connected properties to our GIS systems for mapping purposes; and
- transfer asset information between systems.

All of our customer, network billing and asset data flows through this platform. The annual throughput includes:

- $1.4 billion in network charges;

- 238,000 high-priority service orders;
- 3 million meter reads;
- 3.4 million business-to-business transactions;
- 9 million market transactions;
- 10,000 new customer connections;
- 22,500 life support customers; and
- support and maintenance of around 900,000 National meter identifiers (**NMIs**) and associated customer information, as well as 1.2 million meters.

Secure transfer of customer data is a key requirement of our integration platform, including:

- connectivity between our operational and business systems for customer notifications;
- call centre interactions and identification;
- network billing processes;
- outage management; and
- critical life-support information.

If our core integration platform and critical integrations are not adequately supported and secured, there is high risk of service disruption, liability concerns, and negative experiences for both customers and employees. Key risks include the following:

- Customer data could be at risk if appropriate security patching is not available and applied.
- SA Power Networks could fail to meet our obligations as a distribution network service provider (**DNSP**), metering data provider or metering coordinator within the NEM.
- Timely, accurate information regarding life-support customers, site risk or health and safety requirements may not be available to our staff, which could result in potential injuries or loss of life.

3.1 The scope of this business case

This business case covers the replacement of our core system integration platform software.

The following items are considered as being in scope for this business case:

- Upgrade or replacement of the current SAP PO software
- Upgrade or replacement of the SAP Data Services software
- Building the new environment required for integration and data extracts.
- Migration of the current integrations and data extracts
- Decommissioning of the existing environments – this includes decommissioning the network file system and developing this functionality inside a modern and secure cloud-based platform.

The following items are considered as being out of scope for this business case:

- Implementation of new integrations

It should also be noted that there are other major projects within the SA Power Networks 2025–30 RCP submission that are dependent on our integration platform, including Asset Management Transformation

Program, Click Replacement, Customer Technology Program, Energy Transition, and National Market changes. As a result, this business case considers the timing of delivery of these projects.

3.2 Our performance to date

Since 2015, our reliance on this system has become more critical as we are now all living in an increasingly interconnected world. Our focus has moved from point-to-point connectivity within our own data centres to highly available, 24 x 7 cloud-based systems that provide customers access to data and online outage information, and the ability for customers to report faults/outages and streetlights that aren't working directly to us. More recently, we have invested in this technology to underpin our billing and customer services and mobile services for our customers and field crews.

3.3 Drivers for change

Our IT Asset Management Plan states that an application's end of life should be managed to avoid the consequences of that application's vulnerabilities and failure. Once applications are no longer being supported by their vendors, there is an increased risk of the key services that rely on those applications failing. It is no longer possible to keep them appropriately secured and fit for purpose.

We have been advised by SAP that standard vendor support for both SAP PO and SAP Data Services will stop as of December 2027. Extended support will be available between 2027 and 2030 at an additional cost; however, regular updates will cease and security patching will only be available for critical issues. More definitively, from 2030, no formal support will be available for these products and they will require manual support and the implementation of additional controls.

3.4 Industry practice

Integration is a standard component of every utility, providing connectivity between critical business systems and the NEM, and addressing the continual need for new, increasingly complex data sharing between systems.

4. The identified need

The driver for the investment action being considered in this business case is to address issues associated with our need to maintain our existing services and our current levels of risk through the cost-effective and timely replacement of our core integration platform.

Simply put – all of our customer, network billing and asset data flows through this platform. However, our current platform software is no longer being updated and will go out of mainstream support in December 2027, with support ceasing completely in 2030. This recommendation seeks to maintain our existing customer and business services by ensuring that our core integration platform is fit for purpose, i.e., it is a modern, secure and reliable asset, not an old, end-of-life, vulnerable liability.

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, National Electricity Law and jurisdictional regulations. As a result of these considerations, the identified need for our Integration Platform Replacement project is:

a) To respond to customers' concerns, identified through our consumer and stakeholder engagement process, regarding their explicit service level recommendations in that:
   - for SA Power Networks to operate an electricity distribution network, it is imperative that we ensure core processes, such as scheduling and dispatching field crew workers, call centre access and outage information, are available to our customers. Lack of integration between core systems could lead to service disruption, liability concerns, and negative experiences for both customers and employees.

b) To continue to comply with applicable regulatory obligations/requirements[4], in this case with specific reference to:
   - As the only DNSP in South Australia, we have a responsibility to ensure our systems are available, reliable and secure.
   - We must ensure we continue to meet our obligations as a DNSP, metering data provider and metering coordinator within the NEM – ensuring life-support, metering data management, service orders and customer billing functions.

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.
   - As a critical infrastructure provider, we have regulatory obligations with respect to cyber security to ensure all application security vulnerabilities are remediated in accordance with the risk and threats they pose. This would be difficult on a system that is no longer supported by a vendor, especially where the purpose of the system is to provide high-availability, secure access to/from our systems by customers, staff, other businesses, suppliers, retailers, and regulatory bodies. If this is not done properly, then we risk a breach of confidential customer information, loss of trust in our IT systems or even loss of electricity network control.

d) To drive efficiency in our IT applications – ensuring continuity of essential services for the minimum possible long-term cost.

5. Comparison of options

5.1 The options considered

Table 3: Summary of options considered.

Option	Description
Option 0 – Do nothing (Retain existing integration systems (Base case)	Do not replace integration and data services solutions.
Option 1– Staggered deployment of SAP solution in the 2025–30 RCP	Replace existing integration and data services functionality in the 2025–30 reset period via a gradual staggered approach to deployment.
Option 2 – Big-bang deployment of SAP solution in the 2025–30 RCP	Replace existing integration and data services functionality in the 2025–30 reset period via a big-bang approach to deployment.
Option 3 – Deployment of an alternative product solution	Replace existing integration and data services functionality in the 2025–30 reset period with an alternative product.
Option 4 – Defer replacement into 2030–35 RCP	Replace existing integration and data services functionality the 2030–35 reset period.

5.2 Options investigated but deemed non-credible

We considered an option of replacing our integration systems with an SAP solution and utilising extended support (available until December 2030) to defer this work to later in the 2025–30 period. The upfront project costs of this option would be similar, and extended support costs are minor, so prima-facie, the outcome of this option would be a similar or slightly better NPV.

However, as discussed in section 3.1, there are other major projects within our 2025–30 RCP submission that will need to integrate with our integration systems. Each of these projects delivers a new or upgraded system that will require connection to the new integration platform. Delaying the integration project until after these systems have been delivered would therefore result in rework, as they would need to connect initially to the current integration platform and then later to the new one. The cost of this effort duplication, including requiring the business to retest their systems and processes again, would far outweigh the small incremental NPV benefit from deferring this project until later in the period. As a result, this option has not been modelled.

We also considered the Do-nothing option, where we would not attempt to maintain the integration systems at a reasonable level of security and reliability. However, as a company we have an obligation to:

- ensure the resilience and availability of systems that support critical business processes.
- protect the confidentiality, integrity and availability of data.
- protect against cyber treats.

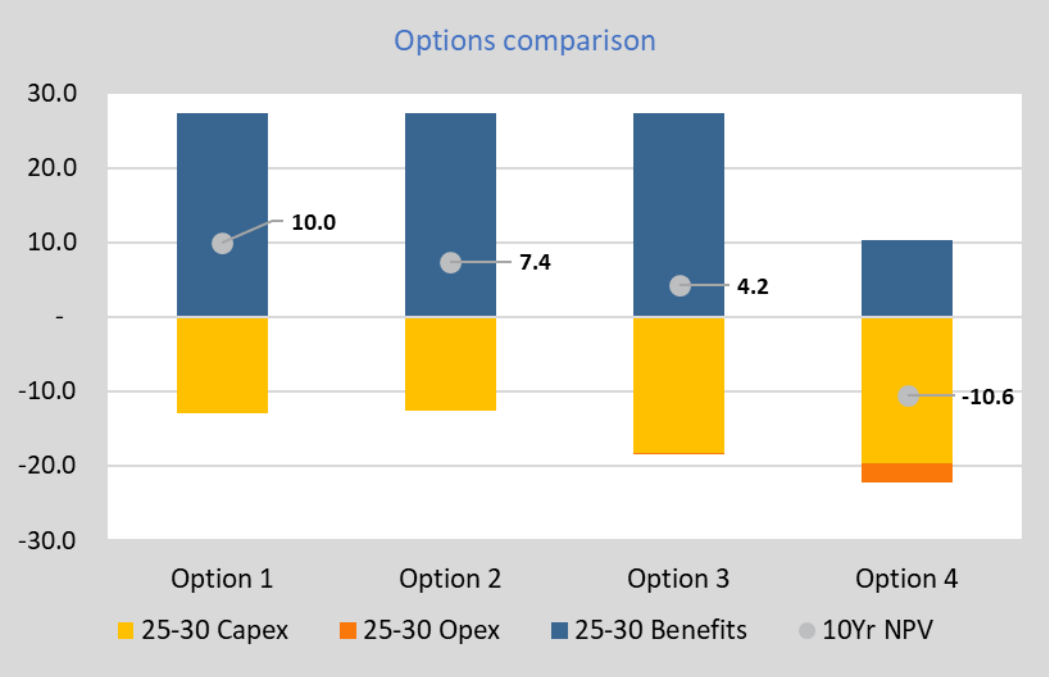
Therefore, an option for Do nothing (retain existing integration systems) is included.

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 10-year period, $m, $ Jun 2022 real.

Option	10-year program costs			2025–30 program costs			10-year benefits [6]	10-year NPV[7]	Overall risk rating[8]	Ranking
	Capex	Opex	Total	Capex	Opex	Total				
Option 0 – Do nothing (Retain existing system)[9]	-	-	-	-	-	-	-	-	Extreme	5
Option 1 – Staggered deployment of SAP solution in the 2025–30 RCP	13.0	-	13.0	13.0	-	13.0	27.4	10.0	Medium	1
Option 2 – Big-Bang deployment of SAP solution in the 2025–30 RCP	12.6	2.6	15.2	12.6	2.6	15.2	27.4	7.4	Medium	2
Option 3 – Deployment of an alternative product solution	18.3	0.1	18.5	18.3	0.1	18.5	27.4	4.2	High	3
Option 4 – Defer replacement until 2030–35 RCP	19.5	2.6	22.1	5.1	-	5.1	10.2	-10.6	Extreme	4



[6] Represents the total capital and operating risk reduction and 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.
[7] 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%.
[8] The overall risk level for each option after the proposed option implemented. Refer to Appendix B – risk assessment for details.
[9] The costs and NPV of option 0 (base case) have been set to zero as the costs associated with this option have been included as benefits of other options as appropriate.

Assumptions

The following assumptions are applicable under all options:

- Approximately 200 integrations in the PO platform will need to be migrated.
- Accelerators (SAP-provided conversion tools) will be available for 80% of the PO interfaces, resulting in efficient migration.
- Migration of the existing system environments – development, test, quality assurance and production (live)

5.3.2 Recommended option

The proposed option is **Option 1 – Staggered deployment of SAP solution in 2025–30 RCP**. This includes a migration of SAP PO to SAP Integration Suite and replacement of SAP Data Services with SAP Data Intelligence and Microsoft Azure Data Factory. The project will be delivered early in the RCP in order to maximise reuse and minimise costs for those programs and projects that require the integration changes during the RCP.

This solution:

- ensures continued operation of our current systems and services;
- provides a long-term stable and secure integration environment;
- is less complex and less expensive than the other options; and
- avoids rework costs and reduces business impact, as integration with other new systems and user acceptance testing only take place once.

This option will maintain our existing customer and business services by ensuring that our core integration platform is fit for purpose, secure and reliable. It ensures the continued reliable and efficient provision of services to our customers.

5.4 Option 0 – Do nothing (Retain existing integration systems)

5.4.1 Description

This option does not invest in upgrading the end-of-life SAP integration platform. Instead, it implements risk management activities. This includes increased cyber security monitoring, hardening and isolation techniques, along with considerable ongoing manual and custom workarounds to manage the risk of continuing to run a platform beyond end of life and vendor support. It also requires completing increased industry testing activities for our market systems to ensure a high level of security integrity across the environment.

5.4.2 Costs

Table 5: Option 0 – Costs by cost type ($m Jun 2022 real)

Cost Type	2025 H1	2025-26	2026-27	2027-28	2028-29	2029-30	Total 2025 - 30	2030-31	2031-32	2032-33	2033-34	2034-35	Total 2025-35
Capex	-	-	-	1.2	1.6	2.2	5.1	2.4	2.5	2.5	2.6	2.6	**17.6**
Opex	-	-	-	-	-	-	-	-	-	-	-	-	**-**
TOTAL	**-**	**-**	**-**	**1.2**	**1.6**	**2.2**	**5.1**	**2.4**	**2.5**	**2.5**	**2.6**	**2.6**	**17.6**

Costing assumptions are:

- Manual patching, security hardening and increased monitoring beginning H1 CY2028 at a cost of $2 million per annum
- Rehearsal and pre-loading of systems is required prior to Dec 2030 in order to successfully transition into a self-supported landscape.
- Replacement of the network drive at a cost of $0.5 million in 2027-28
- No changes to licensing, subscription, storage or compute (Operating expenditure (**Opex**)) costs, as nothing is changing.

5.4.3 Risks

Table 6: Risk assessment summary

Risk consequence category	Current risk level[10] (Option 0)
Safety – Harm to a worker, contractor or member of the public	High
Performance and growth – Financial impact	Extreme
Network – Failure to transport electricity from source to load	High
Customers – Failure to deliver on customer expectations	Extreme
Overall risk level	Extreme

Doing nothing will cause some systems to stop functioning without ongoing updates and upgrades. This will likely result in some of our services and core functions becoming unavailable during the period. The chances of a cyber security incident will also increase dramatically over time due to the lack of security patching on the systems.

5.4.4 Advantages and disadvantages

The advantages and disadvantages of Option 0 are summarised in Table 7.

Table 7: Advantages and disadvantages

Advantages	Disadvantages
Lower upfront capital cost.	Increasingly difficult to provide continuity of service to ensure that appropriate data sharing between systems and the market is taking place in a timely and reliable way.
No requirement to train, upskill or buy-in resources to learn and operate new technologies.	As applications age, there is an increased risk of the key services that are relying on those applications failing. That is, once applications are no longer being supported by their vendors, it is no longer possible to keep them appropriately secured and fit for purpose.
	When critical integrations are not adequately supported and secured, there is high risk of service disruption to many of our services. For example, secure transfer of customer data is a key requirement of our integration platform, including: • Connectivity between our operational and business systems for customer notifications • Call-centre interactions and identification • Network billing processes • Outage management • Critical life-support information Consequences of disruptions to these services could include liability, and negative experiences for both customers and employees.
	Cyber security risk will increase if application security vulnerabilities are not remediated in accordance with the risk and threats they pose (improving our cyber security was strongly supported in our People's Panel discussions).
	There is increased potential that less accurate information regarding life-support customers, site risk or health and safety requirements could result in injuries or loss of life.

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

Advantages	Disadvantages
	Any new integrations required and deployed during 2025-30 will result in additional rework, recoding and retesting, creating additional cost post–2030 and increased impact to the business.
	Extended support is offered up to December 2030. If these technologies are not upgraded at end of life when extended support ends, the costs go up significantly, as these products will require manual support and additional controls to be implemented to mitigate the escalating risks associated with the reduced level of system security.
	As the only DNSP in the state, if we could not facilitate industry and market testing with other South Australian market participants, this could seriously impact them and their customers by them not being able to connect to the NEM.

5.5 Option 1 – Staggered deployment of SAP solution in the 2025–30 RCP

5.5.1 Description

This option continues the proactive management of our business applications. This option involves:

- a staggered deployment of SAP PO to SAP Integration Suite
- replacement of SAP Data Services with SAP Data Intelligence and Microsoft Azure Data Factory.

It addresses the end-of-life issues associated with our core SAP integration platforms before the vendor service end date of December 2027.

5.5.2 Costs

The forecast for Option 1 has been prepared on a bottom-up basis. The timing of costs reflects migration to the new integration platform at the start of the 2025–30 RCP. This enables other key technology projects that are being delivered within the RCP to connect with the new integration platform, avoiding significant rework that would include requiring the business to test their systems and processes again. The cost profile for this option is shown in Table 8, with detailed estimates listed in Appendix A.

Table 8: Option 1 – Costs by cost type ($m Jun 2022 real)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30	2030–31	2031–32	2032–33	2033–34	2034–35	Total
Capex	4.3	4.1	4.6	-	-	**13.0**	-	-	-	-	-	**13.0**
Opex	-	-	-	-	-	**-**	-	-	-	-	-	**-**
Total	**4.3**	**4.1**	**4.6**	-	-	**13.0**	**-**	**-**	**-**	**-**	**-**	**13.0**

5.5.3 Risks

The detailed risk assessments are provided in Appendix B.

Table 9: Risk assessment summary

Risk consequence category	Current risk level[11] (Option 0)	Residual risk level[12] (Option 1)
Safety – Harm to a worker, contractor or member of the public	High	Medium
Performance and growth – Financial impact	Extreme	Medium
Network – Failure to transport electricity from source to load	High	Medium
Customers – Failure to deliver on customer expectations	Extreme	Medium
Overall risk level	Extreme	Medium

5.5.4 Advantages and Disadvantages

The advantages and disadvantages of Option 1 are summarised in the table below.

Table 10: Advantages and disadvantages

Advantages	Disadvantages
Enabling a modern toolset with the latest methods and technology to support the business.	Requiring an additional, temporary three-tier support environment to parallel run systems.
De-risking the business from products that are nearing end of life.	
Increased our ability to use a modern security and integration feature set.	
Aligning the technology roadmap with software vendors' latest products.	
Aligning with the vendor's family of cloud-based development and monitoring tools to reduce issue resolution times.	

5.5.5 Quantified benefits

Table 11 provides estimates of quantified benefits for the 10 years starting in July 2025 for Option 1.

Table 11: Option 1 – Benefits by expenditure type ($m Jun 2022 real)

Benefit Type	2025 -26	2026 -27	2027 -28	2028 -29	2029 -30	Total 2025 - 30	2030 -31	2031 -32	2032 -33	2033 -34	2034 -35	Total 2025-35
Capex	2.2	2.2	2.7	1.6	2.2	**10.9**	3.1	5.0	3.3	2.6	2.6	**27.4**
Opex	-	-	-	-	-	**-**	-	-	-	-	-	**-**
Customer	-	-	-	-	-	**-**	-	-	-	-	-	**-**
TOTAL	**2.2**	**2.2**	**2.7**	**1.6**	**2.2**	**10.9**	**3.1**	**5.0**	**3.3**	**2.6**	**2.6**	**27.4**

[11] The level of risk post current controls (ie, after considering what we currently do to mitigate the risk).
[12] The future level of risk once treatments proposed in this option have been implemented.

The primary quantifiable benefit of implementing Option 1 is avoiding the costs of SA Power Networks self-supporting our current SAP integration environment when it is out of mainstream maintenance in December 2027. It also avoids any potential costs associated with cyber security risk resulting from maintaining an unpatched and unsupported system and identifies that there will be a cost for rehearsal of manual support processes and pre-loading of systems is required prior to Dec 2030 in order to successfully transition into a fully self-supported landscape.

Costs of $9.8 million for the future re-work required to transition to a new system post 2030 have been estimated based on the proposed integration and testing costs for Click, Customer and SAP Lifecycle projects planned in this period. This figure is considered conservative as no environment build or project/change management has been included.

Table 12 provides a breakdown of the cost and risk avoidance benefits generated by not undertaking self-support of our current integration environment, including:

- manually applying software maintenance patches to solve functionality and security issues.
- provision of end-to-end encryption across all messages
- increasing our monitoring of interface messages to identify increased trends in failures or corruption of data.
- provision for break/fix expenditure to remediate and resolve issues quickly.
- increased need for user support as problems with interfaces occur more regularly.
- There are further benefits from removing the need to carry out rework on any interfaces required prior to 2030.

Table 12: Option 1 – Benefits breakdown ($m Jun 2022 real)

Benefit Type	Benefit Description	2025-26	2026-27	2027-28	2028-29	2029-30	2030-31	2031-32	2032-33	2033-34	2034-35
Cost avoidance	Manual patching of PO Landscape	-	-	-	-	0.5	0.5	0.5	0.5	0.5	0.5
	Security hardening of interfaces	-	-	0.2	0.3	0.2	0.2	0.2	0.2	0.3	0.3
	Increased monitoring	-	-	0.1	0.3	0.3	0.2	0.2	0.2	0.3	0.3
	Break/fix remediation	-	-	0.4	0.4	0.5	0.6	0.6	0.6	0.6	0.6
	User Support	-	-	0.1	0.3	0.2	0.2	0.2	0.2	0.3	0.3
Risk avoidance	Cyber risk	-	-	0.4	0.4	0.5	0.6	0.6	0.6	0.6	0.6
Cost avoidance	Re-Work	2.2	2.2	1.5	-	-	0.7	2.5	0.8	-	-
TOTAL		**2.2**	**2.2**	**2.7**	**1.6**	**2.2**	**3.1**	**5.0**	**3.3**	**2.6**	**2.6**

5.6 Option 2 – Big-bang deployment of SAP solution in the 2025–30 RCP

5.6.1 Description

This option also continues proactive management of our business applications. This option involves:

- a big-bang deployment of SAP PO to SAP Integration Suite
- replacing SAP Data Services with SAP Data Intelligence and Microsoft Azure Data Factory.

As with Option 1, it addresses the end-of-life issues associated with our core SAP integration platforms before the vendor service end date of December 2027.

5.6.2 Costs

The forecast for Option 2 has been prepared on a bottom-up basis. The timing of costs reflects migration to the new integration platform at the start of the 2025–30 RCP. This enables other key technology projects being delivered within the RCP to connect with the new integration platform, avoiding significant rework. The cost profile for this option is shown in Table 13, with detailed estimates listed in Appendix A.

Table 13 : Option 2 – Costs by cost type ($m Jun 2022 real)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30	2030–31	2031–32	2032–33	2033–34	2034–35	Total 2025–35
Capex	12.6	-	-	-	-	**12.6**	-	-	-	-	-	**12.6**
Opex	2.6	-	-	-	-	**2.6**	-	-	-	-	-	**2.6**
Total	**15.2**	**-**	**-**	**-**	**-**	**15.2**	**-**	**-**	**-**	**-**	**-**	**15.2**

Option 2 costs are slightly greater than Option 1, as this approach is more complex (a number of dress-rehearsal trial runs are required prior to actual cutover) and less flexible (as Option 1 staging allows a smaller team to create repeatable migrations that are spread out to have less impact on the business).

5.6.3 Risks

Table 14: Risk assessment summary

Risk consequence category	Current risk level[13] (Option 0)	Residual risk level[14] (Option 2)
Safety – Harm to a worker, contractor or member of the public	High	Medium
Performance and growth – Financial impact	Extreme	Medium
Network – Failure to transport electricity from source to load	High	
Customers – Failure to deliver on customer expectations	Extreme	Medium
Overall risk level	Extreme	Medium

5.6.4 Advantages and Disadvantages

The advantages and disadvantages of Option 2 are summarised in the table below.

Table 15 : Advantages and disadvantages

Advantages	Disadvantages
Enabling a modern toolset with the latest methods and technology to support the business.	Requiring an additional, temporary three-tier support environment to parallel-run systems.
De-risking the business from products that are nearing end of life.	Requiring five additional testing environments to be established for systems integration, dress rehearsal and user acceptance tests.

[13] The level of risk post current controls (i.e. after considering what we currently do to mitigate the risk).
[14] The future level of risk once treatments proposed in this option have been implemented.

Advantages	Disadvantages
Increasing our ability to use a modern security and integration feature set.	Stabilising systems is harder as so many changes are being made at the same time.
Aligning the technology roadmap with software vendors' latest products.	
Aligning with the vendor's family of cloud-based development and monitoring tools to reduce issue resolution times.	

5.6.5 Quantified benefits

Table 16 provides estimates of quantified benefits for the 10 years starting July 2025 for Option 2.

Table 16: Option 2 – Benefits by expenditure type ($m Jun 2022 real)

Benefit Type	2025-26	2026-27	2027-28	2028-29	2029-30	Total 2025 - 30	2030-31	2031-32	2032-33	2033-34	2034-35	Total 2025-35
Capex	2.2	2.2	2.7	1.6	2.2	**10.9**	3.1	5.0	3.3	2.6	2.6	**27.4**
Opex	-	-	-	-	-	**-**	-	-	-	-	-	**-**
Customer	-	-	-	-	-	**-**	-	-	-	-	-	**-**
TOTAL	**2.2**	**2.2**	**2.7**	**1.6**	**2.2**	**10.9**	**3.1**	**5.0**	**3.3**	**2.6**	**2.6**	**27.4**

Similar to Option 1, the primary quantifiable benefit of implementing Option 2 is avoiding the costs of SA Power Networks self-supporting our current SAP integration environment when it is out of maintenance in December 2027. It also avoids any potential costs associated with cyber security risk resulting from maintaining an unpatched and unsupported system. There are further benefits from removing the need to carry out rework on any interfaces required prior to 2030. The details in Table 17 are the same as those in Table 12, above.

Table 17: Option 2 – Benefits breakdown ($m Jun 2022 real)

Benefit Type	Benefit Description	2025-26	2026-27	2027-28	2028-29	2029-30	2030-31	2031-32	2032-33	2033-34	2034-35
Cost avoidance	Manual patching of PO Landscape	-	-	-	-	0.5	0.5	0.5	0.5	0.5	0.5
	Security hardening of interfaces	-	-	0.2	0.3	0.2	0.2	0.2	0.2	0.3	0.3
	Increased monitoring	-	-	0.1	0.3	0.3	0.2	0.2	0.2	0.3	0.3
	Break/fix remediation	-	-	0.4	0.4	0.5	0.6	0.6	0.6	0.6	0.6
	User Support	-	-	0.1	0.3	0.2	0.2	0.2	0.2	0.3	0.3
Risk avoidance	Cyber risk	-	-	0.4	0.4	0.5	0.6	0.6	0.6	0.6	0.6
Cost avoidance	Re-Work	2.2	2.2	1.5	-	-	0.7	2.5	0.8	-	-
TOTAL		**2.2**	**2.2**	**2.7**	**1.6**	**2.2**	**3.1**	**5.0**	**3.3**	**2.6**	**2.6**

5.7 Option 3 – Deployment of an alternative product solution

5.7.1 Description

Option 3 also continues the proactive management of our business applications. This option involves investigating and deploying the most suitable alternative to our current SAP integration products and then decomissioning the existing SAP systems.

It addresses the end-of-life issues associated with our core SAP integration platforms before the vendor service end date of December 2027.

5.7.2 Costs

Option 3 costs are based on Option 1 costs, with a scaling factor of a 50% increase (a conservative estimate) applied to the implementation costs to account for several factors:

- This approach requires more design and development activities, reflecting the need for additional effort for a full rebuild on a new platform.
- An alternative supplier will not provide migration assessment, tooling and test automation software.
- Our unfamiliarity with the new integration products and tools will increase the time required and the risk on the project.
- We would not expect to get the same efficiencies in integration activities that we get from our existing SAP integration toolset.
- Additional ongoing costs, resulting from the increased customisation of existing code that would be required to support the increased number of integration products needed to maintain our systems.
- There is no allowance for Opex cost as it is assumed that the incoming product would require an equivalent level of compute/storage/licensing/subscription.
- Pre-built processing code, connectors and adapters would not be provided by the alternative supplier.
- The additional cost of establishing identity management, monitoring and alerting, which we have already implemented for the existing SAP cloud product.

The timing of costs reflects migration to the new integration platform at the start of the 2025–30 RCP. This enables other key technology projects being delivered within the RCP to connect with the new integration platform, avoiding significant rework. The cost profile for this option is shown in Table 18, with detailed estimates listed in Appendix A.

Table 18: Option 3 – Costs by cost type ($m Jun 2022 real)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025 – 30	2030–31	2031–32	2032–33	2033–34	2034–35	Total 2025–35
Capex	18.3	-	-	-	-	**18.3**	-	-	-	-	-	**18.3**
Opex	0.1	-	-	-	-	**0.1**	-	-	-	-	-	**0.1**
Total	**18.5**	-	-	-	-	**18.5**	-	-	-	-	-	**18.5**

5.7.3 Risks

Table 19: Risk assessment summary

Risk consequence category	Current risk level[15] (Option 0)	Residual risk level[16] (Option 3)
Safety – Harm to a worker, contractor or member of the public	High	Medium
Performance and growth – Financial impact	Extreme	Medium
Network – Failure to transport electricity from source to load	High	
Customers – Failure to deliver on customer expectations	Extreme	High
Overall risk level	Extreme	High

The overall residual risk under this option would be reduced to High – slightly higher than Options 1 and 2. Option 3 would result in additional security risk due to limitations with older-style SAP integrations not being supported, the increased customisation and rebuilding of software required, and technical limitations imposed by not providing hybrid opportunities securing both on-premise and cloud platforms.

5.7.4 Advantages and disadvantages

The advantages and disadvantages of Option 3 are summarised in the table below.

Table 20: Advantages and disadvantages

Advantages	Disadvantages
Enabling a modern toolset with the latest methods and technology to support the business.	More complex migration path and cost of product selection.
De-risking the business from products that are nearing end of life.	More expensive and additional support costs, and additional team/skills required to support new product.
Increased our ability to use a modern security and integration feature set.	Increased licensing costs required as SAP integration will still be needed.
	Additional monitoring and administration tools required.
	More complex problem troubleshooting, analysis, remediation, and resolution of issues as end-to-end support is not provided by a single vendor.

Table 21 provides estimates of quantified benefits for the 10 years starting in July 2025 for Option 3.

Table 21: Option 3 – Benefits by expenditure type ($m Jun 2022 real)

Benefit Type	2025-26	2026-27	2027-28	2028-29	2029-30	Total 2025 - 30	2030-31	2031-32	2032-33	2033-34	2034-35	Total 2025-35
Capex	2.2	2.2	2.7	1.6	2.2	**10.9**	3.1	5.0	3.3	2.6	2.6	**27.4**
Opex	-	-	-	-	-	**-**	-	-	-	-	-	**-**
Customer	-	-	-	-	-	**-**	-	-	-	-	-	**-**
TOTAL	**2.2**	**2.2**	**2.7**	**1.6**	**2.2**	**10.9**	**3.1**	**5.0**	**3.3**	**2.6**	**2.6**	**27.4**

[15] The level of risk post current controls (i.e. after considering what we currently do to mitigate the risk).
[16] The future level of risk once treatments proposed in this option have been implemented.

Similar to the previous options, the primary quantifiable benefit of implementing Option 3 is avoiding the costs of SA Power Networks self-supporting our current SAP integration environment when it is out of maintenance in December 2027. It also avoids any potential costs associated with cyber security risk resulting from having to maintain an unpatched and unsupported system and cost of rework.

Table 22: Option 3 – Benefits breakdown ($m Jun 2022 real)

Benefit Type	Benefit Description	2025-26	2026-27	2027-28	2028-29	2029-30	2030-31	2031-32	2032-33	2033-34	2034-35
Cost avoidance	Manual patching of PO Landscape	-	-	-	-	0.5	0.5	0.5	0.5	0.5	0.5
	Security hardening of interfaces	-	-	0.2	0.3	0.2	0.2	0.2	0.2	0.3	0.3
	Increased monitoring	-	-	0.1	0.3	0.3	0.2	0.2	0.2	0.3	0.3
	Break/fix remediation	-	-	0.4	0.4	0.5	0.6	0.6	0.6	0.6	0.6
	User Support	-	-	0.1	0.3	0.2	0.2	0.2	0.2	0.3	0.3
Risk avoidance	Cyber risk	-	-	0.4	0.4	0.5	0.6	0.6	0.6	0.6	0.6
Cost avoidance	Re-Work	2.2	2.2	1.5	-	-	0.7	2.5	0.8	-	-
TOTAL		**2.2**	**2.2**	**2.7**	**1.6**	**2.2**	**3.1**	**5.0**	**3.3**	**2.6**	**2.6**

5.8 Option 4 – Defer Integration Platform replacement until 2030–35 RCP.

5.8.1 Description

This option continues extended support with the vendor until end of life of the SAP integration platform in December 2030. We would then implement risk management activities, including increased cyber monitoring, hardening and isolation, along with manual and custom workarounds, to manage the risk of continuing to run a platform beyond end of life and vendor support. The integration platform would then be replaced in the 2030–35 RCP.

5.8.2 Costs

Total costs for this option are provided in Table 23. This is made up continuing the Option 0 Do-nothing (retain existing system) and then implementation of our Option 2 – Big-Bang approach in 2030-31. There will also be a cost to continue self-supporting the integration landscape for the duration of the cut over to a new integration system.

Table 23 Option 4 – Costs by cost type ($m Jun 2022 real)

Cost type	2025 H1	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30	2030–31	2031–32	2032–33	2033–34	2034–35	Total 2025–35
Capex		-	-	1.2	1.6	2.2	**5.1**	14.4	-	-	-	-	**19.5**
Opex	-	-	-	-	-	-	**-**	2.6	-	-	-	-	**2.6**
Total		**-**	**-**	**1.2**	**1.6**	**2.2**	**5.1**	**17.0**	**-**	**-**	**-**	**-**	**22.1**

5.8.3 Risks

Table 24: Risk assessment summary

Risk consequence category	Current risk level[17] (Option 0)	Residual risk level[18] (Option 4)
Safety – Harm to a worker, contractor or member of the public	High	High
Performance and growth – Financial impact	Extreme	Extreme
Network – Failure to transport electricity from source to load	High	High
Customers – Failure to deliver on customer expectations	Extreme	Extreme
Overall risk level	Extreme	Extreme

As with Option 0, this option would result in a high risk of some systems no longer functioning without ongoing updates and upgrades during the unsupported period. This would likely result in some of our services and core functions becoming unavailable during the period. The chances of a cyber security incident would also increase dramatically over time due to the lack of security patching on the systems.

5.8.4 Advantages and disadvantages

The advantages and disadvantages of Option 4 are summarised in the table below.

Table 25: Advantages and disadvantages

Advantages	Disadvantages
Capital expenditures will be deferred into the next reset period.	As applications age, there is an increased risk of failure of the key services relying on those applications. That is, once applications are no longer being supported by their vendors, it is no longer possible to keep them appropriately secured and fit for purpose.
	When critical integrations are not adequately supported and secured, there is high risk of service disruption, which results in liability concerns and negative experiences for both customers and employees.
	Cyber security risk will increase if application security vulnerabilities are not remediated in accordance with the risk and threats they pose (improving our cyber security was strongly supported in our People's Panel discussions).
	There is increased potential for less accurate information regarding life-support customers, site risk or health and safety requirements to result in potential injuries or loss of life.
	Any new integrations required and deployed during 2025–30 will result in additional rework, recoding and retesting, creating additional cost post–2030 and increased impact to the business.

[17] The level of risk post current controls (i.e. after considering what we currently do to mitigate the risk).
[18] The future level of risk once treatments proposed in this option have been implemented.

Advantages	Disadvantages
	Extended support is offered up to December 2030. If these technologies are not upgraded at end of life when extended support ends, the costs go up significantly, as these products require manual support and additional controls to be implemented to mitigate the escalating risks associated with the reduced level of system security.
	As the only DNSP in the state, if we could not facilitate industry and market testing with other South Australian market participants, we could seriously impact them and their customers by them not being able to connect to the NEM.

5.8.5 Quantified benefits

Table 26 provides estimates of quantified benefits for the 10 years starting July 2025 for Option 4.

Table 26: Option 4 – Benefits by expenditure type ($m Jun 2022 real)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30	2030–31	2031–32	2032–33	2033–34	2034–35	Total 2025–35
Capex	-	-	-	-	-	-	-	2.5	2.5	2.6	2.6	**10.2**
Opex	-	-	-	-	-	-	-	-	-	-	-	**-**
Total	-	-	-	-	-	-	**-**	**2.5**	**2.5**	**2.6**	**2.6**	**10.2**

The primary quantifiable benefit of implementing Option 4 is avoiding the costs of SA Power Networks self-supporting our current SAP integration environment post-implementation of a replacement system in 2030–31. It also avoids any potential costs associated with cyber security risk that would result from maintaining an unpatched and unsupported system over the last four years of the 2030–35 RCP.

The benefits detailed in Table 27, below, are the same as those for the previous options. However, the benefit start date is delayed by four years compared to the other options, due to the delayed implementation date of 2030-31.

Table 27: Option 4 – Benefits breakdown ($m Jun 2022 real)

Benefit Type	Benefit Description	2025-26	2026-27	2027-28	2028-29	2029-30	2030-31	2031-32	2032-33	2033-34	2034-35
Cost avoidance	Manual patching of PO Landscape	-	-	-	-	-	-	0.5	0.5	0.5	0.5
	Security hardening of interfaces	-	-	-	-	-	-	0.2	0.3	0.3	0.3
	Increased monitoring	-	-	-	-	-	-	0.2	0.3	0.3	0.3
	Break/fix remediation	-	-	-	-	-	-	0.6	0.6	0.6	0.6
	User Support	-	-	-	-	-	-	0.2	0.3	0.3	0.3
Risk avoidance	Cyber risk	-	-	-	-	-	-	0.6	0.6	0.6	0.6
TOTAL		**-**	**-**	**-**	**-**	**-**	**-**	**2.5**	**2.5**	**2.6**	**2.6**

6. Deliverability of recommended option

SA Power Networks successfully completed two major integration projects in May 2021 and March 2022 and both projects achieved zero loss of data. The recommended option incorporates lessons learned from those projects, including:

- limiting the impact on business teams by confining testing to specific and agreed timeslots aligned to their business processes;
- having a gradual, Agile (staggered) approach to migration, initially starting with simpler interfaces and then moving to more complex integrations as the team gains experience; and
- bundling integrations into types and patterns so repeatable migration processes can be developed.

7. How the recommended option aligns with our engagement

Customers expect that we will maintain our existing levels of service and risk, and there is also an expectation on SA Power Networks to manage our assets prudently and cost-effectively.

Our IT Asset Management Plan outlines an asset management framework to ensure IT investment is prudent and targeted at managing risk and value. This approach requires us to manage applications' end of life to avoid the consequences of application vulnerabilities and failure.

As applications age, there is an increased risk of the key services that rely on those applications failing. That is, once applications are no longer being supported by their vendors, it is no longer possible to keep them appropriately secured and fit for purpose, so they must be replaced or upgraded.

This project was mentioned in the IT Focused Conversation with the Consumer Advisory Board as 'for information'. The total costs and bill impacts were included in all customer engagement conversations as part of Scenario 2 – maintain but was not specifically drawn out in these conversations.

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 and Data Strategy

Our **Digital and Data Strategy** identifies that new approaches to core IT provide significant opportunities to adopt a more flexible, scalable and cost-effective core environment. This can only be achieved with the provision of a modern enterprise integration toolset with the latest methods and technology. This supports the business to address the following areas.

Tighter system integration

The network of the future will leverage a wider use of technologies, which will include tighter integration between IT and OT systems. This will provide greater insights and 360-degree views of our operational network, assets, work, and customers, resulting in more seamless customer experiences being delivered by reliable, supported and secure modern core systems.

Openness

A significant expansion in energy market participation will create an increased need to collect and exchange data with external parties in real or near-real-time format. Core efficient, secure and reliable IT systems and services will enable a more diverse and open environment, and this presents a range of challenges, including open standards, integration and resilient data and cyber security.

Digitally enabled work practices

The real impact of digital integration capabilities on the business as a whole will emerge when we start to use them to reshape our business processes. Integrated data and richer pictures of end-to-end workflows, coupled with intelligent machines making decisions, will enable us to streamline our business processes end to end.

9. Reasonableness of cost and benefit estimates

Costing for this business case has been prepared on a bottom-up basis by creating a fully resourced, high-level plan for each option. This estimate has been validated and refined in multiple ways:

- **Review by our portfolio and program delivery teams:** they are familiar with the approaches identified and the complexity of the requirements, based on our own experiences of similar-sized projects.
- **Assessment by our internal team:** using experience gained from successful migration of our SAP systems to the cloud in March 2022. This $7.1 million project included the transition of our SAP integration platform from our on-premise data centres to the cloud.
- **Engagement of an independent third party:** (Capgemini, who are familiar with our SAP environment as they were the system implementation partner on the billing replacement program) to estimate the costs.

10. Reasonableness of input assumptions

The quotes and licensing costs reflect the most recently available cost provided by SAP (the application vendor).

We have used independently benchmarked labour rates. While labour costs have increased significantly in the current market due to increased demand and workforce shortages associated with the COVID-19 pandemic, we are conservatively assuming that costs will stabilise at current levels. While it is very possible that in the next RCP, real dollar unit rates will either continue to increase or will revert to pre-pandemic levels, there is no basis on which to assume that either of these scenarios will occur.

A. Appendix A – Cost models

Option	Description	Name
Option 0	Do nothing	Integration Platform Replacement - Option 0 Do Nothing
Option 1	Staggered deployment of SAP solution in the 2025–30 RCP	Integration Platform Replacement - Option 1 PIPO Upgrade - Preferred
Option 2	Big-bang deployment of SAP solution in the 2025–30 RCP	Integration Platform Replacement - Option 2 Big Bang
Option 3	Deployment of an alternative product integration solution	Integration Platform Replacement - Option 3 Alt Integ Platform
Option 4	Defer deployment until 2030–35 RCP	Integration Platform Replacement - Option 4 Deferred PIPO Upgrade
Benefits	Benefits allocation method	Integration Platform Replacement - Benefits

B. Appendix B – Risk assessment

				Current risk (Options 0 – Non-credible and 4 – Defer)			Residual risk (Options 1 and 2 – Retain SAP)			Residual risk (Option 3 – Alternative)		
ID	Risk scenario	Consequence description	Consequence category	Consequence	Likelihood	Risk level	Consequence	Likelihood	Risk level	Consequence	Likelihood	Risk level
1	Failure or performance degradation of IT applications, due to integration systems being past their useful life, unsupported or unavailable.	Network reliability is affected as the distribution networks' operation and reliability is heavily dependent on the data provisioned by our integration systems; any network reliability issue can, in turn, result in liability and/or increased frequency and duration of network outages for customers.	**Network** – Failure to transport electricity from source to load	4	3	High (7)	4	2	Medium (6)	4	2	Medium (6)
			Customer – Failure to deliver on customer expectations	4	3	High (7)	4	2	Medium (6)	4	2	Medium (6)
		Network outage management teams are 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 these customers. We have more than 22,500 NMIs recorded for life-support customers.	**Safety** – Harm to a worker, contractor, or member of the public	5	3	High (8)	5	1	Medium (6)	5	1	Medium (6)
		Productivity reduces and tasks take longer to be completed, impacting cashflows and financial transactions. Potential breach of SLAs resulting in financial impact > $2m and < $10m.	**Performance and growth** – Financial Impact	4	4	High (8)	4	1	Low (5)	4	1	Low (5)
		Ability to generate accurate regulatory and reliability reporting, which is heavily dependent on IT systems, could be compromised, resulting in regulatory/financial penalties > $2m and <$10m.	**Performance and growth** – Financial Impact	4	5	Extreme (9)	4	1	Low (5)	4	1	Low (5)

		Reputational damage caused by customer impacts requiring repeated intervention by Ombudsman or regulators.	**Customer** – Failure to deliver on customer expectations	4	5	**Extreme (9)**	4	1	**Low (5)**	4	1	**Low (5)**
		Market billing is impacted as our ability to generate DUoS (Distribution Use of Services) billing to retailers is impeded, placing the main corporate cashflow at risk and potentially restricting business operations. Total loss of trust in our billing systems.	**Performance and growth** – Financial Impact	5	5	**Extreme (10)**	5	1	**Medium (6)**	5	1	**Medium (6)**
2	Failure or performance degradation of IT Applications, due to integration systems being vulnerable to cyber-attacks.	A successful cyber security event could result in loss of data, impact reliability of supply or compromise control systems. We could also expect significant penalties from regulators and aggrieved party legal actions.	**Network –** Failure to transport electricity from source to load	4	3	**High (7)**	4	1	**Low (5)**	4	2	**Medium (6)**
		Long-term, irreversible loss of customer or strategic partners' trust.	**Performance and Growth (Financial Impact)**: Litigation and/or penalties	5	3	**High (8)**	5	1	**Medium (6)**	5	2	**High (7)**
		Total loss of trust in network control or billing systems.	**Safety –** Harm to a worker, contractor or member of the public	5	3	**High (8)**	5	1	**Medium (6)**	5	1	**Medium (6)**
		Significant unauthorised access or disclosure of highly confidential or customer data.	**Customers** – Failure to deliver on customer expectations	5	4	**Extreme 9**	5	1	**Medium (6)**	5	2	**High (7)**
			Overall risk level[19]			**Extreme**			**Medium**			**High**

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