ICT Business Case: Recurrent - IT Applications Refresh

2025-2030 Regulatory Proposal

Supporting document [5.12.4]

January 2024

SA Power Networks

Empowering South Australia

Contents

Glossary

Acronym / term	Definition
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AMP	Asset Management Plan
ATO	Australian Tax Office
Capex	Capital expenditure
CER	Customer energy resources
DER	Distributed energy resources
GIS	Geographic Information System
ICT	Information and communication technology
IT	Information technology
NPV	Net present value
NEM	National Electricity Market
Opex	Operating expenditure
RCP	Regulatory Control Period
RIN	Regulatory Information Notice
SaaS	Software as a service
STP	Single Touch Payroll

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 Networks IT (Information Technology) Applications for the 2025–30 Regulatory Control Period (**RCP**).

1.2 Expenditure category

- Non-network Information and communication technology (**ICT**) capital expenditure (**capex**): Recurrent
- Non-network ICT operating expenditure (**Opex**) Step Change: software as a service (**SaaS**) related Capex to Opex Shift – Base Year Adjustment

1.3 Related documents

Table 1: Related documents

Title		Version / date
5.12.1 - IT Investment Plan 2025-30	SA Power Networks	Jan 2024
5.12.8 - Data, Analytics & Intelligent Systems Refresh Business Case	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 provides the justification for the recurrent ICT expenditure required to prudently maintain our existing customer, network and business services and manage risk through the program of periodic application version upgrades, security patching, minor enhancements, and defect remediation for the SA Power Networks' information technology (**IT**) application portfolio. These business-critical applications support the effective management of our distribution network services, including asset management, planning and design, customer services, life-support customers, works management and scheduling, and corporate services (such as finance, payroll and procurement).

SA Power Networks has a proven efficient and practical maintenance regime governed by our IT Asset Management Plan. This requires us to ensure that our business-critical systems remain available and secure for customers and staff, ensuring business continuity and management of system outage risks. Upgrades, updates and continuous improvement initiatives are applied to reflect Asset Management Plan principles, including consideration of the business purpose, system criticality, and prescribed vendor security patches for the application.

- While patching, updating and maintaining applications is a necessary ongoing requirement in a digital world, there are several key drivers for changes in the level of this activity in the 2025–30 RCP:
- The ever-increasing use of, and reliance on, IT applications over time, resulting is us implementing additional capacities, particularly mobile applications, which need ongoing refresh
- We planned an investment 'dip' during the 2020-25 RCP as some of the large non-recurrent programs undertook some of the recurrent activities. However, going forward maintaining the levels of investment and risk in these new core systems means a reversion to previous higher levels of expenditure.
- New compliance requirements in areas such as The Australian Tax Office's (**ATO**) Single Touch Payroll (**STP**).
- Implementation of SaaS-based versions of applications over time, replacing on-premise versions and requiring a switch from capital to operating expenditure.

This business case recommends continuing with our risk-based approach to managing our IT applications via a prudent and timely patching and refresh regime. This includes prioritising our maintenance activities to ensure availability of our applications, as well as prioritising application of vendor patches that provide enhanced security capability. It also includes continuing to manage the application cycle of expansion then consolidation over time, towards a modern set of application platforms that are robust and secure.

The total 2025–30 RCP forecast for the preferred option is **$77.2 million, comprising $62.8 million of capex and $14.4 million of opex**.[1] The $14.4 million of opex represents the applications' refresh costs over the RCP associated with the gradual implementation of SaaS-based applications, and hence is an inherent capex-opex shift (treated as a base-year adjustment). The 10-year net present value (**NPV**) is -$126.3 million and the overall residual risk rating is Medium, as a result of continuing these ongoing maintenance activities. Two other options were considered:

1. **Patch and upgrade of systems constrained to the recent historical average expenditure level:** This option provides a state where most business-critical systems will be patched and have changes applied. The remaining systems will be at risk of service levels not being maintained and security issues arising from system vulnerability threats when refresh rates are extended. Consequently, the overall residual risk associated with this option is High.
2. **Patch and upgrade all systems irrespective of business criticality and in accordance with vendor release schedules:** This option provides a state where all systems will be patched and have changes

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

applied, though on a more frequent basis. This option reduces the risk rating to Medium, similar to the preferred option, however, the increased cost does not represent an efficient investment.

The preferred option was selected because it enables the key program drivers by:

- balancing the efficient costs with a level of risk that is prudent for SA Power Networks to accept, in accordance with good electricity industry practice; and
- prioritising our investment to ensure business-critical applications are secure, remain online and are available to customers and staff – this is consistent with what we heard from the customer engagement, that customers expect us to keep their data safe and secure.

If this business case is funded at lower than the preferred option, not all of our business-critical IT applications will be maintained appropriately, impacting our ability to deliver energy services and remain compliant. The impact analysis modelling identifies increasing levels of risk to the health and safety of staff and customers, including life-support customers. It will also impact our ability to critically manage bushfire events to protect people, assets and property. In addition to the safety impacts, our ability to securely manage the network, its assets and associated data, and customer data, will be at risk.

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

	2025–2030 costs			10-year estimates		Residual risk rating[3]
Option	**Capex**	**Opex**	**Total**	**Benefits**	**NPV**[4]	
Option 1 – Maintain existing levels of expenditure	58.4	12.2	70.5	N/A	-115.3	High
Option 2 – Maintain existing levels of service with a prudent level of expenditure	62.8	14.4	77.2	N/A	-126.3	Medium
Option 3 – Patch and upgrade all systems based on vendor recommended cycles	86.2	15.2	101.4	N/A	-167.6	Medium

[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 is 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%.

3. Background

SA Power Networks operates a distribution network that stretches across South Australia, comprising over 90,000 kilometres of powerlines and 400+ substations. Our IT applications are an integrated portfolio of technology software packages that support all of our core processes, and therefore enable the delivery of distribution services to customers and enterprise business services.

Maintaining our portfolio of applications in a fit-for-purpose state is critical to the efficient and prudent operation and maintenance of our network. If business-critical IT applications are not maintained appropriately, it will impact our ability to deliver energy services, including:

- Health and safety of staff and customers, including life-support customers;
- Execution of all field work across the state, including outage restoration);
- Critical bushfire risk management processes that protect people, assets and property;
- Customer messaging alerts and restoration information;
- Security of customer information and the network
- Timely and accurate information to customers during outages;
- Network asset management; and
- Ability to interact with National Electricity Market (**NEM**) systems.

Our approach to maintaining our application portfolio is governed by our IT Asset Management Plan (**AMP**). The IT AMP outlines an asset management framework to ensure IT investment is prudent and targeted at managing risk and business value. We keep applications current, operational and fit for purpose by applying periodic application version upgrades, defect and/or compliance remediation, security patching, and minor enhancements to the IT applications portfolio in a timely and considered manner. Specifically, the IT AMP requires us to:

- Prioritise investment towards ensuring business-critical IT applications remain online and available to customers and staff, and are secure;
- Retain a conservative but prudent approach to maintain the supportability of, and compatibility between, our IT application and IT infrastructure assets;
- Adopt a ‘standardise, leverage and consolidate’ approach, as follows:
  - **standardise** on a core, modern set of large application suites or platforms that are robust, allow flexible selection of capability, and are more maintainable and supportable in the longer term;
  - **leverage** these standard platforms wherever possible for implementation of new capability; **and**
  - **consolidate** existing legacy systems onto these platforms over time.
- Leverage cloud technologies where it is prudent and secure to do so;
- Continuously review our IT operating model and focus on the efficient and cost-effective delivery of IT services; and
- Extend the useful life of IT assets (including our applications) by sweating the asset, when prudent, possible and secure to do so.

Applications are periodically refreshed. Factors that influence the prioritisation and timing of refreshes include:

- Customer-facing applications must be highly available, secured, and function on customer mobile devices.

- All application security vulnerabilities are remediated in accordance with the risk and threats they pose.
- Application end-of-life is managed to avoid the consequences of application vulnerabilities and failure.
- Ongoing regulatory and statutory change requirements are complied with.
- Vendor security patches are complied with as a priority.
- Patch updates applied for statutory and compliance reasons are applied as a priority, in time to meet the obligation.
- Vendor-imposed software upgrades, release cycles and cloud-based strategies are complied with, where prudent to do so.
- Resolution time for software issues is minimised.
- Testing of applications and updates to integration services are aligned to the frequency of change driven by vendors.
- Application maintenance and enhancement activities that are dependent on involvement from the business must not disrupt their seasonal business cycle, where it exists.
- The frequency of an application's changes are adjusted, as necessary, for the business functional area impacted by that application, to ensure currency and relevance of the application.
- Compatibility with external entities is maintained, so that integration and access to their services are highly available.

3.1 The scope of this business case

For ease of management, our IT applications are categorised into application platform groups, as described below.

- **Application integration:** These systems provide integration and data transfer between our various systems, as well as connection between us and third parties, such as local, state and federal governments. They also provide connectivity to the NEM, enabling us to fulfill our information and billing obligations.
- **Asset management small systems, safety and risk management:** Supports the ongoing optimisation of expenditure for electricity network asset management, replacement, service delivery and safety. It includes: asset lifecycle management; work value identification and prioritisation; asset risk cost modelling; asset sensor data management; work scheduling; identification of potential network-related fire or weather risks; safety and risk management; field asset inspection; and desktop asset inspection.
- **Asset planning and design:** These are systems for the engineering design of network infrastructure. They support customer connections, customer developments and switching of the network to ensure our field staff can work safely on the network and community safety isn't compromised.
- **Corporate systems:** These are back-office business technologies, such as finance, HR and payroll, time recording, warehouse management, project delivery, procurement, regulatory reporting and customer billing.
- **Customer systems and mobile applications:** This includes systems to support customer and third-party contractor communications, such as the SA Power Networks website, online outage/fault reporting, our customer portal and our electricians' portal.
- **Customer small systems:** These are systems that perform specific customer data management functions, including customer network billing functions (eg, self-service portal enabling customers to access their meter data and related analysis), meter reading scheduling and reporting, and meter data management and analytics.

- **Field operations systems:** The works management and scheduling system, which allows for optimisation of field crew work schedules and enables field crews to manage their tasks via mobile devices, ensuring work is performed cost-effectively and in a timely manner.
- **IT management and operations systems**: These include issue reporting and management tools, diagnostic tools, software testing tools, architecture design and planning tools, and project management tools. They support the effective management of IT systems, including facilitating faster restoration from IT outages, in turn minimising the potential for distribution network outages and customer impacts.
- **Location intelligence:** These are systems that record and manage electricity network asset geolocation information, as-built electrical connectivity and non-asset datasets to support visual problem resolution and route planning. Asset location data also supports customer-facing mobile applications, such as streetlights out, public lighting portal, vegetation management and outage map.
- **National Electricity Market systems:** These systems allow us to participate in the NEM. The systems maintain our business and market rules, ensuring compliance and our ability to perform our market participant role as the sole distribution network in South Australia. Australian Energy Market Operator (**AEMO**) publishes procedures that govern how participants, including SA Power Networks, must interact within the market. These procedures are constantly updated via industry change consultations that result in multiple rule changes each year. These rule changes require a combination of system, process, reporting and business process changes, and AEMO conducts regular audits to ensure compliance. The market transactions that are supported include network billing, customer connections, reconnections and disconnections, meter reading, including validating and provision of meter data to the market for customer billing, and market settlements, maintenance of life-support and customer data.
- **Office and collaboration tools:** These are the core customer, stakeholder, industry and internal communication mechanisms (eg, email), desktop work productivity, document management and online collaboration and communication capabilities (eg, Microsoft SharePoint, Teams).
- **Network Operations Centre systems:** These systems support the real-time delivery of electricity network services, including safety management, through the network operations control systems. This includes real-time customer outage information map services; tools for customer services staff and Network Operation Centre operators to use when communicating with customers reporting outages; provision of network configuration load information based on user demand, enabling network management; and electrical network protection device settings configuration and management information systems, which are used to isolate the wider network from electrical faults.

This business case specifically excludes the following:

- Data, analytics and intelligent systems: These activities were previously included within the IT Applications Refresh but have now been segregated into a separate business case (Data, Analytics and Intelligent Systems Refresh) as the scope and scale of the data-related activities continues to grow.
- Application refresh associated with Distributed Energy Resource (**DER**) systems: These will be newly designed and developed applications during the 2025–2030 RCP, and treated as a separate reporting category from a regulatory reporting perspective. Therefore, the expenditure is included in a separate business cases related to CER Integration and Demand Flexibility.[5]
- Infrastructure-related tooling (eg, systems monitoring etc): This is included within the recurrent IT Infrastructure Refresh Business Case.
- Major application replacements, upgrades or new capabilities: These are covered by individual non-recurrent business cases.

[5] 5.7.4 - CER Integration Business Case & 5.7.5 - Demand Flexibility Business Case

3.2 Our performance to date

The major achievements in our applications portfolio for the 2020–25 RCP were generally driven by the large (non-recurrent) replacement, upgrade and consolidation programs, as we updated our aged, large systems and consolidated onto modern platforms, putting in place the foundations for the future. The most significant changes in this regard were:

- Successfully completing the replacement of our legacy billing and national market integration systems with SAP ISU;
- Successful upgrading our ERP capabilities to SAP S4HANA; and
- Successfully consolidating our Geographic Information System (**GIS**) capabilities on to ESRI ArcGIS.

The focus of the Applications Refresh expenditure was to keep the rest of our services and systems secure and operational while these large changes were being undertaken. We continued to take the opportunity, during small-medium upgrades, to:

- consolidate our systems onto newer platforms across other functions to manage our costs, eg, planning and design legacy systems onto Autodesk, and IT service management tools onto ServiceNow; and
- gradually move to cloud versions of software, where it proved secure and financially viable.

Table 3 summarises the actuals/forecast compared to the allowance for the 2020–25 RCP, excluding the allowance reallocated to the Data, Analytics and Intelligent Systems. The overall variation compared to the allowance is a reduction of $4.8 million reflecting a reduction in recurrent activity as the very large non-recurrent upgrade and replacements undertook part of this activity at the start of the RCP.

Table 3: Actuals/forecast capex compared to allowance for the 2020–25, $m, $ June 2022 real

Cost type	2020–21	2021–22	2022–23	2023–24 FC	2024–25 FC	Total 2020–25
Allowance (exc. Data, analytics and intelligent systems expenditure)	15.3	14.7	11.3	11.1	13.5	66.0
Actual/forecast (FC)	13.4	10.1	11.6	11.3	14.8	61.2
Difference	**-1.9**	**-4.6**	**0.3**	**0.2**	**1.3**	**-4.8**

As detailed in Figure 1, below, going into the 2020–25 RCP, we planned a ’dip’ in the recurrent ICT applications investment compared to the 2015–20 expenditure, due to our large non-recurrent replacement and upgrade programs (ie, billing replacement, GIS consolidation) undertaking some of the recurrent refresh activity. We did, however, expect the costs to start increasing again at the end of the RCP, as the systems we had recently replaced started to require ongoing investment to maintain the value created during their replacements, as well as the provision of security updates and patches for these new platforms.

The ‘dip’ occurred earlier than expected in the RCP as we found it far more efficient to deliver the very large programs serially early in the RCP, with the same Program management teams, with no gaps in between as we had originally planned.

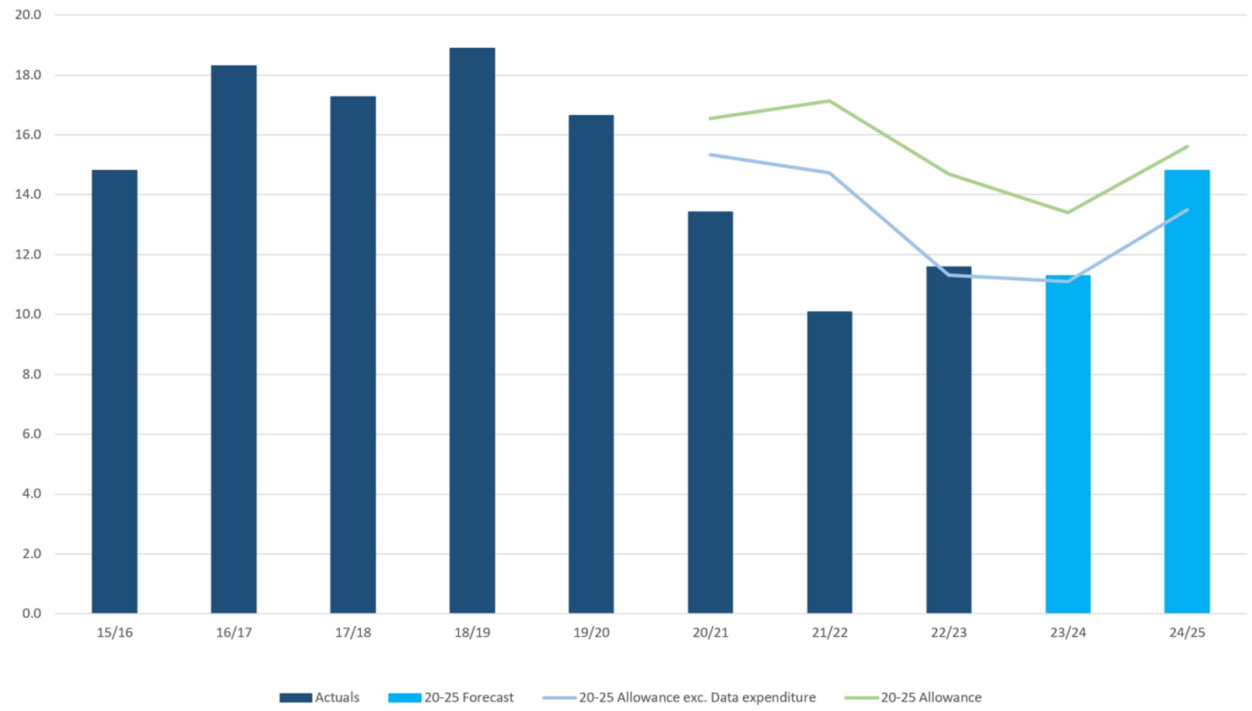


Figure 1: 2015–20 vs 2020–25 Recurrent ICT Applications allowance and actuals

Table 4 summarises the key changes that have impacted on the IT Application Refresh allowance during the RCP.

Table 4: Allowance to Forecast key changes 2020-25, $m, $ June 2022 real.

Component	Amount
Initial IT Applications Allowance (2020-25)	77.4
Reallocate to Data, Analytics and Intelligent Systems Refresh	- 11.4
Recurrent activity reduced due to large non-recurrent projects	-4.8
Actuals / Forecast 2020-25	**61.2**

Shifted allowance to refresh data capabilities

A significant increase in the number and capability of our enterprise data systems has resulted in a growing requirement for recurrent investment to support these systems. This is particularly for analytics, reporting and visualisation systems, centralised database and content management systems, and our enterprise data platform. While an allowance for this was included within IT Applications, the rapid development of a number of key systems meant we needed to allocate more recurrent investment to maintain these systems. In the 2025–30 funding submission, we now separate these data systems out into their own category[6].

3.3 Drivers for change

Patching, updating and maintaining applications is a necessary recurring requirement. There are several key drivers for an increased level of activity in the 2025–30 period, and these are described below.

[6] See the 5.12.8 - Data, Analytics & Intelligent Systems Refresh Business Case

Uplifts in compliance requirements during the 2020–25 RCP

During the 2020–25 RCP, we experienced increases in two sets of costs associated with maintaining our compliance, and we expect these will continue to grow into the next RCP:

1. Increased National Market minor enhancements to enable the energy transition, resulting from ongoing strategic national programs, such as the NEM Reform Roadmap. We expect these will grow to an average additional $1.0 million per annum across the 2025–30 period.
2. The ATO STP changes, which require significant uplifts on an ongoing basis, eg, superannuation reporting is next on the list. The estimated cost for meeting these requirements is expected to grow to $0.77 million per annum in the next RCP.

Maintaining our investment value in our new strategic platforms

As discussed in Section 3.2, we have implemented new strategic platforms over the last several years, predominantly as part of the replacement and upgrade program. This amounts to $170 million of non-recurrent expenditure. While the systems are brand new, they require lower levels of refresh and updates. As time passes, refresh costs increase and maintaining those systems; therefore, costs will be slightly more in the next RCP. Hence, this expenditure is fundamentally about maintaining and securing the investment value we have already created.

Maintaining secure and reliable IT applications within an increasing cyber security risk environment

Securing critical infrastructure continues to be recognised as a key challenge for the utilities sector. One of the most effective defence mechanisms against cyber security threats is regularly updating and patching application software, as this reduces vulnerabilities and therefore the likelihood of a security breach. As applications increasingly move to cloud environments and/or to sharing more with external parties, regularly updating applications has become a core part of securing our network infrastructure.

Changing recurrent capex to opex as more applications are moved to software as a service (SaaS)

Existing software products are gradually being transitioned to the cloud by vendors, and this delivery of SaaS is expected to continue over the foreseeable future. Accounting rule clarification in early 2021[7] confirmed that the costs of configuring and customising application software in a cloud-computing or SaaS arrangement should not be capitalised, with the business no longer having control over the asset. The effect of this is to require this component of IT application refresh work to be expensed, switching from capex to opex, as these products transition to cloud-based.

Recategorising IT management and operations investment expenditure into IT applications

Previously, we reported a separate category of IT Management and Operations under ICT recurrent expenditure within our Regulatory Information Notice (**RIN**) reports. This expenditure is principally related to the IT Applications and amounted to ~$5m over the RCP. To simplify our reporting and management, we have moved the majority of this forecast into IT Applications for the 2025–30 proposal.[8]

Maintaining the growing portfolio of mobile applications

To further enable our mobile workforce and meet the information demands of our customers, SA Power Networks have continued to deliver mobile applications in the 2020-25 RCP. This increasing portfolio of apps requires ongoing refresh to ensure the high levels of availability and security are maintained.

[7] International Financial Reporting Interpretations Committee, March 2021

[8] The remaining estimates have been allocated into the other recurrent business cases.

3.4 Industry practice

Our approach described in this business case is consistent with good industry practice. Comparable businesses have similar programs to provide system maintenance and the prudent application of software vendor patches.

4. The identified need

The need is to maintain our existing services, levels of risk and overall investment value through the regular refresh and updates of our application portfolio. Our IT applications support all of our customer and business processes, and therefore enable us to deliver distribution services to customers and enterprise business services. They ensure our workforce can respond to customer and network issues, receive job information in the field, access critical asset and service information, and update customers with timely information on progress. They also facilitate efficient collaboration between workers located at different sites.

Our applications must therefore be fit for purpose and reliable to ensure we can maintain our existing services and manage service risk. This is achieved through the prudent, systematic, and timely refresh of applications to maintain them in a fit state, mitigate cyber security risk and ensure efficient business performance.

These requirements are balanced with cost-effectiveness. This requires prudent application of vendor-prescribed patch updates, extending the life of the existing versions where prudent and appropriate to do so, based on business criticality and risk.

5. Comparison of options

5.1 The options considered

Table 5, below, summarises the three options that have been considered for the Applications Refresh program.

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 level of the last five years. In effect, this option does not take into account that our application base has grown over recent years and requires maintaining and patching on an ongoing basis. This option provides a state where *most* critical systems are patched, maintained and upgraded in a timely manner, in line with our asset management strategy and principles and vendor-prescribed refresh cycles. Applications are prioritised using a risk-based approach. This option would result in some critical work being deferred into the following period at high risk to those applications.
Option 2 – Maintain existing levels of service with a prudent level of expenditure	This option involves maintaining our existing service levels via a risk-based approach to managing IT applications, reflecting prudent management of the larger application base. This option provides a state where systems are patched, upgraded and supported in a prudent, timely and effective manner, in line with our asset management principles and vendor-prescribed refresh cycles. Under this option, all critical application refresh work is funded.
Option 3 – Patch and upgrade all systems	Patch and upgrade of all systems, irrespective of business criticality and in accordance with vendor release schedules. This option provides a state where all systems would be patched, upgraded and supported according to the release schedules provided by vendors. Under this option, all critical application refresh work is funded. Version upgrades are applied promptly when these become available from vendors. In addition, this option caters for some minor enhancements to systems that are over and above that which is included in vendor updates.

5.2 Options investigated but deemed non-credible

Any option that involves doing nothing, or investing less than current spend levels, has not been considered, as these options would result in:

- failure to apply critical vendor patches that mitigate cyber security risks;
- failure to keep our systems compliant with regulatory obligations, including National Market requirements and the ATO STP requirements;
- applications that are not fit for purpose and potentially unavailable for use when required; and
- non-compliance with our risk management framework, with a resulting High or Extreme residual risk as at the end of the RCP.

5.3 Analysis summary and recommended option

5.3.1 Options assessment results

Table 6: Costs, benefits and risks of alternative options relative to the base case, $m, $ Jun 2022 real

	10-year program/ project costs			2025–30 program/ project costs			10-year benefits[9]	10-year NPV[10]	Overall risk rating[11]	Ranking
	Capex	Opex	Total	Capex	Opex	Total				
Option 1 – Maintain existing levels of expenditure	114.5	25.0	139.4	58.4	12.2	70.5	n/a	-115.3	High	3
Option 2 – Maintain existing levels of service with a prudent level of expenditure **(Recommended)**	123.7	29.5	153.2	62.8	14.4	77.2	n/a	-126.3	**Medium**	1
Option 3 – Patch and upgrade all systems based on vendor schedules	171.8	31.0	202.8	86.2	15.2	101.4	n/a	-167.6	**Medium**	2

5.3.2 Recommended option

The recommended option is Option 2 – a risk-based approach that extends the useful life of IT applications by adopting a prudent and systematic approach to patching and upgrades.

Option 2 has been selected as it enables us to achieve the expenditure objectives and ensures continued compliance with our regulatory obligations. It balances efficient costs with a level of risk that is prudent, in accordance with good electricity industry practice. Option 2:

- Provides continued supportability of, and compatibility between, SA Power Networks' IT applications.
- Ensures that services and information are available when they are needed for both staff and customers.
- Ensures timely vendor patching to mitigate new cyber security threats.
- Supports the key drivers, including an increased level of NEM and ATO obligations.

Option 1 requires necessary refresh activities for some systems to be deferred into the following regulatory period. This would result in higher than acceptable risks to the security and reliability of those applications, and therefore does not meet the actions of a prudent service provider.

While Option 3 does provide some additional benefits (eg, minor enhancements), it requires significant additional expenditure. This option would not represent a prudent level of investment.

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

[10] Net present value (NPV) of the proposal over 10-year cash flow period from 1 July 2025 to 30 June 2035, based on discount rate of 4.05%.

[11] The overall risk level for each option after the proposed option implemented. Refer to Appendix C - for details.

Figure 2 summarises the levels of spend over respective RCPs. In 2025-30 SA Power Networks will revert to prudent levels of application refresh– but which is similar to the 2015-20 expenditure, taking into account the reallocation to the data and analytics systems expenditure.

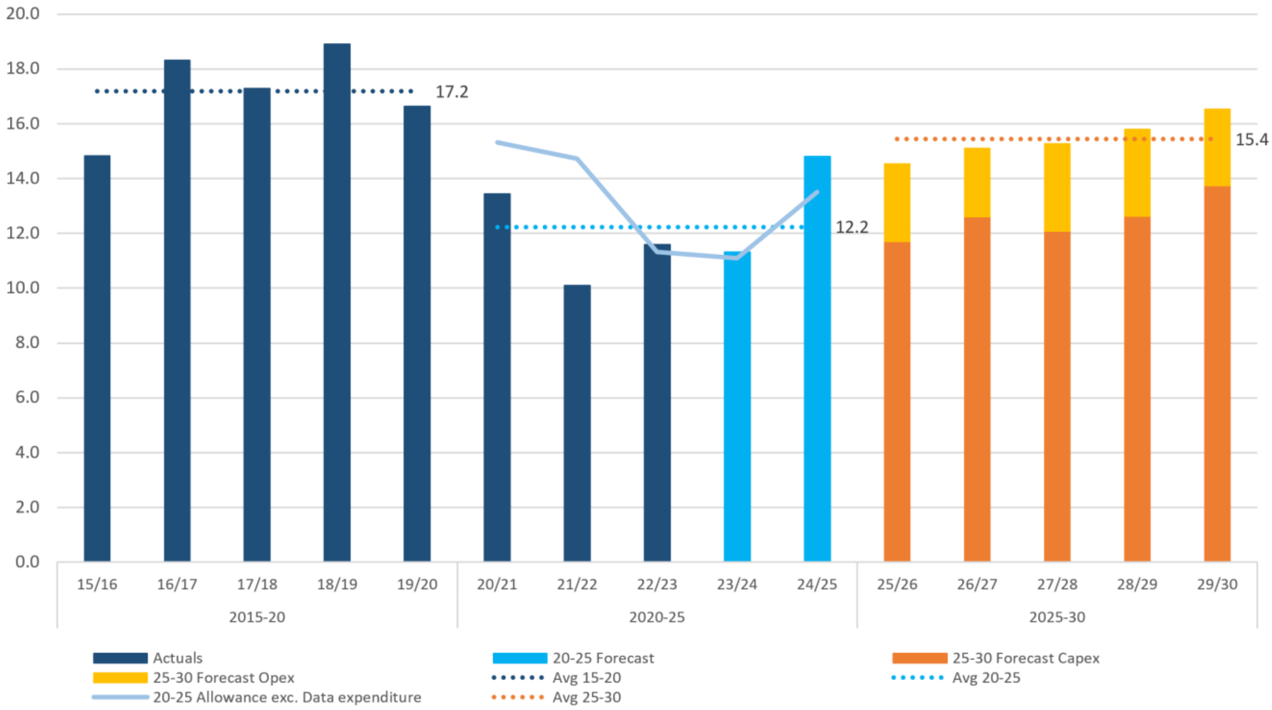


Figure 2: Applications Refresh trend over time

Table 7 summarises the key changes from the 2020-25 RCP forecast to the 2025-30 funding request. The drivers are laid out in more detail in Section 3.3.

Table 7: The changes from the 2020-25 forecast to the 2025-30 forecast, $m, $ June 2022 real.

Component	Amount ($m)
Actuals / Forecast 2020-25	**61.2**
Ongoing refresh of new mobile apps delivered in 2020-25 RCP	+3.5
Additional NEM and ATO compliance activities	+4.8
Return to normal expenditure t**o refresh new core applications**	+4.8
IT Management, Risk and Governance (previously in a separate business case)	+2.8
Forecast for 2025-30	**77.2**

Appendix A provides the links to the cost and benefit models for each option. Appendix B details the SaaS opex adjustments request for the preferred option. Appendix C provides the detailed risk analysis for each option.

5.4 Option 1 – Maintain existing levels of expenditure

5.4.1 Description

This option proposes investing in patching, maintenance and upgrades for applications at a level constrained to that of our most recent five years of historical spend.

This would provide a state where most systems are patched, upgraded and supported in an effective manner in line with our asset management strategy and principles. It results in applying vendor-prescribed system updates on a case-by-case basis, considering the criticality of the application and the risk implications. Refresh work is deferred, where prudent and appropriate to do so.

Under this option, necessary refresh activities for some systems would need to be deferred into the following regulatory period at high risk to those applications. Additional prioritisation activities would ensure the most critical work is completed. For example:

- Legislative, statutory and regulatory compliance change (eg, payroll changes).
- Changes in feeder systems external to SA Power Networks (eg, weather website data).
- Changes to external processes SA Power Networks is a participant in (eg Dial Before You Dig).

However, the utility of the applications will degrade over time without the ability to make small adjustments to adapt to the changing environment.

5.4.2 Costs

The forecast for Option 1 has been determined on a top-down basis, based on revealed average actual expenditure over the last five years, as per Table 8.

Table 8: Last five years actual expenditure: 2018–19 to 2022–23 ($m June 2022 real)

Cost type	2018-19	2019–20	2020–21	2021–22	2022–23	Total	Average
Capex	18.9	16.6	13.4	10.1	11.6	**70.6**	**14.1**

Total costs for this option are $70.5 million, including $58.4 million capex and $12.2 million opex, as profiled in Table 9.

Table 9: Option 1 – Costs by cost type ($m June 2022 real)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025 – 30
Capex	12.7	11.8	10.6	11.5	11.8	**58.4**
Opex	2.7	2.0	2.7	2.7	2.0	**12.2**
Total	**15.4**	**13.9**	**13.3**	**14.2**	**13.8**	**70.5**

Table 10 provides breakdowns of the capital and operating forecasts required for this option. This reflects a bottom-up forecast that meets the five-year historical expenditure level, ensuring funding for the highest priority systems and activities within each application group.

Table 10: Option 1 Total by Application Group ($m June 2022 Real)

Application platform group	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Application integration	0.6	0.6	0.6	0.6	0.6	**3.0**
Asset management	0.6	0.6	0.6	0.6	0.6	**3.2**
Corporate systems	3.3	2.5	3.0	3.3	2.5	**14.7**
Customer-facing systems	0.6	0.3	0.3	0.3	0.6	**2.0**
Customer small systems	1.0	1.0	1.0	1.0	1.0	**4.9**
Design and engineering	1.0	1.0	1.0	1.0	1.0	**4.8**
Field operations systems	1.0	1.0	1.0	1.0	1.0	**4.9**
IT management and operations systems	0.9	0.9	0.9	0.9	0.9	**4.6**
Location intelligence	1.2	1.2	1.2	1.2	1.2	**5.9**
National Electricity Market	3.6	3.6	3.1	3.6	3.6	**17.6**
Network operations	1.2	0.8	0.4	0.4	0.4	**3.1**
Office productivity	0.4	0.4	0.4	0.4	0.4	**1.9**
Total capex	**15.4**	**13.8**	**13.3**	**14.2**	**13.8**	**70.5**

As discussed in Section 3.3, recent accounting treatment clarifications now require SaaS-based products to be classified as opex, to comply with accounting standards. Any Applications Refresh costs associated with our SaaS applications is being treated as capex in the regulatory accounts in the current RCP. Consistent with Australian Energy Regulator (**AER**) guidance, this is to be transitioned to opex as at the start of the regulatory period as a base-year opex adjustment. Impacted applications are included in Appendix C.

5.4.3 Risks

Table 11: Option 1 – Risk assessment summary

Risk consequence category	Residual risk level (Option 1)	Residual risk Level (Do nothing)
Safety – Harm to a worker, contractor or member of the public	High	Extreme
Performance and growth – Financial impact – Cash or earning impacts	Medium	High
Performance and growth – Financial impact – Litigation and/or penalties	High	Extreme
Network – Failure to transport electricity from source to load	High	Extreme
Customers – Failure to deliver on customer expectations	High	Extreme
Culture and workforce – Misalignment in the beliefs and behaviours of workers, management and customers	Medium	High
Technology – Disruption of access to, or use of, systems	High	Extreme
Technology – Unauthorised access, modification, or control of systems	High	Extreme
Technology – Unauthorised access and disclosure of information	High	Extreme
Overall risk level	High	Extreme

The residual risk level associated with Option 1 is High. This is driven by potential Catastrophic consequence associated with Safety, Network, Customer and Performance risk events.

5.4.4 Quantified benefits

Tangible benefits have not been assessed for this business case, and as such there are no tangible quantifiable benefits associated with this option.

5.4.5 Unquantified benefits

Option 1 results in most of our applications being maintained at a level that enables the provision of safe, secure and reliable distribution services, consistent with our IT AMP. It means continued compliance with our regulatory obligations and updates to our most critical business systems.

However, the lower level of funding available would result in higher than acceptable risks to the security and reliability of those applications where the refresh time has been extended.

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

5.5.1 Description

This option proposes a prudent and timely approach to patching, maintenance and upgrades for applications, providing a state where systems are patched, upgraded and supported in an effective manner in line with our asset management strategy and principles. It results in applying vendor prescribed system updates on a case-by-case basis, considering the criticality of the application and the risk implications. Refresh work is deferred where prudent and appropriate to do so.

As noted in Section 3.3, we have invested $170 million in new strategic platforms over the last several years and need to ensure we appropriately maintain this significant investment. Investment levels under Option 2 cater for increased maintenance requirements associated with new systems, as well as new compliance obligations (eg, STP) and the additional frequency and complexity of systems patching to support new cyber security functionality software.

While there has been a reduction in the long-term level of investment in Applications Refresh from the levels seen in previous RCPs, the 2025–30 period requires a higher amount of investment than will be spent in the current 2020–25 period. This is shown in Figure 2, above.

5.5.2 Costs

The forecast for Option 2 has been prepared on a bottom-up basis by determining the frequency of each type of system refresh and applying to this an efficient unit cost for this upgrade type. Total costs of $77.2 million for this option include $62.8 million capex and $14.4 million new opex, as profiled in Table 12.

Table 12: Option 2 – Total cost by cost type ($m June 2022 real)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Capex	11.7	12.6	12.1	12.6	13.8	**62.8**
Opex	2.8	2.5	3.2	3.2	2.8	**14.4**
Total	**14.5**	**15.1**	**15.3**	**15.8**	**16.5**	**77.2**

Table 13 provides breakdowns of the capital and operating forecasts required for this option.

Table 13: Option 2 – Total by application ($m June 2022 real)

Application platform group	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Application integration	0.5	0.6	0.6	0.6	0.7	**3.1**
Asset management	0.6	0.7	0.7	0.7	0.7	**3.3**
Corporate systems	3.3	2.9	3.8	3.7	3.3	**17.1**
Customer-facing systems	0.4	0.4	0.8	0.8	0.5	**2.9**
Customer small systems	1.1	1.2	1.2	1.2	1.4	**6.2**
Design and engineering	0.8	1.0	1.0	1.0	1.1	**4.8**
Field operations systems	0.9	1.0	1.0	1.0	1.1	**5.0**
IT management and operations systems	0.9	1.0	1.0	1.0	1.2	**5.3**
Location intelligence	1.2	1.4	1.4	1.4	1.6	**7.0**
National Electricity Market	3.2	3.6	3.1	3.6	4.1	**17.6**
Network operations	1.1	0.8	0.4	0.4	0.5	**3.2**
Office productivity	0.3	0.4	0.4	0.4	0.4	**1.9**
Total	**14.5**	**15.1**	**15.3**	**15.8**	**16.5**	**77.2**

As discussed in Section 3.3, recent accounting treatment clarifications now require SaaS-based products to be classified as opex to comply with accounting standards. Any Applications Refresh costs associated with the SaaS applications is being treated as capex in the regulatory accounts in the current RCP. Consistent with AER guidance, this is to be transitioned to opex as at the start of the regulatory period as a base-year opex adjustment. Impacted applications are included in Appendix C.

5.5.3 Risks

Table 14: Option 2 – Risk assessment summary

Risk consequence category	Residual risk level (Option 2)	Residual risk level (Do nothing)
Safety – Harm to a worker, contractor or member of the public	Medium	Extreme
Performance and growth – Financial impact – Cash or earning impacts	Low	High
Performance and growth – Financial impact – Litigation and/or penalties	Medium	Extreme
Network – Failure to transport electricity from source to load	Medium	Extreme
Customers – Failure to deliver on customer expectations	Medium	Extreme
Culture and Workforce – Misalignment in the beliefs and behaviours of workers, management and customers	Low	High
Technology – Disruption of access to, or use of, systems	Medium	Extreme
Technology – Unauthorised access, modification, or control of systems	Medium	Extreme
Technology – Unauthorised access and disclosure of information	Medium	Extreme
Overall risk level	Medium	Extreme

Under this option, consequence ratings for all risk events move from Unlikely to Rare. This results in a Medium residual risk as at the end of the 2025–30 RCP.

5.5.4 Quantified benefits

Tangible benefits have not been assessed for this business case, and as such there are no tangible quantifiable benefits associated with this option.

5.5.5 Unquantified benefits

Option 2 means that applications are patched, upgraded, managed and secured at a level that can reliably support the needs of the business, and allows for the provision of safe, secure and reliable distribution services. It means:

- Our customer and network services are maintained and secured.
- The continued supportability of, and compatibility between, SA Power Networks' IT applications.
- Operational staff have access to critical safety and job information when they need it, to enable the safe and efficient delivery of energy services.
- Services and information are available when they are needed for both staff and customers.
- Continued compliance with our regulatory obligations.

5.6 Option 3 – Patch and upgrade all systems based on vendor schedules

5.6.1 Description

Option 3 is to patch and upgrade all systems, irrespective of business criticality, based on vendor patch-release schedules.

This option takes a conservative approach to IT application security, reliability and vendor support, where all applications would be patched and maintained without reference to their relative importance to our day-to-day business activities. As per Option 2, investment levels under this option cater for increased maintenance requirements associated with new systems, as well as new compliance obligations (eg, STP) and the additional frequency and complexity of systems patching to support new cyber security functionality software.

5.6.2 Costs

The forecast for Option 3 has been prepared on a bottom-up basis by determining the frequency of each type of system refresh and applying to this an efficient unit cost for this upgrade type. The refresh rate for some systems is reduced under this option. Total costs of $101.4 million for this option include $86.2 million capex and $15.2 million opex, as profiled in Table 15 below.

Table 15: Option 3 – Costs by cost type ($m June 2022 real)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Capex	17.9	17.3	16.8	16.8	17.3	**86.2**
Opex	3.3	2.6	3.3	3.3	2.6	**15.2**
Total	**21.3**	**19.9**	**20.1**	**20.1**	**20.0**	**101.4**

Table 16 provides breakdowns of the capital and operating forecasts required for this option. Consistent with the other options, the opex forecast covers the cost of upgrading the listed SaaS applications.

Table 16: Option 3 – Total by application ($m June 2022 real)

Application platform group	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Application integration	0.9	0.9	0.9	0.9	0.9	**4.4**
Asset management	1.0	1.0	1.0	1.0	1.0	**5.1**
Corporate systems	5.2	4.4	5.2	5.2	4.4	**24.4**
Customer-facing systems	0.8	0.7	0.7	0.7	0.8	**3.8**
Customer small systems	1.2	1.2	1.2	1.2	1.2	**6.2**
Design and engineering	1.6	1.6	1.6	1.6	1.6	**7.8**
Field operations systems	1.1	1.1	1.1	1.1	1.1	**5.5**
IT management and operations systems	1.2	1.2	1.2	1.2	1.2	**5.9**
Location intelligence	1.9	1.9	1.9	1.9	1.9	**9.6**
National Electricity Market	4.5	4.5	4.5	4.5	4.5	**22.4**
Network operations	1.5	1.0	0.5	0.5	1.0	**4.5**
Office productivity	0.4	0.4	0.4	0.4	0.4	**1.9**
Total	**21.3**	**19.9**	**20.1**	**20.1**	**20.0**	**101.4**

5.6.3 Risks

Table 17: Option 3 – Risk assessment summary

Risk consequence category	Residual risk level (Option 3)	Residual risk level (Do nothing)
Safety – Harm to a worker, contractor or member of the public	Medium	Extreme
Performance and growth – Financial impact – Cash or earning impacts	Low	High
Performance and growth – Financial impact – Litigation and/or penalties	Medium	Extreme
Network – Failure to transport electricity from source to load	Medium	Extreme
Customers – Failure to deliver on customer expectations	Medium	Extreme
Culture and workforce – Misalignment in the beliefs and behaviours of workers, management and customers	Low	High
Technology – Disruption of access to, or use of, systems	Medium	Extreme
Technology – Unauthorised access, modification, or control of systems	Medium	Extreme
Technology – Unauthorised access and disclosure of information	Medium	Extreme
Overall risk level	Medium	Extreme

The likelihood of the risk occurring under all of the identified risk scenarios is the same under Option 3 as Option 2.

5.6.4 Quantified benefits

Tangible benefits have not been assessed for this business case, and as such there are no tangible quantifiable benefits associated with this option.

5.6.5 Unquantified benefits

Option 3 results in all applications being maintained in line with vendor schedules. It means that applications are patched, upgraded, managed and secured at a level that supports the needs of the business, and allows for the provision of safe, secure and reliable distribution services. Consistent with option 2, this means:

- Continued supportability of, and compatibility between, SA Power Networks' IT applications.
- Operational staff have access to critical safety and job information when they need it, to enable the safe and efficient delivery of energy services.
- Services and information are available when they are needed for both staff and customers.
- Continued compliance with our regulatory obligations.

An added benefit is that this option requires less proactive management of the IT applications portfolio, as there is no need to apply a prioritisation lens as business criticality changes over time. In addition, this option provides for minor enhancements to systems, outside of those included as part of vendor patches.

6. Deliverability of recommended option

Delivery of the Applications Refresh program is coordinated and monitored by our Corporate Project Management office and executed by the respective teams that have accountability for each application platform group. This is a mature and stable capability.

The level of application refresh activity proposed is consistent with what has been delivered in recent history. There are no expected resourcing or delivery issues associated with delivering this program in the 2025–30 period.

7. How the recommended option aligns with our engagement

Customers expect that we will maintain our existing levels of risk. The recommended investment ensures our applications are fit for purpose to enable SA Power Networks to continue to deliver a reliable, resilient and safe electricity network and access to information and services for our customers.

This program is consistent with the high importance that our customers attributed to cyber security and the privacy of their data at our People's Panel forum.

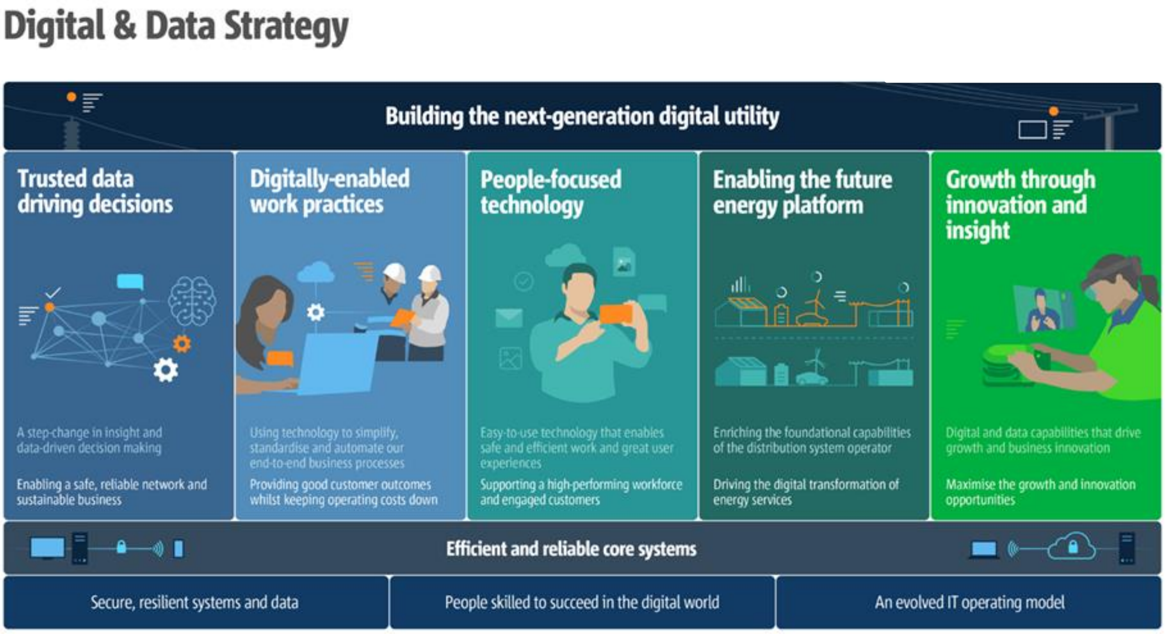
As part of the Focused Conversation stages of the customer engagement, we presented the costs for this business case as 'for information' at the IT workshop with the Consumer Advisory Board. These costs were included in Scenario 1 – Business as Usual for all other customer workshops and pricing analysis.

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 3, below.

The strategy describes core components of the '*Efficient and reliable core IT systems*' enabler that includes:

- Keeping core systems and applications operational, current and maintained to an acceptable level of risk
- Systems and data remain secure via regular patching and updates
- Continued application and to decrease the risk profile of our legacy environment



Digital & Data Strategy

Building the next-generation digital utility

Trusted data driving decisions

A step-change in insight and data-driven decision making

Enabling a safe, reliable network and sustainable business

Digitally-enabled work practices

Using technology to simplify, standardise and automate our end-to-end business processes

Providing good customer outcomes whilst keeping operating costs down

People-focused technology

Easy-to-use technology that enables safe and efficient work and great user experiences

Supporting a high-performing workforce and engaged customers

Enabling the future energy platform

Enriching the foundational capabilities of the distribution system operator

Driving the digital transformation of energy services

Growth through innovation and insight

Digital and data capabilities that drive growth and business innovation

Maximise the growth and innovation opportunities

Efficient and reliable core systems

Secure, resilient systems and data

People skilled to succeed in the digital world

An evolved IT operating model

Figure 3: SA Power Networks Digital & Data Strategy

9. Reasonableness of cost and benefit estimates

The bottom-up cost estimates for this business case have been validated using historical trends on an application by application basis, then modified by our mature top-down application criticality and prioritisation approach. We manage our risk effectively but do not just follow the vendor release schedules.

10. Reasonableness of input assumptions

Pricing is competitive and is based on a prudent market selection process by our procurement team, for ICT services. The costs are reflective of competitive market rates for the blend of internal resources and external resources/professional ICT services required to deliver our applications portfolio investment initiatives.

Refresh rates for the preferred option reflect our historically evidenced refresh rates and vendor upgrade paths.

A. Appendix A – Cost Models

Option 1:

2025 – 30 Reset – Applications Refresh forecast template – Option 1.xlsm

Option 2:

2025 – 30 Reset – Applications Refresh forecast template – Option 2 Preferred.xlsm

Option 3:

2025 – 30 Reset – Applications Refresh forecast template – Option 3.xlsm

B. Appendix B: Base-year opex adjustment (preferred option)

Category	Application function	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025 – 30
Base-year adjustment: Accounting treatment change	Corporate systems	1.7	1.2	1.9	1.9	1.4	8.1
	Customer small systems	0.4	0.4	0.4	0.4	0.5	2.2
	Field operations systems	0.2	0.2	0.2	0.2	0.3	1.2
	IT management and operations systems	0.2	0.2	0.2	0.2	0.3	1.1
	Office productivity	0.3	0.3	0.3	0.3	0.4	1.7
	Total base-year opex adjustment	**2.8**	**2.5**	**3.2**	**3.2**	**2.8**	**14.4**

Accounting treatment change

Topic	Detail
Background	Accounting rule clarification in early 2021 confirmed that the costs of configuring and customising application software in a cloud-computing or SaaS arrangement should not be capitalised, with the business no longer having control over the asset. The effect of this is to require this component of IT application refresh work to be expensed, switching from capex to opex as these products transition from local data centres to cloud-based hosting. For 2025–30, examples of the impacted applications are Microsoft 365, Project Online, ServiceNow, SAP Success Factors, SAP ALM, SAP Budgeting Planning Consolidation, SAP Concur.
Request	A base-year opex adjustment of $14.4 million as substitution for a similar value of capex.

C. Appendix C – Risk assessment

				Current risk Current runrate (Option 1)			Residual risk – Maintain existing risk (preferred) (Option 2)			Residual risk – All upgrades (Option 3)			Residual Risk – Do nothing		
ID	**Risk scenario**	**Consequence description**	**Consequence category**	**Consequence**	**Likelihood**	**Risk Level**	**Consequence**	**Likelihood**	**Risk Level**	**Consequence**	**Likelihood**	**Risk Level**	**Consequence**	**Likelihood**	**Risk Level**
1	Applications pass the end of their useful lives and aren't fit for purpose, or stop functioning entirely.	Untimely or no detection and correction of network faults, causing increased frequency and duration of network outages for customers. Inability to identify, notify and maintain reliability of supply to our ~9,500 critical and life-support customers. Inability to accurately identify impacts of switching activities in the field through lack of GIS information. This can have WH&S consequences for Field Services personnel, other emergency services personnel, and the general public, particularly during severe weather events.	**Network** – Failure to transport electricity from source to load	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)
			Customer – Failure to deliver on customer expectations	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)
			Performance and growth – Financial impact – Litigation and/or penalties	4	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)
			Safety – Harm to a worker, contractor, or member of the public	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)

		Inability to proactively manage the network, in particular, to effectively and efficiently perform planned asset maintenance, including identifying, planning and scheduling inspections and maintenance work. These tasks require data that is maintained within various IT systems.	**Network** – Failure to transport electricity from source to load	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)
			Performance and growth – Financial impact – Litigation and/or penalties	4	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)
		Ineffective management of emergency response field crews, including in dealing with management of bushfire risks. This requires several systems integrated together to enable determination of when critical assets should be switched off to protect customers or properly report on and manage vegetation-related risks. In the event of bushfire caused by SA Power Networks, in addition to loss of life and property, there could be significant penalties from regulators and aggrieved party legal actions.	**Network** – Failure to transport electricity from source to load	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)
			Customer – Failure to deliver on customer expectations	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)
			Performance and growth – Financial impact – Litigation and/or penalties	4	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)
			Safety – Harm to a worker, contractor, or member of the public	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)

		Market billing – ability to generate DUoS billing to retailers impeded, placing the main corporate cashflow at risk and potentially restricting business operations.	**Performance and growth** – Financial impact – Cash or earning impacts	4	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)
		Legal compliance – Unable to efficiently implement regulatory compliance changes to IT systems, such as payroll, superannuation, tax changes and Australian Securities and Investments Commission mandated alterations to accounting standards, exposing us and our directors to market and statutory penalties. HR issues due to incorrect application of tax rates and superannuation could lead to issues with workforce, including industrial action. NEM obligations could potentially be compromised by delayed processing of customer transactions, resulting in significant non-compliance penalties.	**Performance and growth** – Financial impact – Cash or earning impacts	4	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)
			Culture and workforce – Misalignment in the beliefs and behaviours of workers, management and customers	4	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)
			Customer – Failure to deliver on customer expectations	4	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)
		Regulatory and reliability reporting – Ability to generate accurate regulatory and reliability reporting, which is heavily dependent on IT systems, could be compromised.	**Customer** – Failure to deliver on customer expectations	4	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)
			Performance and growth – Financial impact – Cash or earning impacts	4	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)

2	Cyber security event leads to unauthorised access to, or corruption of, data of unsupported application.	Security – The vulnerability of an IT system to security breaches is related to its security configuration and encryption levels, and whether regular security patching is being applied. 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	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)
			Customer – Failure to deliver on customer expectations	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)
			Performance and growth – Financial impact – Litigation and/or penalties	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	5	Extreme (9)
			Safety – Harm to a worker, contractor, or member of the public	4	2	Medium (6)	4	1	Low (5)	4	1	Low (5)	4	4	High (8)
			Technology – Disruption of access to, or use of, systems	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)
			Technology – Unauthorised access, modification, or control of systems	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)
			Technology – Unauthorised access and disclosure of information	5	2	High (7)	5	1	Medium (6)	5	1	Medium (6)	5	4	Extreme (9)
			Overall risk level[12]			High			Medium			Medium			Extreme

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