



Supporting
document 6.2

IT Applications Refresh Business Case

2020-2025
Regulatory Proposal
January 2019





SA Power Networks

IT Applications Refresh Business Case



IT regulatory submission for the 2020-25 regulatory control period

31/1/2019 – 0.18

Contents

Contents	2
1. Executive Summary	3
2. Drivers	10
2.1 Introduction.....	10
2.2 Factors that influence IT Applications maintenance	13
2.3 Issues and risks associated with not proceeding.....	14
2.4 Detailed description of drivers	19
3. Scope	21
3.1 In Scope	21
3.1.1 Asset Location Information	21
3.1.2 Asset Management Small Systems and Safety & Risk Management	22
3.1.3 Asset Planning and Design.....	22
3.1.4 Customer Facing Website and Customer Mobile Applications	23
3.1.5 Customer Small Systems.....	23
3.1.6 IT Management Systems	24
3.1.7 National Electricity Market Systems.....	24
3.1.8 Network Operations Centre Systems	24
3.1.9 Office and Collaboration Tools	25
3.1.10 SAP Suite (including Analytics and Reporting and Corporate Systems)	25
3.1.11 Works Management and Scheduling.....	26
3.2 Out of Scope	26
4. Options Assessment	27
4.1 Options considered.....	27
4.2 Options assessment.....	27
4.3 Costs, benefits and risks of Option 1	28
4.4 Costs, benefits and risks of Option 2	34
4.5 Summary of cost, benefit and risk assessment of each option.....	40
4.6 Option selected	42
4.7 Supporting evidence.....	42
4.8 Dependencies	42
4.9 Regulatory framework.....	43
Glossary.....	45
A. Appendix A: SA Power Networks Risk Management Framework	46
B. Appendix B: Click capex to opex substitution step change proposal.....	48
C. Appendix C: Cost Model.....	50

1. Executive Summary

Topic	Detail
Category of expenditure	<ul style="list-style-type: none"> Recurrent non-network Information Technology (IT) capital expenditure (capex) Operating expenditure (opex) step change from efficient capex to opex substitution
Context / background	<p>SA Power Networks' IT Applications are an integrated portfolio of technology software packages comprising approximately 80 supported applications. An example of an application is Enablon which is software platform used for safety and risk management registration, tracking and compliance reporting.</p> <p>The forecast recurrent non-network IT capex for IT Applications relates to the delivery of periodic application version upgrades, defect and/or compliance remediation, security patching and minor enhancements over the 2020-25 regulatory control period (RCP) for that portfolio.</p> <p>The IT Applications portfolio enables the delivery of distribution services for customers and efficient and effective management of our distribution network. The portfolio includes software packages for:</p> <ul style="list-style-type: none"> asset management; safety and risk management; asset planning and design; asset location information systems; works management and scheduling; customer facing websites and customer mobile applications; workforce mobility; customer network billing; national electricity market systems; Network Operations Centre systems; analytics and reporting systems; corporate systems (eg finance, payroll, HR, procurement); office and collaboration software; and IT management systems. <p>To balance risk and cost with the need to keep the IT Applications portfolio fit for purpose we have used a strategy of retaining a conservative approach to maintain supportability of, and compatibility between, IT application assets. This has included a focus on consolidating to a core set of applications, removing applications no longer required and considering appropriate support options including the use of cloud services. This strategy is reflected in our IT Asset Management Plan 2019-2023¹, which describes how we manage our IT assets and aligns with the SA Power Networks Asset Management Policy². Following this strategy has enabled us to continue to respond to continual demand for new capabilities within the existing budgets.</p> <p>Finally, during the 2015-20 RCP the current version of our work management and scheduling software, Click, reaches end-of-life and there is no upgrade path for</p>

¹ SA Power Networks: *SA Power Networks IT Asset Management Plan 2019-2023*, V2.0

² SA Power Networks Asset Management Policy, Major Version 4

Topic	Detail
	the existing on-premise solution. We have assessed replacement options, including assessment of alternative vendors, to address this challenge. The option being implemented in the 2015-20 RCP is to retain our current vendor who is moving their software to the cloud.
Drivers	<p>To enable SA Power Networks to meet its regulatory obligations to maintain safe, secure and reliable distribution services to its South Australian customers, the supporting IT Applications portfolio needs to be current, operational and fit for purpose.</p> <p>The key drivers behind this program are the achievement of the following objectives:</p> <ul style="list-style-type: none"> • ensuring the safety of SA Power Networks' workers and the community; • maintaining secure and reliable IT Applications in an increasingly digitised industry as cyber security risks are increasing; • enabling compliance with regulatory obligations and requirements; • maintaining the capability to respond to customer demand for timely and relevant information, particularly during outages; • effectively and strategically managing IT assets; and • ensuring the supportability of, and compatibility between, SA Power Networks' IT Applications. <p>These drivers are explained in more detail in Section 2 of this Business Case.</p>
Options considered	<p>We undertook an options assessment to determine an optimal and cost-effective approach to managing our IT Applications portfolio in the 2020-25 RCP. As part of this process, we performed a business impact assessment of our integrated applications portfolio to better understand the impact on business operations of IT system unavailability. The assessment considered a range of factors including customer impact, business criticality, operational risk and the potential effects of these on our ability to reliably deliver distribution services to our customers.</p> <p>The baseline used during assessment of options for this business case was the total IT Applications recurrent capex actuals/forecast for the 2015-20 RCP of \$80.0 million³ capex. The IT Applications recurrent capex actuals/forecast is less than the 2015-20 RCP allowance of \$81.6 million for the 2015-20 RCP⁴ due to additional consolidation of applications.</p> <p>We explored two options to determine whether they would provide better outcomes than the baseline with respect to a range of factors including cost and operational risk:</p> <ul style="list-style-type: none"> • Option 1 – Patch and upgrade all systems, irrespective of business criticality, to Vendor Release Schedule: doing more across the IT Applications portfolio by adopting the practise of implementing patches and upgrades as they are released by the respective vendors, irrespective of business criticality; and

³ Unless otherwise specified, all costs in this business case are expressed in June 2017 dollars and exclude corporate overheads.

⁴ Our 2015-20 Regulatory Proposal included the total of \$78.4 million capex (June \$2015) for the IT Applications Minor Upgrades and Enhancements, Business System Upgrades and National Market Systems, which equates to the total of \$81.6 million (Dec \$2017). This expenditure was accepted by the AER in its Final Decision and formed part of the total non-network IT capex allowance of \$270.5 million (Dec \$2017) for the 2015-20 RCP.

Topic	Detail
	<ul style="list-style-type: none"> • Option 2 – Risk-based approach to manage IT Applications: use a risk-based approach to manage IT Applications, aligned to the IT Asset Management Plan which incorporates our learnings, and continues to implement the approach taken in the 2015-20 RCP. <p>As noted in the Context / background section, we commenced moving our Click software to cloud in the 2015-20 RCP. Both options include completion of this project and decommissioning of the on-premise version of Click in the 2020-25 RCP. However, no opex for the new cloud-based Click software is required until 2020/21 and therefore no new opex has been included in our proposed reveal year (ie 2018/19). For this reason, we propose to include a \$3.6 million opex step change related to the capex to opex substitution in our opex forecast for the 2020-25 RCP. We have reduced our recurrent capex proposed in this business case to reflect the foregone capex related to what would have otherwise been spent on ongoing upgrades to the on-premise Click software. The details are provided in the Click Capex Opex Substitution Proposal (Appendix B).</p> <p>The costings for these two options over the 2020-25 RCP are:</p> <ul style="list-style-type: none"> • Option 1: <ul style="list-style-type: none"> – \$125.4 million capex and \$3.6 million opex step change from an efficient capex to opex substitution for Click Software-as-a-Service (Saas). • Option 2: <ul style="list-style-type: none"> – \$69.8 million capex and \$3.6 million opex step change from an efficient capex to opex substitution for Click Saas.
Option selected	<p>Option 2 has been selected as the preferred option because it:</p> <ul style="list-style-type: none"> • achieves the expenditure objectives (eg managing the demand for network services, complying with applicable regulatory obligations and requirements, and maintaining the reliability and safety of the distribution system); • balances 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 • enables the key drivers.
Estimated cost	<p>The total forecast expenditure for Option 2 is \$69.8 million capex and \$3.6 million opex step change from an efficient capex to opex substitution⁵ for the 2020-25 RCP⁶.</p> <p>This total forecast expenditure (capex and opex step change from efficient capex to opex substitution) is a reduction compared both with the capex allowance of</p>

⁵ Click capex to opex substitution for Click Software as a Service (refer Appendix B).

⁶ These costs assume the SAP Upgrade, Geographic Information System Consolidation and Protection Settings System Redevelopment projects occur during the 2020-25 RCP.

Large replacements, upgrades, and other significant changes (eg compliance) are the subject of separate business cases and not considered here.

Topic	Detail
	<p>\$81.6 million for the 2015-20 RCP⁷ and with the actual/forecast total capex of \$80.0 million for the same period.</p>
Estimated benefits	<p>The benefits of proceeding with Option 2 are:</p> <ul style="list-style-type: none"> • Lower cost option than both Option 1 and the baseline (ie, IT Applications recurrent capex actuals/forecast for 2015-20 RCP). • Applications are maintained at a level that can properly support⁸ the business to provide safe, secure and reliable distribution services. • Field service staff have access to critical safety and job information when they need it to enable the safe and efficient delivery of distribution services. • Continued compliance with our regulatory obligations and requirements. • Services and information are available for our customers when needed as the applications are patched, upgraded, managed and secured. • Compliant with our IT Asset Management Plan which is to extend the useful life of systems by prudent upgrades and updates. • Ensures the supportability of, and compatibility between, our IT Applications. <p>Refer to Section 4 for further detail on the benefits of the selected option.</p>
Risks of not proceeding	<p>The overall risk of not proceeding has been identified as Extreme.</p> <p>The risks of not proceeding include:</p> <ul style="list-style-type: none"> • Significantly increased risk of repeated and extended interruptions in our distribution services due to an increased likelihood of IT system failures and dependence of emergency response field crews on IT systems. • Our regulatory market obligations potentially compromised by delayed processing of customer transactions and National Electricity Market (NEM) transactions. • SA Power Networks could be exposed to significant work health and safety risks related to reduced reliability of IT systems used to: <ul style="list-style-type: none"> – identify, notify and maintain reliability of supply to critical and life support customers; – proactively manage bushfire vegetation risks and determine when critical assets should be switched off to protect customers or property; and – provide asset location information used to accurately identify impacts of switching activities in the field on field services personnel, other emergency services personnel and the public. • Our ability to generate market Distribution Use of System (DUoS) billing could be impeded which would place the main corporate cashflow at risk. • Our ability to generate accurate regulatory and reliability reporting could be compromised. • We would be unable to efficiently implement regulatory compliance changes to IT systems such as payroll, superannuation, tax changes and ASIC mandated alterations to accounting standards.

⁷The total cost of Option 2 (recurrent capex and opex step change) is \$69.8 million + \$3.6 million = \$73.4 million. The allowance for the 2015-2020 RCP was \$81.6 million (Dec \$2017). The reduction in actual/forecast expenditure of \$80.0 million for the 2015-20 RCP compared to the allowance has been made possible by our focus on consolidating systems onto strategic application platforms.

⁸ As per our IT Asset Management Plan which aligns with the SA Power Networks Asset Management Policy.

Topic	Detail
	<ul style="list-style-type: none"> • The ability to effectively manage network asset data used for identification, planning and scheduling inspections and maintenance work over the long-term could be impacted. This would have an adverse impact on ongoing costs (both opex and network asset replacement expenditure (repex)). • Increased risk of exposure to cyber security intrusions and disruptions to electricity due to applications not being patched properly. • Increased risk of integration failure if components of integrated systems and platforms are not maintained to an appropriate level. • Significantly increased costs if SA Power Networks' is required to revert to manual processes to address any of the above, which would also reduce customer service levels and introduce time delays. <p>For further detail on risk assessment and the benefits associated with reducing the identified risks, refer to Section 2.3, and sections 4.2 and 4.3.</p>
Regulatory framework	<p>This expenditure is required in order to achieve each of the following capex objectives:</p> <ul style="list-style-type: none"> • clause 6.5.7(a)(1) [Meet or manage expected demand for standard control services]; • clause 6.5.7(a)(2) [Comply with all applicable regulatory obligations and requirements]; and • clause 6.5.7(a)(3) [Maintain the quality, reliability and security of supply]; and • clause 6.5.7(a)(4) [Maintain the safety of the distribution system], <p>and the corresponding opex objectives in clause 6.5.6(a) of the NER, as the proposed expenditure is necessary for the effective and efficient operation of SA Power Networks' IT Applications and systems, which, in turn, are critical for the effective and efficient operation of the network.</p> <p>The forecast capex and opex also meet the capex and opex criteria in clauses 6.5.6(c) and 6.5.7(c) of the NER as expenditure associated with the IT Applications portfolio is:</p> <ul style="list-style-type: none"> • efficient because we have been able to reduce the required expenditure without significantly increasing the operational risks; • prudent because it addresses the significant operational risks posed by the failure to maintain the IT Applications portfolio; and • realistic because the figures used to determine the costs have been based on historical costs and approaches. <p>Further detail is provided in Section 4.9.</p>
Supporting evidence	<p>All DNSPs and other utility providers are reliant on fit for purpose IT systems to operate in the NEM. To address this business need, all DNSPs undertake programs of work similar to the IT Applications proposed in this business case.</p> <p>In addition, recent cyber security events around the world and related regulatory obligations and requirements arising under the <i>Security of Critical Infrastructure Act 2018</i> (Cth) have also focused attention on the cyber security risks to our IT systems, and the Notifiable Data Breaches scheme under Part IIIC of the <i>Privacy Act 1988</i> (Cth) has passed through Parliament. Cyber security threats are reduced by implementing vendor supplied patching when available. Almost all recent DNSP</p>

Topic	Detail
	proposals highlight the importance of ensuring IT systems and data similar to our IT Applications are secure from cyber security threats.
Dependencies	<p>The following non-recurrent IT projects included in our 2020-25 IT work program affect the cost estimates in this business case. They are:</p> <p>1) SAP Upgrade If the expenditure associated with our preferred option for the SAP Upgrade Business Case is not accepted by the AER, then additional costs of \$1.214 million will need to be assigned to this IT Applications program for the 2020-25 RCP. This expenditure reflects adjustments to the IT Applications program, for the SAP-related maintenance activities being undertaken as part of the SAP upgrade, which will otherwise need to be performed as part of the IT Applications program. Further to this, if the SAP upgrade does not proceed during the 2020-25 RCP there will be a significant uplift in recurrent IT capex in 2025-30 RCP and beyond. The uplift would be related to the costly workarounds and remediation work following the lapse in SAP support, and the attempted resolutions of issues related to that lapse of support as they are realised, from 2025 onwards.</p> <p>2) GIS Consolidation If the expenditure associated with our preferred option for the Geographic Information System (GIS) Consolidation Business Case is not accepted by the AER, then additional costs of \$0.649 million, for maintenance activities taken on by that project while it is operating, will need to be assigned to this IT Applications program for the 2020-25 RCP.</p> <p>3) PSS Redevelopment If the expenditure associated with our preferred option for the Protection Settings System (PSS) Redevelopment Business Case is not accepted by the AER, then additional costs of \$1.672 million, for the ongoing maintenance activities associated with the existing PSS, will need to be assigned to this IT Applications program for the 2020-25 RCP.</p>
Customer and stakeholder engagement	<p>Our recent customer engagement surveys and workshops have shown that <i>“customers place a very high priority on receiving timely and accurate information about our services but particularly during outages. They consider this as important as reliability or price”</i> (SA Power Networks, Customer Research, 2017).</p> <p>This initiative was presented at the IT Deep Dive workshop with stakeholders and the Consumer Challenge Panel on 26 June 2018. We received feedback that customers wish to be recognised as key users of our IT Systems⁹. We understand from this that factors influencing our customers’ ability to reliably and easily access the information they want, such as changing mobile device types, are factors which should influence the prioritisation of applications maintenance activities¹⁰ (refer Section 2.2).</p>

⁹ Think Human, *IT Deep Dive Workshop Report: SA Power Networks*, 28 June 2018, V1, page 13.

¹⁰ Maintenance activities include periodic application version upgrades, defect and/or compliance remediation, security patching and minor enhancements.

Topic	Detail
	<p>We also received feedback that customers and stakeholders are keen to better understand how our IT Applications support the services they receive¹¹. This has been addressed in Section 3.1 of this business case where we describe the customer value provided by each group of applications in our portfolio.</p>

¹¹ Think Human, *IT Deep Dive Workshop Report: SA Power Networks*, 28 June 2018, V1, pages 12-13.

2. Drivers

2.1 Introduction

SA Power Networks operates a distribution network that stretches across South Australia, comprising thousands of kilometres of powerline and hundreds of substations. Our integrated IT application portfolio enables the delivery of distribution services to customers and enterprise business services, that are critical to the efficient and prudent operation and maintenance of our network, managing safety and risks to both staff and customers, and the supply of timely and accurate information to customers during outages.

Our IT Applications are an integrated portfolio of technology software packages that provide capability for:

- asset management;
- safety and risk management;
- asset planning and design;
- asset location information;
- works management and scheduling;
- workforce mobility;
- customer facing websites and customer mobile applications;
- customer network billing;
- national electricity market operations;
- network operations;
- analytics and reporting;
- corporate business (eg finance, payroll, HR, procurement);
- office and collaboration tools; and
- IT management.

We keep the IT 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.

As identified from our business impact analysis modelling, 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 which protect people, assets and property;
- customer messaging alerts and restoration information;
- security of customer information and the network;
- network asset management; and
- SA Power Network's ability to interact with NEM systems.

Figure 1 demonstrates a scenario in which our IT Applications portfolio is used to enable us to deliver services and information to its customers. As shown, a number of applications are required to enable us to provide distribution services to customers. If there is a failure with any of these applications, our ability to deliver these services will be compromised.

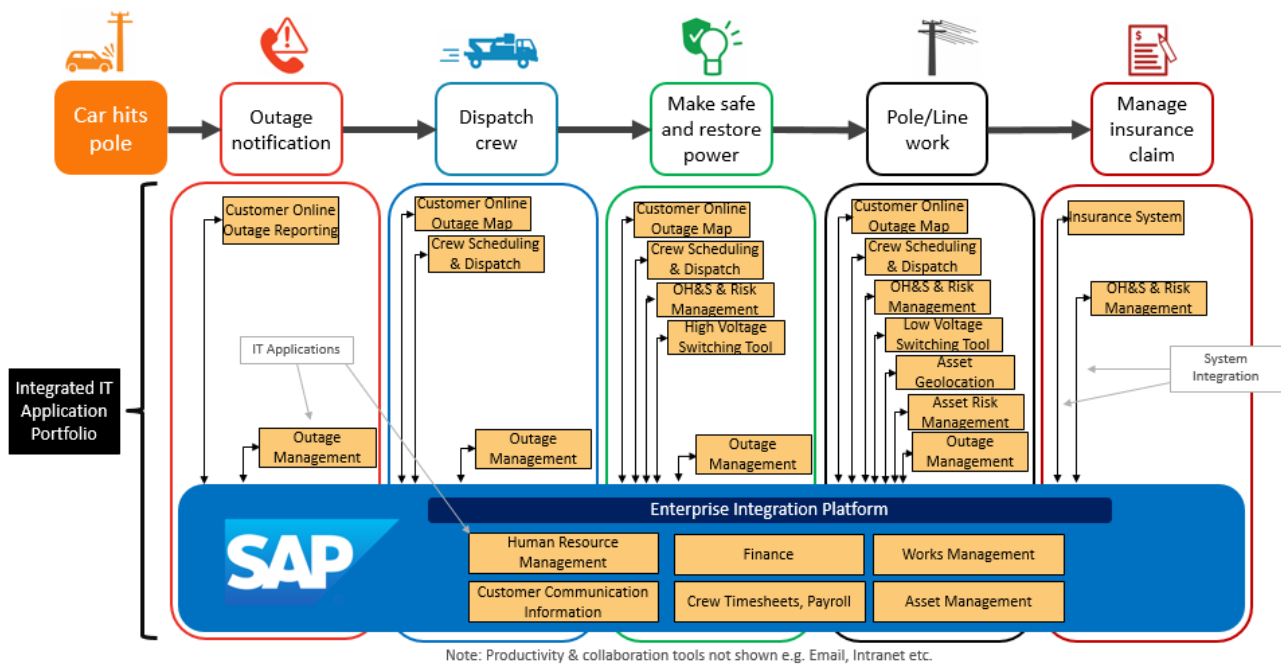


Figure 1: Business Scenario – Car hits pole causing outage

Keeping our IT Applications relevant

During the 2015-20 RCP demand for IT capabilities increased significantly, and this was reflected in the growing enablement of business capability by IT Applications. Key new capabilities implemented include:

- **Mobility Management:** With the growing use of mobile technologies, managing information securely is a significant requirement and requires the use of specialised technologies.
- **Centralised Design Management:** In a dynamic network environment ensuring assets standards and designs are consistent and well maintained is essential to providing reliable network services.
- **Integration Management:** SA Power Networks' customers and business are seeking more timely and integrated information on which to make decisions. The advent of Cloud technologies has meant there is a greater focus on providing reliable and secure integration of data across systems.
- **Job Estimating:** As the amount of activity on the network has increased SA Power Networks has implemented systems to support quoting on customer jobs to provide a more consistent service.
- **Customer Management:** We have updated a number of systems which directly support the delivery of distribution services to customers to improve our customer information and processes as a direct consequence of the customer demand for more accurate and timely data during outages¹². For example, our Outage Management System (OMS) has proven to be too slow and unable to provide accurate enough information to locate customers effectively during outages, so was updated.
- **Field Data Collection:** Customer demand for more timely and accurate information necessitated significant improvements in our field technologies to support the collection of that field data.
- **Asset Management:** Regulatory obligations and requirements for improved RIN reporting has driven a replacement of the general ledger, and significant improvements in data collection, analytics and financial reporting.

¹² The numerous and widespread electricity outages in 2016 disrupted South Australia and we identified our IT integrated systems could not support timely data and information on outages. <https://www.aemo.com.au/Media-Centre/Review-of-the-Black-System-South-Australia-Report-System-event-of-28-September-2016> and 'Distribution Licence Compliance Review – SA Power Networks, 27-28 December 2016 severe weather event, June 2017, Essential Services Commission of South Australia, p26'.

- **Work Scheduling and Field Management:** To ensure work is performed cost effectively by optimising field crew work schedules and enabling field crews to manage their tasks via mobile devices.

SA Power Networks' Approach to Managing the Applications Portfolio

We have designed an efficient and practical maintenance regime which is geared towards ensuring business continuity and managing system outage risks. Upgrades, updates and continuous improvement initiatives are applied based on the business role, criticality and the general support obligations for the application.

Our approach to maintaining our IT Application portfolio is governed by our IT Asset Management Plan. The IT Asset Management Plan outlines an asset management framework to ensure IT investment is prudent and targeted at managing risk and business value. The approach requires us to:

- prioritise investment towards ensuring business critical IT Applications remain online, available to customers and staff, and secure;
- retain a conservative but prudent approach to maintain the supportability of, and compatibility between, SA Power Networks' IT Application and IT infrastructure assets;
- adopt a 'standardise, leverage and consolidate' approach which is as follows:
 - **standardise** on a core modern set of large application suites or platforms that are more 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.
- commence the necessary journey to Cloud technologies where it is prudent and secure to do so; and
- continuously review our IT operating model and focus on the efficient and cost-effective delivery of IT services.

This approach has allowed us to:

- continue to manage the growing portfolio of capability within the existing budgets; and
- reduce our IT Applications recurrent costs below allowances for the 2015-20 regulatory control period (RCP).

2.2 Factors that influence IT Applications maintenance

There are a number of factors that influence the level of maintenance activity required to ensure the IT Application portfolio maintains the capability to deliver the required business outcomes. These are listed in the Table 1 below:

Table 1: Factors that influence the IT Applications maintenance

Factors that influence applications maintenance	Description
Customer Facing Applications must be kept available, secure and functional on customer mobile devices.	Continually changing mobile device types require ongoing modifications to the website and portal applications to ensure the applications continue to work as required.
Security vulnerability levels	As owners and operators of critical infrastructure, SA Power Networks is required to appropriately manage the vulnerability of our IT systems to cyber security threats. If this is not done then we risk the leak of confidential customer information, loss of trust in our IT systems or even loss of network control.
End of life	As applications age there is an increased risk of failure of 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.
Vendor roadmaps and impact of their cloud-based strategies	Increasingly vendors are indicating on their product roadmaps that they are transitioning their products to the cloud. Cloud based services are becoming the standard architectural approach for consumption of IT services. Cloud services generally enable greater scalability and flexibility and increases agility of IT service delivery ¹³ . An effect of this will be a shift of IT support costs from capex to opex over time (refer Appendix B).
Hosting arrangements	SaaS or Cloud Hosted platforms bring with them a change frequency driven by the vendor which requires more frequent testing and updates of integration services.
Software vendor-imposed upgrade or release Cycles	Vendors of some software systems are now imposing a minimum level of upgrades that must be implemented during a given release cycle.
Resolution time for software issues	Deferral of patches can add to the time required to restore service (ie to perform break-fix activities) after an application outage. Vendors require up to date systems before they provide support.
Early adoption of software updates is not always prudent	Early adoption of new technology, such as software updates, can introduce risks because fixes to defects may not have been released by the vendor (ie early adopters often discover these issues as they implement these early releases).

¹³ SA Power Networks Digital Strategy, V6.4, p12

Factors that influence applications maintenance	Description
Seasonal business cycle	Some areas of the business are subject to seasonal workloads which increase their reliance on IT systems or reduce their capacity to assist with the testing of software updates. In these situations, the implications of applying software updates, for the affected area of the business, need to be considered. (ie in bushfire season, storms)
Maintain linkages between systems	There is an increased risk of integration failure if components of integrated systems and platforms are not maintained to an appropriate level.
Maintain compatibility with external entities	The change frequency on a number of SA Power Networks' applications are now determined by parties external to SA Power Networks. To be part of that service (eg Dial Before You Dig), or to remain compatible with that external feed (ie weather data from the Bureau of Meteorology) SA Power Networks must upgrade when requested to do so.
Ongoing regulatory changes	SA Power Networks is obligated to keep its systems in compliance with changing regulatory obligations and requirements. For example, tax changes are required to be updated annually.
Frequency of changes in a given functional area of the business	Areas of the business that are undergoing rapid change require regular small changes for their systems to stay "current" and remain fit for purpose. These small ongoing changes help to extend the operational life of those systems and applications without fundamentally altering their overall functionality.

2.3 Issues and risks associated with not proceeding

There are both operational and delivery risks associated with failing to perform regular maintenance activities on the IT Applications portfolio.

Operational Risks

Given the criticality of the IT Applications portfolio at SA Power Networks, if we did not apply software patches and updates to IT Applications, we would not be able to meet our regulatory obligations to deliver safe and reliable distribution services to our customers.

The following operational risk assessment has been conducted in accordance with SA Power Networks' Corporate Risk Framework (refer Appendix A). This includes the application of the appropriate qualitative measures of likelihood and consequence, and the resulting overall risk rating. The risks are assessed against 'Not Proceeding' with any planned activity in respect of the IT Applications portfolio.

Table 2: Not Proceeding - Operational Risk Assessment

Risk ID	Risk Description	Consequence Description	Likelihood	Consequences	Risk Rating
1	Network Reliability	<p>The operation and reliability of the distribution network is heavily dependent on the IT Applications portfolio and any network reliability issue can, in turn, result in liability. The management of emergency response field crews is also heavily dependent on IT Systems.</p> <ul style="list-style-type: none"> Reliability (> 40,000 customers affected for an extended period of time) Financial (\$10m > Service Level Agreements (SLAs) < \$100m) Reputation / Customer Service (Repeated interventions by ombudsman or regulators) 	Possible	Major	High
2	Market Obligations	<p>If NEM obligations are compromised by delayed processing of customer transactions, then SA Power Networks would be liable for significant non-compliance penalties.</p> <ul style="list-style-type: none"> Financial (\$1m < Penalties < \$10m) 	Likely	Moderate	High

Risk ID	Risk Description	Consequence Description	Likelihood	Consequences	Risk Rating
3	<p>Health and Safety</p> <ul style="list-style-type: none"> Critical and Life Support Customers Bushfire Risk Management Switching Activities 	<p><u>Critical and Life Support Customers:</u> Network outage management teams unable to identify, notify and maintain reliability of supply to critical and life support customers. There are potentially catastrophic consequences associated with not being able to identify critical and life support customers. SA Power Networks has more than 9,500 National Metering Identifiers (NMIs)¹⁴ recorded for life support customers.</p> <ul style="list-style-type: none"> WH&S (Multiple Fatalities) Financial/Regulatory (> \$100m penalties for notification failures) Reputation (adverse media coverage/repeated intervention by Regulator) <p><u>Bushfire Risk Management:</u> SA Power Networks unable to manage bushfire risks as several systems are integrated together to enable SA Power Networks to determine 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 regulators and aggrieved party legal actions.</p> <ul style="list-style-type: none"> WH&S (Multiple Fatalities) Financial / Regulatory (Fines, Court Action, Compensation Costs for loss of life and property) Reputational (Adverse media campaigns, Intervention by Regulator) <p><u>Switching Activities:</u> GIS information integrated with other key IT systems is used to accurately identify impacts of switching activities in the field. This can have WH&S consequences for field services personnel, other emergency services personnel, and the general public, particularly during severe weather events.</p> <ul style="list-style-type: none"> WH&S (Death or Permanent Disability) Financial / Regulatory (Related Fines, Workcover, Court Action, Compensation Costs) Reputation (Adverse media coverage) Organisational (Industrial action in the event workers are injured or killed) 	Possible	Catastrophic	High

¹⁴ Per SAPN SAP report run 9 September 2018.

Risk ID	Risk Description	Consequence Description	Likelihood	Consequences	Risk Rating
4	Market Billing	Ability to generate DUoS billing to Retailers impeded, placing the main corporate cash flow at risk and potentially restricting business operations. <ul style="list-style-type: none"> Financial (\$10m > Cash Flow < \$100m) 	Unlikely	Major	Medium
5	Legal Compliance	Unable to efficiently implement regulatory compliance changes to IT systems such as payroll, superannuation, tax changes and ASIC mandated alterations to accounting standards exposing SA Power Networks and its 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. <ul style="list-style-type: none"> Financial/Regulatory (\$1m < Penalties < \$10m) Organisational (Significant impact due to HR issues, industrial action and related reputational damage) 	Almost Certain	Minor	High
6	Regulatory and Reliability Reporting	Ability to generate accurate regulatory and reliability reporting, which is heavily dependent on IT systems, could be compromised. <ul style="list-style-type: none"> Reputation (Intervention by regulators) Regulatory / Financial (\$1m < Penalties >\$10m) 	Likely	Moderate	High
7	Planned Asset Maintenance	Ability to effectively manage network assets, the data for which is maintained within IT systems and used as inputs for identifying, planning and scheduling inspections and maintenance work over the long-term, could be impacted. The inability to prioritise, plan and schedule planned work correctly would have an adverse impact on ongoing costs (both opex and repex). <ul style="list-style-type: none"> Financial (Cost impact > \$10m) 	Possible	Major	High
8	Security	The vulnerability of an IT system to security breaches is related to its security configuration, 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. SA Power Networks could also expect significant penalties from regulators and aggrieved party legal actions. <ul style="list-style-type: none"> Reliability (> 40,000 customers without supply for extended period) Regulatory / Financial (>\$100m due to fines, legal action, damaged equipment) WH&S (Death or permanent disability) Reputation (Adverse media, intervention by regulators) 	Likely	Catastrophic	Extreme

Risk Summary	
The overall risk rating for not proceeding with this program has been determined to be:	Extreme

The following scenario is used to illustrate how a lack of maintenance activity on the IT Applications portfolio could impact the ability of SA Power Networks to respond to restore energy supply when outages occur.

Scenario: Responding to outages and restoration of supply

A well maintained and integrated IT Applications portfolio is integral to SA Power Networks' ability to respond rapidly and effectively to outages in the network as illustrated by Figure 1 (refer section 2.1) for the business scenario where a car has hit a pole causing an outage.

In the above scenario, if our integrated IT Applications have not been well maintained, they may not be reliably working together. This would introduce delays into the process of restoring supply because accurate information is not available, in the right place at the right time or where the integrity of information is compromised. This would affect our ability to efficiently and appropriately:

- prioritise and locate the outage;
- dispatch field crews to investigate, make the area safe for the community, and resolve the problem; and
- provide accurate and timely communications to affected customers.

Now consider extrapolating the effects of this from a single car and pole to a much larger outage situation in which our integrated IT Applications portfolio has become less reliable due to lack of maintenance or events beyond our control. During the numerous and widespread electricity storm related outages in 2016, we learnt that issues in one application can have an impact on SA Power Networks' overall service.

It is not unusual for a storm event to affect 10,000 to 20,000 customers. Previous Major Event Days (**MEDs**) have affected around 150,000 customers. If such a storm were to occur while we were attempting to resolve issues within or between one or more of our key IT Applications, potentially without vendor assistance due to the lapse of support arrangements, the scale of liability that we could incur would be large. If unable to restore power to those customers within 48 hours in such circumstances, we could be liable for between \$2 million and \$3.5 million in Guaranteed Service Level (**GSL**) payments¹⁵, from just that single event which would be passed through to customers. In the event of a severe storm the impact would be much worse. Further, depending on the systems involved, there could be significant and potentially life-threatening risks to the health and safety of life support customers as we would struggle to identify which faults were affecting them as well as to other critical customers such as those located at hospitals who provide many essential services on which the South Australian public rely.

There could also be significant economic impacts to the broader South Australian community if restoration of power to South Australian businesses is delayed. The 2016 state-wide blackout was estimated to have cost South Australian businesses \$367m¹⁶, a figure which was based on 70% of the affected businesses having power restored within 24 hours and, given the blackout occurred late in the trading day, effectively losing only one trading day of business.

Delivery Risks

The IT-related delivery risks associated with failing to perform regular maintenance activities on the IT Applications portfolio are as follows:

¹⁵ Based on revised GSL payments from July 2020 and the number of historical Major Event Days (refer Electricity Fact Sheet – Changes to SA Power Networks GSL scheme – January 2019 – Public – I2 – A2)

¹⁶ [https://business-sa.com/Commercial-Content/Media-Centre/Latest-Media-Releases/September-Blackout-Cost-State-\\$367-Million](https://business-sa.com/Commercial-Content/Media-Centre/Latest-Media-Releases/September-Blackout-Cost-State-$367-Million).

- **Impact on other planned capital IT programs:** If no upgrades are performed on IT Applications within the portfolio this will have two impacts on the other IT capital projects planned for the 2020-25 RCP because:
 - an upgrade provides technology and functional features required for these projects, which would not otherwise be available; and
 - introduction of significant functionality through planned IT capital work on an unpatched application environment will introduce delivery risk for those programs due to unexpected impacts from the unpatched systems being worked on.
- **Impact on future operational cost of managing the IT Applications portfolio:**
 - With no patches or upgrades, the operational cost of managing the IT Application portfolio would exceed planned spend for the 2020-25 RCP and beyond.

2.4 Detailed description of drivers

The key drivers for this business case are the following:

1. *Ensuring the safety of SA Power Networks' workers and the community*

SA Power Networks uses the IT Applications portfolio to ensure the safety of both its workers and the community. Some examples include:

- identification, notification and maintenance of reliability of supply to critical and life support customers;
- management of manage bushfire risks to enable us to determine when critical assets should be switched off to protect customers and their property;
- reporting on and related management of vegetation related risks; and
- using GIS information integrated with other key IT systems to accurately identify impacts of switching activities in the field to protect field services personnel, other emergency services personnel, and the general public during severe weather events.

2. *Maintaining secure and reliable IT Applications in an increasingly digitised industry as cyber security risks are increasing*

Securing critical infrastructure is recognised as a key challenge. As stated recently by the Hon Peter Dutton MP "Owners, operators and regulators of critical infrastructure are the first line of defence."¹⁷ One of the recognised defence mechanisms is regular updates and patching of application software to reduce vulnerabilities. As applications increasingly move to Cloud environments and/or to sharing more with external parties, regularly securing applications has become a core part of securing our network infrastructure.

3. *Enabling compliance with regulatory obligations and requirements*

Maintaining compliance with our statutory, legislative and regulatory obligations and requirements, including our reporting requirements, drives change in our IT systems. The change frequency for these types of activities for applications is determined by external stakeholders, for example, government departments and regulators.

4. *Maintaining the capability to respond to customer demand for timely and relevant information, particularly during outages*

Customers are key users of our IT systems which means factors influencing their ability to reliably and easily access the information they want, such as changing mobile device types, are key factors influencing the prioritisation of applications maintenance activities.

¹⁷ The Hon Peter Dutton MP, Opening address to the Australian Cyber Security Centre Conference, Canberra, 11 April 2018, <http://minister.homeaffairs.gov.au/peterdutton/Pages/australian-cyber-security-conference.aspx>.

During the numerous and widespread electricity outages of 2016, we learnt that customers have no tolerance for a lack of outage information, and that issues in one application can have an impact on our overall capability to deliver this information in a timely manner.

Our recent customer engagement surveys and workshops have demonstrated that *“customers place a very high priority on receiving timely and accurate information about our services but particularly during outages. They consider this as important as reliability or price”*¹⁸ and want timely and relevant information which will enable them to make proactive decisions.

We therefore need to maintain an up-to-date, robust, secure and integrated portfolio of applications to maintain services to customers. These require regular activities to cost effectively maintain them. Up-to-date and maintained applications also provide the basis for keeping pace with changes in the evolving energy markets and customer preferences. Looking forward to the 2020-25 RCP, customer and business dependency on technology is expected to continue to increase especially with customers moving from consumers of electricity to suppliers of electricity.

The Future Network Strategy details the organisational strategic response to the emergence of the two-way flow electricity network. IT technologies will play a larger role in the ongoing management of SA Power Networks’ network and in making data visible to help customers to make timely and informed decisions about their network usage. Increasingly these decisions will be ‘real time’ and rely on machine learning as capabilities like energy trading start to gain traction. Our IT Applications will need to be robust and secure to support those capabilities.

5. Effectively and strategically managing IT assets

We are conscious that our operational costs form part of the costs of electricity borne by our customers. As general principle, we retain applications as long as possible to maximise the return on investment in, and efficient operation and use of, the distribution services provided by those applications.

We are working to contain costs by carrying out a rigorous strategy of implementing new capability on our existing key technology platforms rather than implementing additional new systems that would increase maintenance complexity and cost. Our approach is outlined in further detail in our IT Asset Management Plan.

6. Ensuring the supportability of, and compatibility between, SA Power Networks’ IT Applications

We will continue to leverage and explore technologies to ensure our distribution services are delivered as cost effectively as possible. As a result, dependence on the IT Application portfolio will continue to grow. We need to continue to balance an increased need to respond with agility, with the need to maintain the integrity and reliability of our core systems.

Maintaining compatibility between our IT Applications and those of external entities, including as required by ongoing regulatory and market changes, drives change in our IT systems. The change frequency for these types of activities for applications is determined by others. To enable us to continue to provide our services our IT platforms need to be vendor-supported and, when prompted by those services, upgraded, in order to maintain compatibility between the services and our IT systems. An example is the need to ensure that our national market systems and billing systems integrate and operate with the Australian Energy Market Operator (AEMO).

¹⁸ SA Power Networks, Customer Research, 2017.

3. Scope

3.1 In Scope

Our IT Applications portfolio is grouped into software platform groupings. The following sections summarise the function of each Application Platform Group which has been included in the scope of this business case and the associated reasons for the IT Application investment activity within that group.

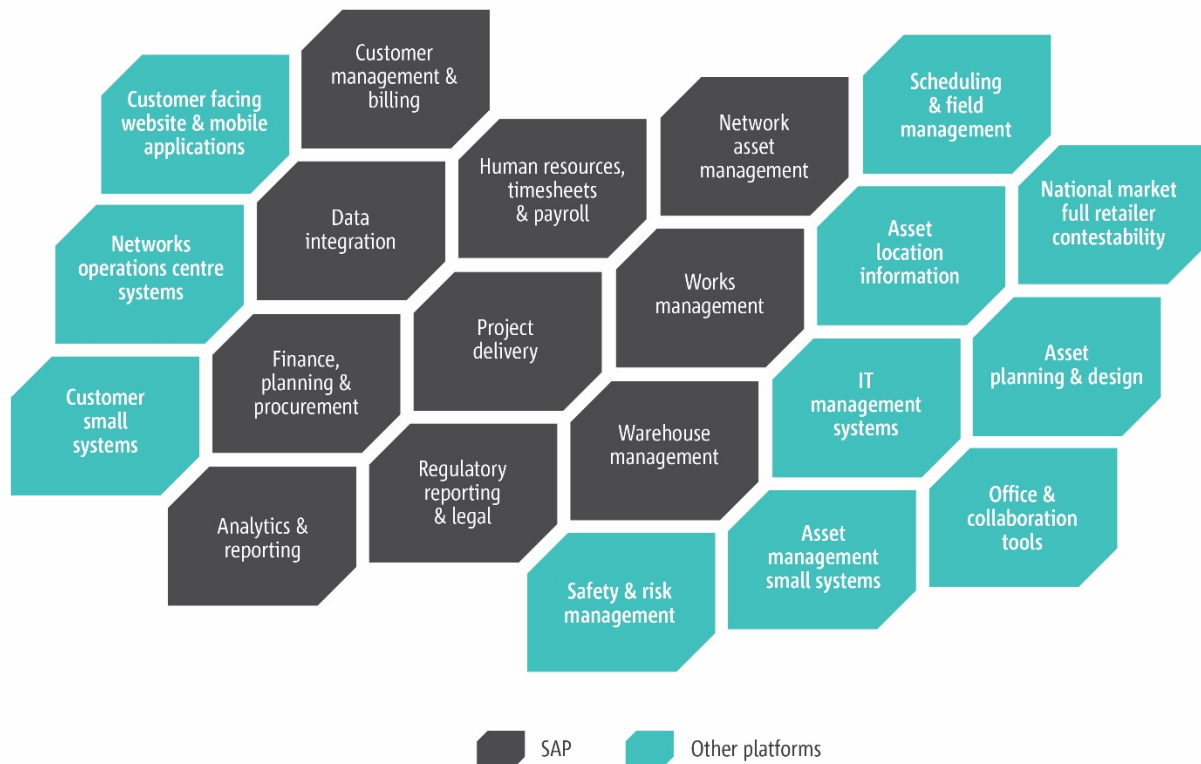


Figure 3: SA Power Networks integrated IT application portfolio

3.1.1 Asset Location Information

Asset Location Information	
Customer Value	Enables problem resolution and asset management. Records and manages electricity network asset geolocation information and feeds it to both field crews, and to systems, for visual problem resolution and route planning. That is, having specific asset location information recorded enables assets, including customer NMIs, to be located more quickly so that when customers report problems they can be more quickly identified. Asset location data also supports our customer facing mobile applications such as Street Lights Out and Outage Map.
Enterprise Critical Functions of Applications in this Group	<ul style="list-style-type: none"> • Master model of SA Power Networks' electrical network. • System of record for Life Support and other critical customer data, depot zones, bushfire zones and corrosions zones. • Provides geolocation data for asset data. • Geolocation data provision for SA Power Networks underground assets to 'Dial Before You Dig' service.

Asset Location Information	
	<ul style="list-style-type: none"> Customer Relations department uses data from these systems to accurately record new customer connection information.
2015-20 Achievements	<ul style="list-style-type: none"> Commenced consolidation of multiple systems on to ESRI GIS as a core platform.
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> ESRI GIS platform consists of multiple applications and the vendor mandates the lifecycle of its applications which determines the upgrade frequency. In the past, an upgrade for each of the applications has been required every 3 years. Hexagon G/Technology, which has the master model of the SA Power Networks' electrical network, also mandates the lifecycle of its applications which determines the upgrade frequency. In the past, an upgrade has been required every 4 years. 'Dial Before You Dig' is a critical safety platform which helps ensure safety of customer, helps prevent accidental damage to network infrastructure and related electrical outages. To continue to obtain this service, SA Power Networks must keep up to date with the requirements of the service.

3.1.2 Asset Management Small Systems and Safety & Risk Management

Asset Management Small Systems and Safety & Risk Management	
Customer Value	Enable the ongoing optimisation of the expenditure for network asset management, replacement, service delivery and safety.
Enterprise Critical Functions of Applications in this Group	<p>Asset management functions including:</p> <ul style="list-style-type: none"> work value identification and prioritisation; asset condition risk modelling; asset sensor data management; network Infrastructure work scheduling; identification of feeders at risk of damage from forecast weather conditions; identification of potential network-related fire risks from forecast weather conditions (ie catastrophic fire danger); and safety and risk management (ie risk management, environment health and safety, and sustainability tool).
2015-20 Achievements	<ul style="list-style-type: none"> The applications that provide this functionality were added during the 2015-20 RCP to enable optimised asset management and work delivery.
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> Consolidation of key capabilities as our experience matures in this space. Ongoing application patching and security updates.

3.1.3 Asset Planning and Design

Asset Planning and Design	
Customer Value	Provides the technology to allow engineering designs for customer connections, customer developments and distribution network developments and changes. Designs are also used to maintain the model of the electrical network to support switching of the network to ensure our field staff can safely work on the network and do not compromise community safety.
Enterprise Critical Functions of	<ul style="list-style-type: none"> Electrical and civil engineering asset drawing creation, information management and storage.

Asset Planning and Design	
Applications in this Group	<ul style="list-style-type: none"> Tools for producing shareable e-drawings for publication on the intranet to field crews and for sharing with suppliers, contractors and customers. Maintenance of the network model which is used to support operational switching decisions in the Network Operations Centre. Design of power lines including related engineering calculations for sag and tension. Design of network infrastructure.
2015-20 Achievements	<ul style="list-style-type: none"> Commenced consolidation of multiple systems on to Autodesk as a core platform.
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> The increasing variety of electricity services that customers want to connect to the network has increased the pace of change in the design applications. Interoperability with underlying application environment as they are upgraded by respective vendors (eg Operating Systems upgrades, Data base upgrades). Very high need to maintain compatibility across the applications platform. The vendor release management policy only allows 2 yearly version gaps for interoperability.

3.1.4 Customer Facing Website and Customer Mobile Applications

Customer Facing Website and Customer Mobile Applications	
Customer Value	Enabling the primary means for customers to report outages, customer communication during outages, access for electricians to log jobs, customer enquiries and general corporate and regulatory information.
Enterprise Critical Functions of Applications in this Group	<ul style="list-style-type: none"> SA Power Networks' website. Customer online outage reporting. Online fault reporting for street lights. Customer outage notification and messaging services. Customer portal. Registered electrician's portal. Other online channels.
2015-20 Achievements	<ul style="list-style-type: none"> Significantly increased the functionality in response to customer demand and improved both the usability and reliability of the website and related mobile applications.
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> Ongoing application and security patching to manage exposure for customer information. Continually changing mobile device types require ongoing modifications to the website and applications to ensure the applications continue to work as required.

3.1.5 Customer Small Systems

Customer Network Billing	
Customer Value	Systems that perform specific functions for managing customer data.
Enterprise Critical Functions of Applications in this Group	<ul style="list-style-type: none"> Customer network billing functions (self-service portal enabling Customers to access their meter data and related analysis). Meter reading scheduling and reporting. Meter data management and analytics.

Customer Network Billing	
2015-20 Achievements	<ul style="list-style-type: none"> Implemented core customer functionality in the new customer relationship management and billing system. Consolidated multiple legacy small customer systems into SAP.
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> Application and security related patching. Ongoing changes in the regulatory and market environments to metering Replacement of remaining legacy customer small systems as end of life is reached.

3.1.6 IT Management Systems

IT Management Systems	
Customer Value	Enables more effective management of IT systems, including facilitating faster restoration from IT outages, which in turn reduce the impact on customer IT and distribution network outages.
Enterprise Critical Functions of Applications in this Group	<ul style="list-style-type: none"> IT issue reporting and management tools. IT diagnostic tools. IT software testing tools. IT architecture design and planning tools. IT project management tools.
2015-20 Achievements	<ul style="list-style-type: none"> Implemented automated testing functions to improve the efficiency of SA Power Network's software regression testing processes. Implemented new IT services management tools which enable more efficient responses to business as usual IT services.
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> Increased criticality of IT capabilities to the business. Application and security related patching and upgrades.

3.1.7 National Electricity Market Systems

National Electricity Market Systems	
Customer Value	Managing customer interval meter data and connectivity and the ability to respond to the NEM.
Enterprise Critical Functions of Applications in this Group	<ul style="list-style-type: none"> Customer interval meter data management. Market transaction system for participation in the NEM.
2015-20 Achievements	<ul style="list-style-type: none"> Maintained as required
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> Yearly batches of NEM driven market and meter data changes (similar expenditure for the last 15 years.)

3.1.8 Network Operations Centre Systems

Network Operations Centre Systems	
Customer Value	Supporting the real-time delivery of electricity network services including safety management through the network operations control systems.
Enterprise Critical Functions of Applications in this Group	<ul style="list-style-type: none"> 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.

Network Operations Centre Systems	
	<ul style="list-style-type: none"> Provision of network configuration load information based on user demand enabling network management. Electrical network protection device settings configuration and management information systems which are used to isolate the wider network from electrical faults.
2015-20 Achievements -	<ul style="list-style-type: none"> Created and improved published real-time customer outage information and notification systems.
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> Continuing to maintain supportability of systems and safety responsiveness in a dynamic network environment.

3.1.9 Office and Collaboration Tools

Office and Collaboration Tools	
Customer Value	Provide core customer, stakeholder, industry and internal communication mechanisms (email), desktop work productivity, document management and collaboration capabilities.
Enterprise Critical Functions of Applications in this Group	<ul style="list-style-type: none"> Email services. Word Processing, Spreadsheets and related desktop productivity tools. Online collaboration and communication tools (eg SharePoint, Skype).
2015-20 Achievements	<ul style="list-style-type: none"> Progressively implemented the cloud technology versions to reduce the need (and hence cost) for installation of server hardware.
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> Microsoft Office 365 updates happen monthly and require testing. Priority updates need to be installed within 3 months and lower priority updates within 18 months. Software ceases to work if these conditions are violated.

3.1.10 SAP Suite (including Analytics and Reporting and Corporate Systems)

SAP Suite (includes Analytics, Reporting and Corporate Systems)	
Customer Value	<p>SAP is the core asset management, customer management, work management and enterprise software application for SA Power Networks. The SAP application suite is critical to the efficient and effective operation and maintenance of the electrical network.</p> <p>SAP is an integrated suite of capabilities that enable:</p> <ul style="list-style-type: none"> management of all network assets; work management including prioritising and executing both planned and supply restoration work for field crews; delivery of customer services including managing the connection, disconnection of customers and customer billing; management of safety of field staff and customers, including life support and critical customers; critical bushfire risk management processes; customer messaging alerts and restoration information; enterprise services including finance, planning, procurement, human resources, payroll, warehouse management and project delivery; and enabling technology services including security, mobility, integration, information management, reporting and analytics.

SAP Suite (includes Analytics, Reporting and Corporate Systems)	
Enterprise Critical Functions of Applications in this Group	<p>SAP supports:</p> <ul style="list-style-type: none"> • Management of the network asset lifecycle; • Delivery of customer services; • Enterprise services including finance, planning and procurement, time recording, human resources and payroll, warehouse management, project delivery, regulatory reporting and legal; and • Enabling technology services including security, mobility, system and data integration, information management and analytics and reporting.
2015-20 Achievements	<ul style="list-style-type: none"> • We have rationalised a number of our applications and implemented new business capability into SAP where it is cost effective to do so.
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> • Regular security patches. • SAP patch updates applied annually for statutory and compliance reasons (eg changes introduced by legislation related to taxes and superannuation). • SAP Application and database upgrades and patching to remediate known issues and maintain interoperability between systems.

3.1.11 Works Management and Scheduling

Works Management and Scheduling	
Customer Value	Ensure work is performed cost effectively, and in a timely manner, by optimising field crew work schedules and enabling field crews to manage their tasks via mobile devices.
Enterprise Critical Functions of Applications in this Group	<ul style="list-style-type: none"> • Scheduling of work and management of resources including field crews and equipment.
2015-20 Achievements	<ul style="list-style-type: none"> • Consolidated on to Click Field Service Edge (Click) as the core scheduling tool.
Factors Driving Activity Frequency in this Group	<ul style="list-style-type: none"> • Click is now only available in a cloud SaaS. • Monthly mandated updates for security, bug fixes and other service improvements. The vendor also releases 3 major updates every year which include new features and upgrades.
Other Comments	During the 2015-20 RCP the current version of our work management and scheduling software, Click, will reach end-of-life and there is no upgrade path for the existing on-premise solution. We have assessed replacement options, including assessment of alternative vendors, to address this challenge. The option being implemented in the 2015-20 RCP is to retain our current vendor who is moving their software to the cloud.

3.2 Out of Scope

This business case excludes maintenance activities for Operational Technology (**OT**) applications including the Advanced Distribution Management System (**ADMS**).

4. Options Assessment

4.1 Options considered

The following options were assessed and considered:

- **Option 1: Patch and upgrade all systems, irrespective of business criticality, to Vendor Release Schedule.** Doing more across the IT Applications portfolio by adopting the practise of implementing patches and upgrades as they are released by the respective vendors, irrespective of business criticality.
- **Option 2: Risk-based approach to manage IT Applications.** Use a risk-based approach to manage IT Applications, aligned to the IT Asset Management Plan which incorporates our learnings, and continues to implement the approach taken in the 2015-20 RCP

4.2 Options assessment

We applied the following options assessment method for recurrent IT capex associated with the IT Applications program:

1. Assessment criteria

Applied the NER expenditure objectives and the processes and methods set out in the AER's Expenditure Forecast Assessment Guidelines as detailed below. In addition, consideration was given to the following additional criteria including:

1. customer impact;
2. the risk to ongoing operations;
3. balance between cost and risk;
4. fit with SA Power Networks' IT Asset Management Plan; and
5. capability to support planned projects.

2. Approach to options assessment

To identify the options for the 2020-25 RCP and to ensure the IT Application portfolio remains fit for purpose we first:

- considered the regulatory proposal submitted to the AER for the 2015-20 RCP, the evolution of the IT Applications portfolio since that document was submitted to the AER and the execution of the works contained in that portfolio in the 2015-20 RCP;
- reviewed the IT recurrent actual/estimated capex for the 2015-20 RCP;
- performed an initial bottom up assessment of the integrated IT Applications portfolio;
- reviewed the related vendor roadmaps and recommended/required update schedules;
- performed a business impact analysis to understand which of our IT Applications were most critical to customers and the business and for those applications:
 - what length of outage could be tolerated by the business;
 - what the impacts of an outage beyond that length would be; and
- considered this in light of the revised IT Asset Management plan¹⁹ to reflect how our IT capability has matured during the 2015-20 RCP;
- rolled the IT Applications up into platform-based groupings to ensure the consideration of synergies between simultaneous system maintenance activities;
- performed a top down review of dependencies and opportunities to reduce overall costs through bundling work across related upgrades; and
- reviewed and reduced costs to take into account expected benefits flowing from other projects acting on the applications environment (eg GIS Consolidation).

¹⁹ A key objective of the IT Asset Management Plan is to extend the useful life of IT assets within an acceptable level of risk.

We then determined a baseline expenditure for the IT Applications portfolio:

- Our regulatory proposal for the 2015-20 RCP recognised that we were at the start of “...*the most significant and transformative change in the distribution sector since the establishment of the [NEM]*”. We expected a large increase in demand for IT services but recognised that our IT systems were legacy, fragmented and unable to meet future demands. To address this we developed a large scale, integrated, IT program to begin to mature that capability and rationalise the existing IT Applications portfolio through consolidation of applications.
- **The total actual/estimated capex expenditure for this activity in the 2015-20 RCP, which forms the baseline for this business case, was \$80.0 million.**
- Thus, the recurrent IT capital plan for the 2020-25 RCP needs to consider:
 - increased maturity that has led to efficiencies in managing the upgrade and patching of applications to manage costs;
 - consolidation of applications to core platforms; and
 - an increase in capability, requiring upgrades and patching, offered through the implementation of new applications.

We have explored the two detailed above options to determine whether they would provide better outcomes than the baseline for cost or for operational risk.

3. Detailed Options Assessment

Assessing the options involved:

- Application of the NER objectives and the additional criteria detailed above.
- A risk assessment of each option using SA Power Networks’ risk management framework.
- The construction of financial models.
- Assessment against the AER’s Expenditure Forecast Assessment Guidelines.

This approach ensured that the risks, costs, benefits and impacts of each option were fully understood and the selected option was the most prudent and efficient.

4.3 Costs, benefits and risks of Option 1

Option 1: Patch and upgrade all systems, irrespective of business criticality, to Vendor Release Schedule, takes a conservative approach to IT Application security, reliability and vendor support by patching and upgrading as these are released by the vendor. This option provides a state where:

- systems would be patched, upgraded and supported according to the release schedule provided by the vendor; and
- small changes would be applied to keep the business functioning in synchronisation with externally driven changes in SA Power Networks’ customer preferences, business and network environment such as:
 - legislative and statutory and regulatory compliance change (eg payroll, superannuation and tax changes or changes to ASIC mandated accounting standards);
 - change in feeder systems external to SA Power Networks (eg weather website data); and
 - changes to external processes in which SA Power Networks is a participant (eg Dial-Before-You-Dig).

This would keep our systems fully up to date in accordance with vendor release schedules for the applications but does not otherwise add or significantly modify functionality. All applications would be patched and maintained without reference to their relative importance to our day to day business activities.

The option scope has been reduced to allow for the fact that there will be a major SAP upgrade during the period and GIS Consolidation performed and as a result there is an opportunity to reduce the amount of

business as usual patching to be undertaken during that time. These programs are the subject of a separate business cases (ie SAP Upgrade Business Case, GIS Consolidation Business Case).

This option will also require \$3.6 million opex uplift as a result of the move of the Click application (used for field work scheduling and works management) to the cloud (refer Appendix B). This opex uplift is common to both options.

Costs

The estimated costs for Option 1 are shown below:

Table 7: Option 1 Summary forecast capex, \$million (Dec \$2017)

Summary forecast capex for Option 1						
Summary	2020/21	2021/22	2022/23	2023/24	2024/25	TOTAL 2020-25
Total IT Applications capex	28.566	28.598	20.595	19.903	27.774	125.437
TOTAL	28.566	28.598	20.595	19.903	27.774	125.437

Table 8: Option 1 forecast capex, \$million (Dec \$2017)

Forecast capex for Option 1 by IT Application Platform Group						
Application Platform Group	2020/21	2021/22	2022/23	2023/24	2024/25	TOTAL 2020-25
Asset Location Information	1.940	2.027	2.027	1.765	1.765	9.525
Asset Management Small Systems and Safety & Risk Management	0.610	1.133	1.133	0.610	0.610	4.098
Asset Planning and Design	1.674	1.674	1.674	1.674	1.674	8.370
Customer Facing Website and Mobile Applications	0.741	0.719	0.763	0.785	0.741	3.749
Customer Network Billing	0.506	0.144	-	0.044	0.044	0.737
IT Management Systems	0.593	0.593	0.593	0.593	0.593	2.964
National Electricity Market Systems	1.874	1.874	1.831	1.831	1.874	9.285
Network Operations Centre Systems	0.924	0.730	0.580	0.607	0.770	3.610
Office and Collaboration Tools	0.384	0.384	0.384	0.384	0.384	1.918
SAP Suite	19.015	19.015	11.306	11.306	19.015	79.656
Works Management and Scheduling	0.305	0.305	0.305	0.305	0.305	1.526
TOTAL	28.566	28.598	20.595	19.903	27.774	125.437

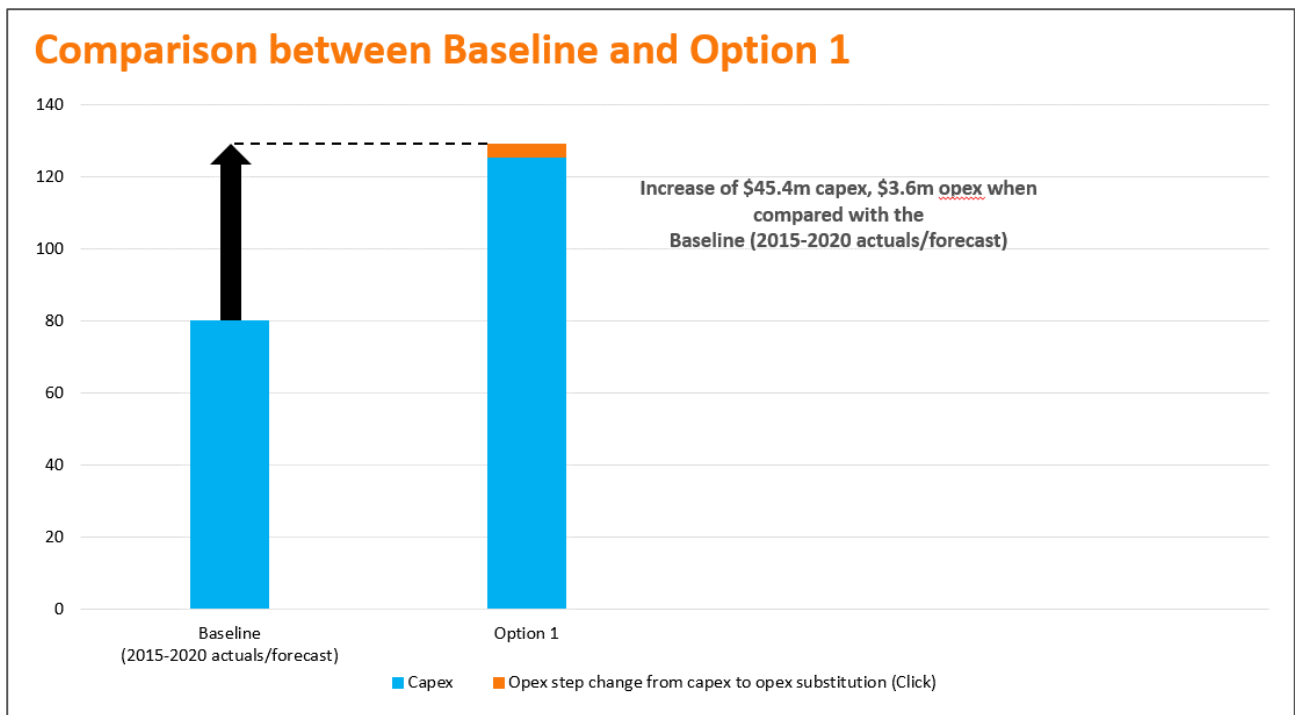


Figure 4: Comparison Between Baseline and Option 1²⁰

Benefits

- Applications are maintained at a level that can properly support the business to provide safe, secure and reliable distribution services.
- Field service staff have access to critical safety and job information when they need it to enable the safe and efficient delivery of distribution services.
- Continued compliance with our regulatory obligations and requirements.
- Customers services and information are available when they are needed as the applications are patched, upgraded, managed and secured.
- New application features are available for use sooner.
- Ensures the supportability of, and compatibility between, our IT Applications.

Disadvantages

- Significant increase in expenditure.
- Early adoption of new technology can introduce risks because fixes to defects may not have been released by the vendor (ie early adopters often discover these issues as they implement these early releases).
- Does not consider the growing maturity of the organisation in managing its Application portfolio more efficiently.
- Does not comply with our IT Asset Management Plan.

Risks

The following operational risk assessment has been conducted in accordance with SA Power Networks' Corporate Risk Framework (refer Appendix A). This includes the application of the appropriate qualitative measures of likelihood and consequence, and the resulting overall risk rating.

The following risks are assessed against Option 1.

²⁰ Refer Appendix B for details of Click capex to opex substitution. The Click opex increase for both options, during the 2020-25 RCP, is \$3.6m

Table 9: Option 1 Risk Assessment

Risk ID	Risk Description	Consequence Description	Likelihood	Consequences	Risk Rating
1	Network Reliability	<p>The operation and reliability of the distribution network is heavily dependent on the IT Applications portfolio and any network reliability issue can, in turn, result in liability. The management of emergency response field crews is also heavily dependent on IT Systems.</p> <ul style="list-style-type: none"> Reliability (> 40,000 customers affected for an extended period of time) Financial (\$10m > SLAs < \$100m) Reputation / Customer Service (Repeated interventions by ombudsman or regulators) 	Unlikely	Major	Medium
2	Market Obligations	<p>If NEM obligations potentially compromised by delayed processing of customer transactions, then SA Power Networks would be liable for significant non-compliance penalties.</p> <ul style="list-style-type: none"> Financial (\$1m < Penalties < \$10m) 	Rare	Moderate	Low

Risk ID	Risk Description	Consequence Description	Likelihood	Consequences	Risk Rating
3	Health and Safety <ul style="list-style-type: none"> Critical and Life Support Customers Bushfire Risk Management Switching Activities 	<p><u>Critical and Life Support Customers:</u> Network outage management teams unable to identify, notify and maintain reliability of supply to critical and life support customers. There are potentially catastrophic consequences associated with not being able to identify critical and life support customers. SA Power Networks has more than 9,500 NMI's recorded for life support customers.</p> <ul style="list-style-type: none"> WH&S (Multiple Fatalities) Financial/Regulatory (> \$100m penalties for notification failures) Reputation (adverse media coverage/repeated intervention by Regulator) <p><u>Bushfire Risk Management:</u> SA Power Networks unable to manage bushfire risks as several systems are integrated together to enable SA Power Networks to determine 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.</p> <ul style="list-style-type: none"> WH&S (Multiple Fatalities) Financial / Regulatory (Fines, Court Action, Compensation Costs for loss of life and property) Reputational (Adverse media campaigns, Intervention by Regulator) <p><u>Switching Activities:</u> GIS information integrated with other key IT systems is used to accurately identify impacts of switching activities in the field. This can have WH&S consequences for field services personnel, other emergency services personnel, and the general public, particularly during severe weather events.</p> <ul style="list-style-type: none"> WH&S (Death or Permanent Disability) Financial / Regulatory (Related Fines, Workcover, Court Action, Compensation Costs) Reputation (Adverse media coverage) <p>Organisational (Industrial action in the event workers are injured or killed)</p>	Rare	Catastrophic	Medium
4	Market Billing	Ability to generate DUoS billing to Retailers impeded, placing the main corporate cash flow at risk and potentially restricting business operations. <ul style="list-style-type: none"> Financial (\$10m > Cash Flow < \$100m) 	Rare	Major	Low

Risk ID	Risk Description	Consequence Description	Likelihood	Consequences	Risk Rating
5	Legal Compliance	<p>Unable to efficiently implement regulatory compliance changes to IT systems such as payroll, superannuation, tax changes and ASIC mandated alterations to accounting standards exposing SA Power Networks and its 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.</p> <ul style="list-style-type: none"> Financial/Regulatory (\$1m < Penalties < \$10m) Organisational (Significant impact due to HR issues, industrial action and related reputational damage) 	Rare	Minor	Negligible
6	Regulatory and Reliability Reporting	<p>Ability to generate accurate regulatory and reliability reporting, which is heavily dependent on IT systems, could be compromised.</p> <ul style="list-style-type: none"> Reputation (Intervention by regulators) Regulatory / Financial (\$1m < Penalties >\$10m) 	Rare	Moderate	Low
7	Planned Asset Maintenance	<p>Ability to effectively manage network assets, the data for which is maintained within IT systems and used as inputs for identifying, planning and scheduling inspections and maintenance work over the long-term, could be impacted. The inability to prioritise, plan and schedule planned work correctly would have an adverse impact on ongoing costs (both opex and repex).</p> <ul style="list-style-type: none"> Financial (Cost impact > \$10m) 	Rare	Major	Low
8	Security	<p>The vulnerability of an IT system to security breaches is related to its security configuration, 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. SA Power Networks could also expect significant penalties from regulators and aggrieved party legal actions.</p> <ul style="list-style-type: none"> Reliability (> 40k customers without supply for extended period) Regulatory / Financial (Fines, legal action, damaged equipment) WH&S (Death or permanent disability) Reputation (Adverse media, intervention by regulators) 	Unlikely	Major	Medium

Risk Summary	
The overall risk rating for this option is:	Medium

Additional Assessment Criteria

Table 10: Option 1 Additional Assessment Criteria Ratings

Operational Assessment Criteria	Rating	Rationale
Likely impact to customers	Low	No customer impacts identified.
Risk of ongoing operation	Medium	From Risk Summary above.
Balance between cost and risk	Poor	Risk level acceptable. Costs significantly above baseline (ie \$47.7 million capex and \$3.2 million opex above 2015-20 RCP actuals/estimates) for no significant reduction in risk.
Fit with SAPNs' IT Asset Management Plan	Poor	Planned activity not based on application criticality to business.
Capability to support planned projects	Fair	The significant uplift in both frequency and scale of ongoing upgrade and patching activities may pose some delivery risk to planned projects.

4.4 Costs, benefits and risks of Option 2

Option 2: Risk based approach to manage IT Applications, proposes a prudent and timely approach to patching, maintenance and upgrades for applications. This option provides a state where:

- systems are patched, upgraded and supported in an effective manner based on their criticality to the business (as identified by the IT Asset Management plan); and
- applications are maintained at a level that can reliably support the business.

This will result in a continued ability to manage system and service risk but does not add or significantly modify functionality.

In common with Option 1, this option has been reduced to allow for the fact that there will be a major SAP upgrade during the period and a GIS Consolidation performed and as a result there is an opportunity to reduce the amount of business as usual patching to be undertaken during that time. These programs are the subject of a separate business cases (ie SAP Upgrade Business Case, GIS Consolidation Business Case).

This option will also require \$3.6 million opex uplift as a result of the move of the Click application (used for field work scheduling and works management) to the cloud (refer Appendix B). This opex uplift is common to both options.

Costs

The estimated costs for Option 2 are shown below:

Table 11: Option 2 Summary forecast capex, \$million (Dec \$2017)

Summary forecast capex for Option 2						
Summary	2020/21	2021/22	2022/23	2023/24	2024/25	TOTAL 2020-25
Total IT Applications capex	15.007	15.503	13.252	12.057	14.015	69.832
TOTAL	15.007	15.503	13.252	12.057	14.015	69.832

Table 12: Option 2 forecast capex, \$million (Dec \$2017)

Forecast capex for Option 2 by IT Application Platform Group						
Application Platform Group	2020/21	2021/22	2022/23	2023/24	2024/25	TOTAL 2020-25
Asset Location Information	1.479	1.567	1.330	1.242	1.242	6.861
Asset Management Small Systems and Safety & Risk Management	0.610	1.133	1.133	0.610	0.610	4.098
Asset Planning and Design	1.151	1.151	1.151	1.151	1.151	5.754
Customer Facing Website and Mobile Applications	0.741	0.719	0.414	0.436	0.741	3.051
Customer Small Systems	0.506	0.144	-	0.044	0.044	0.737
IT Management Systems	0.593	0.593	0.593	0.593	0.593	2.964
National Electricity Market Systems	1.874	1.874	1.831	1.831	1.874	9.285
Network Operation Centre Systems	0.924	0.730	0.580	0.607	0.770	3.610
Office and Collaboration Tools	0.384	0.384	0.384	0.384	0.384	1.918
SAP Suite	6.439	6.902	5.531	4.855	6.301	30.028
Works Management and Scheduling	0.305	0.305	0.305	0.305	0.305	1.526
TOTAL	15.007	15.503	13.352	12.057	14.015	69.832

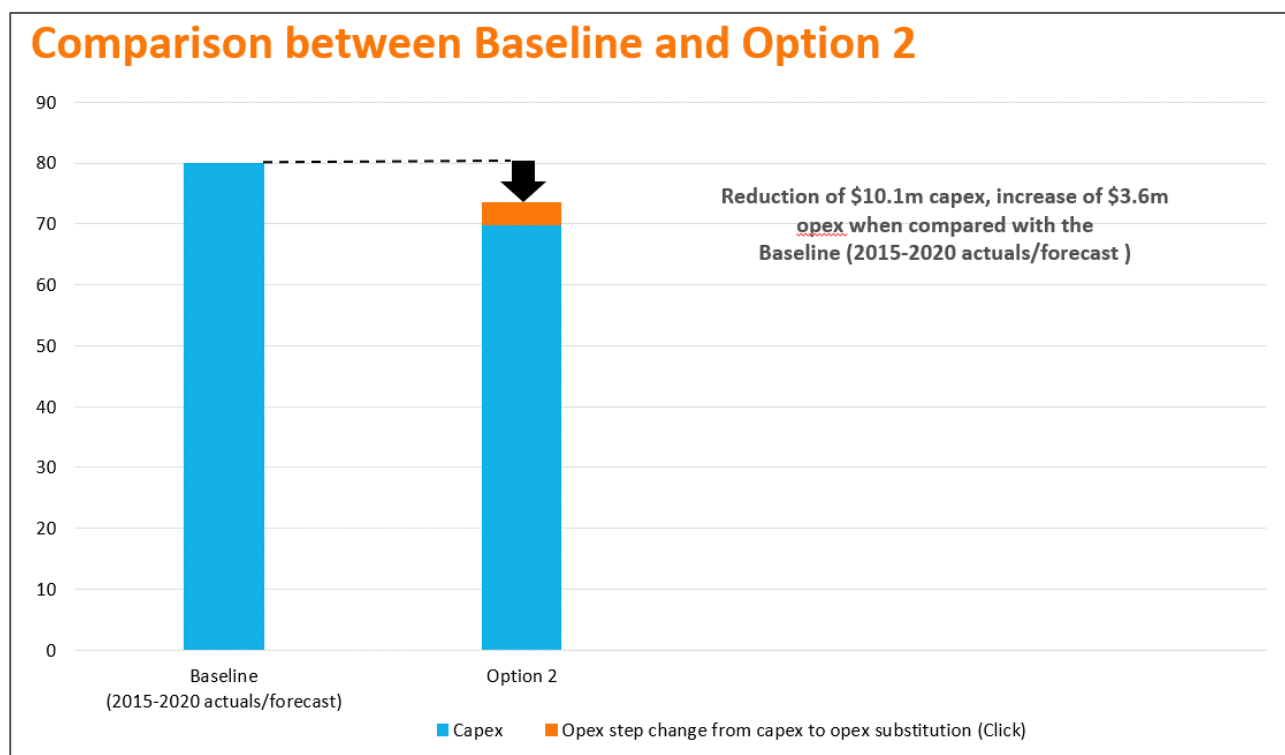


Figure 5: Comparison Between Baseline and Option 2²¹**Benefits**

- Lower cost option than both Option 1 and the baseline (ie IT Applications recurrent capex forecast for 2015-20 RCP).
- Applications are maintained at a level that can properly support the business to provide safe, secure and reliable distribution services.
- Field service staff have access to critical safety and job information when they need it to enable the safe and efficient delivery of energy services.
- Continued compliance with our regulatory obligations and requirements.
- Customers, services and information are available when they are needed as the applications are patched, upgraded, managed and secured.
- Compliant with our IT Asset Management strategy which is to extend the useful life of systems by prudent upgrades and updates.
- Ensures the supportability of, and compatibility between, SA Power Networks' IT Applications.

Disadvantages

- New application features are not immediately available for use.
- This approach requires more proactive management of the IT Applications portfolio as business criticality changes over time.

Risks

The following operational risk assessment has been conducted in accordance with SA Power Networks' Corporate Risk Framework (refer Appendix A). This includes the application of the appropriate qualitative measures of likelihood and consequence, and the resulting overall risk rating.

The following risks are assessed against Option 2.

Table 13: Option 2 Risk Assessment

Risk ID	Risk Description	Consequence Description	Likelihood	Consequences	Risk Rating
1	Network Reliability	<p>The operation and reliability of the electrical distribution network is heavily dependent on the IT Applications portfolio and any network reliability issue can, in turn, result in liability. The management of emergency response field crews is also heavily dependent on IT Systems.</p> <ul style="list-style-type: none"> • Reliability (> 40,000 customers affected for an extended period of time) • Financial (\$10m > SLAs < \$100m) • Reputation / Customer Service (Repeated Interventions by ombudsman or regulator) 	Unlikely	Major	Medium

²¹ The Click opex increase occurring within the 2015-20 RCP, but after the 2018/19 base year, is \$357,000 (refer to Appendix B for details of Click capex to opex substitution). The Click opex step change for both options, during the 2020-25 RCP, is \$3.6m.

Risk ID	Risk Description	Consequence Description	Likelihood	Consequences	Risk Rating
2	Market Obligations	<p>If National Electricity regulatory market obligations potentially compromised by delayed processing of Customer transactions, then SA Power Networks would be liable for significant non-compliance penalties.</p> <ul style="list-style-type: none"> Financial (\$1m < Penalties < \$10m) 	Rare	Moderate	Low
3	<p>Health and Safety</p> <ul style="list-style-type: none"> Critical and Life Support Customers Bushfire Risk Management Switching Activities 	<p><u>Critical and Life Support Customers:</u> Network outage management teams unable to identify, notify and maintain reliability of supply to critical and life support customers. There are potentially catastrophic consequences associated with not being able to identify critical and life support customers. SA Power Networks has more than 9,500 NMI's recorded for Life Support Customers.</p> <ul style="list-style-type: none"> WH&S (Multiple Fatalities) Financial/Regulatory (> \$100m penalties for notification failures) Reputation (adverse media coverage/repeated intervention by regulators) <p><u>Bushfire Risk Management:</u> SA Power Networks unable to manage bushfire risks as several systems are integrated together to enable SA Power Networks to determine 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.</p> <ul style="list-style-type: none"> WH&S (Multiple Fatalities) Financial / Regulatory (Fines, Court Action, Compensation Costs for loss of life and property) Reputational (Adverse media campaigns, Intervention by Regulator) <p><u>Switching Activities:</u> GIS information integrated with other key IT systems is used to accurately identify impacts of switching activities in the field. This can have WH&S consequences for field services personnel, other emergency services personnel, and the general public, particularly during severe weather events.</p> <ul style="list-style-type: none"> WH&S (Death or permanent disability) Financial / Regulatory (Related Fines, Workcover, Court Action, Compensation Costs) Reputation (Adverse media coverage) Organisational (Industrial action in the event workers are injured or killed) 	Rare	Catastrophic	Medium

Risk ID	Risk Description	Consequence Description	Likelihood	Consequences	Risk Rating
4	Market Billing	Ability to generate DUOS billing to Retailers impeded, placing the main corporate cash flow at risk and potentially restricting business operations. • Financial (\$10m > Cash Flow < \$100m)	Rare	Major	Low
5	Legal Compliance	Unable to efficiently implement regulatory compliance changes to IT systems such as payroll, superannuation, tax changes and ASIC mandated alterations to accounting standards exposing SA Power Networks as its 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. • Financial/Regulatory (\$1m < Penalties < \$10m) • Organisational (Significant impact due to HR issues, industrial action and related reputational damage)	Rare	Minor	Negligible
6	Regulatory and Reliability Reporting	Ability to generate accurate regulatory and reliability reporting, which is heavily dependent on IT systems, could be compromised. • Reputation (Intervention by regulators) • Regulatory / Financial (\$1m < Penalties > \$10m)	Rare	Moderate	Low
7	Planned Asset Maintenance	Ability to effectively manage network assets, the data for which is maintained within IT systems and used as inputs for identifying, planning and scheduling inspections and maintenance work over the long-term, could be impacted. The inability to prioritise, plan and schedule planned work correctly would have an adverse impact on ongoing costs (both opex and repex). • Financial (Cost impact > \$10m)	Rare	Major	Low
8	Security	The vulnerability of an IT system to security breaches is related to its security configuration, 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. SA Power Networks could also expect significant penalties from Regulator and aggrieved party legal actions. • Reliability (> 40,000 customers without supply for extended period) • Regulatory / Financial (Fines, legal action, damaged equipment) • WH&S (Death or permanent disability) • Reputation (Adverse media, intervention by regulators)	Unlikely	Major	Medium

Risk Summary		
The overall risk rating for this option is:		
Medium		

Additional Assessment Criteria

Table 14: Option 2 Additional Assessment Criteria Ratings

Additional Assessment Criteria	Rating	Rationale
Likely impact to customers	Low	No customer impacts identified.
Risk of ongoing operation	Medium	From Risk Summary above.
Balance between cost and risk	Good	Risk level acceptable. Costs below baseline (ie actuals/estimates for the 2015-20 RCP). Costs are \$55.7 million lower than Option 1.
Fit with SAPNs' IT Asset Management Plan	Good	Planned activity based on application criticality to business.
Capability to support planned projects	Good	Planned activity has been adjusted to account for planned project work.

4.5 Summary of cost, benefit and risk assessment of each option

A summary of the additional assessment criteria associated with the options is provided in Table 15.

Table 15: Additional Assessment Criteria Ratings versus Options Considered

Option	Additional Assessment Criteria & Ratings				
	Likely impact to customers	Risk of ongoing operation	Balance between cost and risk	Fit with SAPN IT Asset Management Plan	Capability to support planned projects
Option 1: Patch and Upgrade all systems, irrespective of business criticality, to Vendor Release Schedule	Low	Medium	Poor	Poor	Fair
Option 2: Risk-based Approach to Manage IT Applications	Low	Medium	Good	Good	Good

A summary of the costs and benefits associated with the options detailed above is set out in Table 16.

Table 16: Costs, benefits and risks associated with options considered, \$million (Dec \$2017)

Option	5-year analysis: 2020-25 RCP				10-year NPV ²²	Overall Risk Rating	Ranking
	Capex ²³	Opex step change ²⁴	Totex ²⁵	NPV ²⁶			
Do Nothing	-	-	-	-		Extreme	
2015-20 RCP Actuals/Forecast (Baseline)	80.0	-	80.0	75.4	140.8		
Option 1: Patch and Upgrade all systems, irrespective of business criticality, to Vendor Release Schedule	125.4	3.6	129.0	116.7	231.4	Medium	2
Option 2: Risk-based Approach to Manage IT Applications	69.8	3.6	73.4	64.0	124.2	Medium	1

We note that:

- All option costs were supported by detailed cost models and key assumptions, based on industry-standard estimation methods.

²² NPV of the proposed expenditure over the 10-year period from 1 July 2020 to 30 June 2030, based on discount rate of 2.89%. Note that since it is difficult to predict the changing technological factors over such a lengthy timeframe, for the purposes of the ten-year NPV calculation, the expenditure has been extrapolated based on the 2020-25 RCP costs. Where costs have been reduced in the 2020-25 RCP to reflect temporary reduction in maintenance activity due to the SAP S/4 Upgrade, this has been added back, where still relevant, in the 2025-30 RCP.

²³ Represents the total capex associated with the proposed option over the 2020-25 RCP.

²⁴ Represents the total opex step change (new opex minus absorbed opex) associated with the proposed option over the 2020-25 RCP. The step change is from Click capex to opex substitution for Click SaaS (refer Appendix B).

²⁵ The efficiency of the capex to opex substitution expressed as totex (total capital plus opex step change) for the base case minus the totex for the selected option over the period from 1 July 2020 to 30 June 2025. (i.e. +ve is efficient)

²⁶ NPV of the proposed investment over the 2020-25 RCP, based on discount rate of 2.89%.

- Cost estimates were based on both current analysis and historical costs of similar projects.
- The costs have been validated with subject matter experts for reasonableness and completeness.

4.6 Option selected

The selected option is Option 2 to extend the useful life of IT Applications by adopting a prudent and systematic approach to patching and upgrades.

Option 2 has been selected as it:

- achieves the expenditure objectives (eg managing or meeting the demand for standard control services, complying with applicable regulatory obligations and requirements, and maintaining the quality, reliability, security and safety of the distribution system);
- balances efficient costs with a level of risk that is prudent for SA Power Networks to accept in accordance with good electricity industry practice; and
- enables the key drivers.

4.7 Supporting evidence

The electricity industry, including AEMO, has an increasing reliance on fit for purpose IT systems. All DNSPs must maintain their IT systems in a prudent and efficient manner and have submitted regulatory proposals to support similar programs of work.

Almost all recent DNSP proposals highlight the importance of ensuring IT systems and data are secure from cyber security threats. These threats, which have been highlighted by recent cyber security events around the work, can be reduced by (amongst other things) implementing vendor supplied patching when available. The past 12 months have seen new critical infrastructure system and data control obligations arise under the *Security of Critical Infrastructure Act 2018* (Cth) and the Notifiable Data Breaches scheme under Part IIIC of the *Privacy Act 1988* (Cth) (**Privacy Act**) passed through Parliament. Additionally, the Finkel Review has resulted in the establishment of the Energy Security Board, following which we have already been instructed to participate in an audit of our cyber security maturity level and contribute to the Australian Energy Sector Cyber Security Framework. The continued increase in regulatory obligations and requirements in this area is a key driver of making appropriate and prudent levels of investment to ensure our IT systems are secure.

Maintaining compatibility between our IT Applications and those of external entities, including as required by ongoing regulatory and market changes, drives change in our IT systems. The change frequency for these types of activities for applications is determined by others. To enable us to continue to provide our services our IT platforms need to be both vendor-supported and, when prompted by those services, upgraded, to maintain compatibility between the services and our IT systems. An example is the need to ensure that our national market systems and billing systems integrate and operate with AEMO.

4.8 Dependencies

This business case assumes that our selected option for the SAP Upgrade program will take place in the 2020-25 period. This is a very significant change due to the end-of-life of the current SAP version. During the 2015-20 RCP of the migration some maintenance will be subsumed by the project while the transition is occurring. Hence the business as usual maintenance has been reduced during the transition years. The SAP upgrade is the subject of a separate business case. If that business case not be accepted by the AER then additional capital costs of \$1.214 million will need to be added to the expenditure associated with the IT Applications work program for the 2020-25 RCP.

Further to this, if the SAP Upgrade Business Case does not proceed during the 2020-25 RCP there will be a significant uplift in IT recurrent IT capex in 2025-30 RCP and beyond. This uplift would be related to the costly workarounds and remediation work related to the lapse in SAP software support and the attempted resolutions of the issues related to the lapse of support as they are realised from 2025 onwards.

This business case also assumes that our selected option for the GIS Consolidation Business Case will take place in the 2020-25 RCP. During the period of consolidation, some maintenance will be subsumed by the project while the transition is occurring. Hence the business as usual maintenance has been reduced during the transition years. GIS Consolidation is the subject of a separate business case. If the expenditure associated with the GIS Consolidation Business Case is not accepted by the AER, then additional costs of \$0.649 million will need to be added to the expenditure associated with the IT Applications program for the 2020-25 RCP.

Finally, this business case also assumes that our selected option for the PSS Redevelopment Business Case will take place in the 2020-25 RCP. If the expenditure associated with our selected option for the PSS Redevelopment Business Case is not accepted by the AER, then additional costs of \$1.672 million, for the ongoing maintenance activities associated with the existing PSS, will need to be added to the expenditure associated with the IT Applications program for the 2020-25 RCP.

4.9 Regulatory framework

Clauses 6.5.6 and 6.5.7 of the NER set out the capex and opex objectives to be applied in assessing proposed expenditure for the 2020-25 RCP. These objectives, along with the capex and opex criteria and factors applicable to this expenditure, are summarised below.

This expenditure meets the requirements of the capex and opex objectives in clauses 6.5.6(a) and 6.5.7(a) of the NER. In particular, the expenditure is required to:

- ***Meet and manage the demand for network services*** - The proposed expenditure is necessary for the effective and efficient operation of SA Power Networks' IT Applications and systems, which, in turn, are critical for the effective and efficient operation of the network and meeting and managing the demand for network services. The proposed expenditure will also enable SA Power Networks to maintain the reliability of the distribution system using less expenditure than in previous RCPs (and less expenditure over time) and optimising other aspects of the systems that provide services to customers and the business.
- ***Maintain the reliability, security and safety of the distribution system*** – The proposed expenditure will assist in maintaining the secure and reliable operation of SA Power Networks' electrical network by:
 - ensuring SA Power Networks' IT Applications are maintained within an acceptable level of risk (eg via regular upgrades, replacement of small-medium 'end of life' systems) in accordance with their relative criticality to the business;
 - ensuring SA Power Networks' IT Applications and data are secure and operational (eg via regular patching, updates, security checks);
 - ensuring SA Power Networks' IT Applications remain compatible with each other and continue to support our business processes; and
 - ensuring efficient 'break-fix' services and remediation can be undertaken for IT Applications.
- ***Comply with applicable regulatory obligations and requirements*** – The proposed expenditure will enable SA Power Networks to maintain compliance with all applicable regulatory obligations or requirements and small-medium new, changed or removed regulatory obligations or requirements in a timely manner when required.

The forecast expenditure meets the capex and opex criteria in clauses 6.5.6(c) and 6.5.7(c) of the NER because:

- ***Efficient*** – The IT Applications program will enable SA Power Networks to improve the efficiency and effectiveness of SA Power Networks' IT Applications and asset management processes and operational

efficiency generally. The expenditure can therefore be considered consistent with the expenditure that a prudent service provider acting efficiently would incur.

- **Prudent** – The IT Applications program is necessary in order to maintain an acceptable level of risk, and adopt processes which are prudent and consistent with good electricity industry practice, in a way that also minimises the operational costs in doing so in the long-term.
- **Realistic expectation of the demand forecast and cost inputs** – The forecast expenditure for the 2020-25 RCP is based a realistic expectation concerning the need for efficient and efficient IT Applications, which is consistent with the needs of other DNSPs in Australia and the requirements of *good electricity industry* practice. In addition, the expenditure has been developed applying historic costs from the 2015-20 RCP adjusted to reflect the expected volume of activity during the 2020-25 RCP, on an application by application basis. These changes include security patching, small-medium business system upgrades and replacements, minor system changes to maintain currency and/or compliance, and reliability and remediation activities.

Glossary

Acronym / Abbreviation	Definition
AER	Australian Energy Regulator
ASIC	Australian Securities and Investments Commission
BW	Business Warehouse
capex	capital expenditure
CRM	Customer Relationship Management [system]
Click	Click Scheduling software
DBYD	Dial Before You Dig
DNSP	Distribution Network Service Provider
FSE	Field Services Edge [Click Scheduling software]
GIS	Geographic Information Systems
HR	Human Resources
IT	Information Technology
NEM	National Electricity Market
NER	National Electricity Rules
NPV	Net Present Value
OMS	Outage Management System
opex	operating expenditure
PSS	Protection Settings System Redevelopment
RCP	Regulatory Control Period
repex	replacement expenditure
RIN	Regulatory Information Notice
SaaS	Software as a Service
S/4	New version of SAP
SAP	Systems Applications Products [enterprise resource planning software platform]
SAPN	SA Power Networks

A. Appendix A: SA Power Networks Risk Management Framework

The SA Power Networks' risk management framework defines the following quantitative measures of likelihood and consequence that are in turn used to determine the risk rating. The detailed risk assessment instructions are available on the SA Power Networks Intranet site.

Risk Likelihood Rating

Rating	Descriptor	Description	Probability	Indicative Frequency
5	Almost Certain	Is expected to occur	96 – 100%	At least one event per year
4	Likely	It will probably occur	81 – 95 %	One event per year on average
3	Possible	May occur	21 – 80%	One event per 2 – 10 years
2	Unlikely	Not likely to occur	6 – 20%	One event per 11 – 50 years
1	Rare	Most unlikely to occur	0 – 5%	One event per 51 – 100 years

Risk Consequence Rating

Rating	1 Minimal	2 Minor	3 Moderate	4 Major	5 Catastrophic
Financial	Less than \$100,000	\$100,000 or more, but less than \$1m	\$1m or more, but less than \$10m	\$10m or more, but less than \$100m	\$100m or more
OH and S	Incident but no injury	Medical treatment only	Lost time injury	Death or Permanent Disability	Multiple Fatalities
Environment	Brief spill incident. No environmental damage.	Minor spill. Pollutant on site. No environmental damage.	Escape of pollutant causing environmental damage	Significant pollution on and off site < \$0.5 m	Long term environmental damage
Reputation / Customer Service	Localised customer complaints	Widespread customer complaints or Complaints to Ombudsman or Regulator	Intervention by the Ombudsman or Regulator	Repeated intervention by the Ombudsman or Regulator	Loss of Distribution Licence
	Adverse regional media coverage	Adverse State media coverage	Adverse media campaigns by customers, media, industry groups	Severe negative impact on both regulated and un-regulated businesses	Loss of Distribution Licence
Legislative and Regulatory	Minor breaches by employees resulting in customer complaints or publicity	Act or Code infringements resulting in minor fines	Severe Company or Officer fines for Act or Code Breaches	Prison sentences for Directors or Officers	Loss of Distribution Licence
	ACCC require apology and / or corrective advertising	ACCC require special offer be made to all customers / suppliers	ACCC minimum level penalties	ACCC moderate level penalties	ACCC maximum level penalties
	Directors / Officers given minimum fines	Directors / Officers given moderate fines	Directors / Officers given severe fines	Directors / Officers given prison sentences	Loss of Distribution Licence
Organisational	Absorbed without additional management activity	Absorbed with minimal management activity	Significant event which requires specific management	Critical event which can be endured with targeted input	Disaster which can cause collapse of the business

Rating	1 Minimal	2 Minor	3 Moderate	4 Major	5 Catastrophic
Reliability	2000 customers without supply for a min. of 12 hours (ie, a medium size urban feeder)	10,000 customers without supply for a min. of 24 hours (ie, a major storm related outage or a major substation outage)	Up to 40,000 customers without supply for a min. of 48 hours (ie, major multiple zone substation coincident outages)	Over 40,000 customers without supply for longer than 48 hours (ie, major geographical areas off supply)	Adelaide CBD without supply for longer than 24 hours

Risk Classification Rating

Likelihood (Probability)	Threat Consequences				
	Minimal (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Almost Certain (5)	Medium	High	High	Extreme	Extreme
Likely (4)	Low	Medium	High	High	Extreme
Possible (3)	Low	Low	Medium	High	High
Unlikely (2)	Negligible	Low	Low	Medium	High
Rare (1)	Negligible	Negligible	Low	Low	Medium

B. Appendix B: Click capex to opex substitution step change proposal

Topic	Detail	
Background	<p>The Click software is a critical application supporting the planning, scheduling and dispatch of work to field crews and is also widely used by supervisors and managers.</p> <p>During the 2015-20 RCP the current Click software version reaches end-of-life and there is no upgrade path for the existing on-premise solution. The vendor offers an alternative product called Click Field Service Edge (FSE) that is only offered as a software as a service (SaaS) product on a subscription basis.</p> <p>The Click FSE solution is considerably more expensive than the incumbent on-premise Click software. The five-year costs for the current system and the new FSE system are as follows:</p> <ul style="list-style-type: none">• Current system is \$6.8 million comprising \$1.7 million opex (licensing) and \$5.1 million capex (ongoing upgrades / patches).• New FSE system is \$9.2 million in operational subscription cost opex, and \$1.5 million capex (ongoing patch release testing).	
Options considered	<p>We performed a requirements and options analysis and market scan for scheduling and related mobility solutions. Options reviewed included SAP Multi-Resource Scheduling (MRS) in combination with SAP Work Manager and other market participants. However, the alternative products considered do not provide the functionality required to enable the effective and efficient operation of SA Power Networks. We also determined that migrating to the Click cloud version was significantly less disruptive and much lower risk to business operations than migrating to an alternative product.</p>	
Request	<p>We are proposing a capex-opex substitution step change of \$3.6 million to contribute to the ongoing costs of the alternative product, Click FSE. This amount reflects the foregone capex related to what would have otherwise been spent on ongoing upgrades to the on-premise Click software. The residual \$3.9 million in opex will be accommodated within our existing opex allowances.</p> <p>Given the critical nature of the business services supported and enabled by the Click software, the proposed expenditure reflects the efficient and prudent approach required to manage demand for network services, comply with applicable regulatory obligations and requirements, and maintain the security and reliability of our electrical network.</p>	
Opex Position		Value
Existing Click Scheduling/Mobility License Maintenance Opex @ \$340 k p.a. (Actual existing Click Scheduling & Mobility Licence maintenance)		\$1,700,000
Total New Click FSE Opex @ 1.841 m p.a. (Based on vendor negotiation of (\$90 per month per resource, for 1,705 resources consisting of 955 human and 750 non-human resources ²⁷)		\$9,207,000
Total opex impact of moving to Click FSE		\$7,507,000

²⁷ Non-human resources comprise machinery and equipment (eg, tracks) that need to be scheduled.

Topic	Detail	
	Per annum opex value	\$1,501,400
Capex		Value
Forgone – 2 upgrades of click within a 5-year period at \$1.3 million each (Last major Click Scheduling/Mobility Upgrade was \$1.3 million in Dec \$2017 terms)		-\$2,600,000
Forgone – Actual + Forecast Click Scheduling/Mobility patching and minor enhancements (As per actual/estimated capex for the 2015-20 RCP)		-\$2,500,000
New to FSE – New Click FSE release testing and integration		\$1,525,719
	Total capex impact of moving to Click FSE	-\$3,574,281
	Opex amount proposed as capex to opex substitution	\$3,574,281
	Per annum opex value from the proposed capex to opex substitution	\$714,856
Summary		Value
	Total opex impact of moving to Click FSE	\$7,507,000
	Amount proposed as capex to opex substitution	\$3,574,281
	Absorbed opex	\$3,932,719

C. Appendix C: Cost Model

The SAPN IT Applications Portfolio Cost Model document is available on request.