SA
Power
Networks

Supporting document 6.1

IT Infrastructure Refresh Business Case

**2020-2025
Regulatory Proposal**

January 2019

SA Power Networks

IT Infrastructure Refresh Business Case

IT regulatory submission for the 2020-25 regulatory control period

27/01/2019 – Version 3.1

Contents

1 Executive summary

Topic	Detail
Category of expenditure	• Recurrent non-network Information Technology (**IT**) capital expenditure (**capex**) • Operating expenditure (**opex**) step change from efficient capex to opex substitution
Context / background	Reliable IT Infrastructure underpins the delivery of all IT services which are, in turn, critical to the effective operation and maintenance of the electricity network, management of network outages, and provision of distribution services. The IT Infrastructure that enables the delivery of such IT services consists of both: • **Hosting Services** - those IT infrastructure services hosted in a data centre directly related to server-based computing, associated networking and data storage. • **Network Connectivity and Supporting Services** - those infrastructure components that provide network connectivity to hosting services, supporting management and platform capabilities on top of the hosting services, and support resiliency of our IT Infrastructure. Traditionally we have managed our infrastructure refresh program by prudent and efficient replacement of end-of life-assets, deferring replacement where risk is manageable. This was our previous best approach but with the recent advent of new technology we have followed the industry in exploring new ways of managing IT Infrastructure needs using cloud computing such as Infrastructure as a Service (**IaaS**). The Australian Government has recognised the importance of exploring cloud options stating that[1]: *"…agencies must now adopt cloud where it is fit for purpose, provides adequate protection of data and delivers value for money".* In addition to maintaining the distribution services enabled by our IT Infrastructure, we have also needed to respond to our changing business environment. Some of the key changes we are experiencing and have considered are: • customers demand more real time services and information related to electricity supply; • we have an increasing need for data on our ageing assets to manage the security and reliability of electricity supply in a prudent and efficient manner; • there is an increasing dependence on IT systems for the delivery of energy services; • we have increased our staff mobility and need to ensure adequate support and performance for staff from where ever they do their work; and • maintaining reliable services in a changing environment means having cost efficient infrastructure which supports a degree of flexibility in the delivery of the IT services.
Drivers	The key drivers are to achieve the following objectives: • maintaining reliable IT services to enable efficient delivery of distribution services; • maintaining IT infrastructure in an efficient manner while managing risk noting: – the majority of our current hosting infrastructure is end-of-life by 2020; and – we need to manage the service failure risk of Infrastructure Assets;

[1] https://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf, Foreword p.3.

Topic	Detail
	• managing cyber security risks including as required by new Critical Infrastructure Centre administered regulatory obligations and requirements under the *Security of Critical Infrastructure Act 2018* (Cth); • managing our response to vendor and industry driven cloud adoption in a prudent and efficient manner; and • efficiently maintaining support for distribution services whilst being more responsive to changes and peak demands for IT services (eg our increased usage of key services such as customers using outage maps during a storm). These drivers are explained in more detail in Section 2 of this business case.
Options considered	We have investigated options for addressing the drivers outlined above balancing maintaining service levels, cost and risk. The assessment process and related cost benefit analysis for each option are detailed in Section 4 - Options assessment. The inherent risk of not refreshing our IT Infrastructure represents an Extreme risk to the business. As such a Do Nothing option is not a credible option. As our IT Infrastructure comprises two types of services, options were considered separately for each type of service, with each being considered independently with minimal impact on the other. **Hosting Services** As our existing hosting services required a refresh and some of our vendors are driving cloud adoption, we broadened our approach and sought to model multiple scenarios and configurations of cloud and on premises options. The goal was to provide guidance of the most prudent and efficient refresh approach whilst enabling flexibility and scalability. We explored a number of different models and performed detailed cost benefit analysis of the following three options: • **Option 1 - Business as Usual:** continue with our current approach to refresh the assets in our two third-party data centres and adopt cloud solutions only when necessary due to vendor offerings of existing capabilities moving to Software as a Service (**SaaS**). • **Option 2 - Measured move to Cloud**: adopting a hybrid hosting model consisting of IaaS and SaaS, while retaining our two third-party data centres with a reduced footprint. • **Option 3 - Aggressive move to Cloud:** moving as much of our hosting services to the cloud as possible and removing the use of one of our existing third-party data centres. **Network Connectivity and Supporting Services** We considered options for the Network Connectivity and Supporting Services components of our IT infrastructure that were not addressed through the hosting analysis. The following options were considered for these components: • **Option 1 - Industry Standard Refresh:** explore refreshing our assets based on industry and vendor recommended life cycles. • **Option 2 - Business as Usual:** continue to refresh our assets in-line with our current approach.

Topic	Detail
	Adopting Industry Standard Refresh for connectivity and supporting technologies is not efficient (costs increase by 56% across a 10-year period, ie across the 2020 to 2030 period) and does not significantly reduce risks to justify the increase in cost. We therefore chose to retain our business as usual approach for Network Connectivity and Supporting Services and focused on the hosting options as the key differentiator in our holistic options assessment. This gave us three options for consideration in addressing our overall IT Infrastructure needs: • **Option 1** – **Business as Usual:** continue to refresh all our IT infrastructure using the same principles and approaches we have used in the past. The key difference to our existing IT infrastructure refresh being three SAP applications would move to a SaaS model, due to the vendor only providing them via SaaS, thus reducing the need to provision on-premise hosting services for them. • **Option 2** – **Measured Move to Cloud:** continue to refresh our IT infrastructure using the same principles and approaches we have used in the past but commence a measured transition of hosting needs into the cloud (SaaS and IaaS) whilst retaining our existing two third-party data centres with a reduced footprint. • **Option 3** – **Aggressive Move to Cloud:** continue to refresh our IT infrastructure using the same principles and approaches we have used in the past and decommission one of our third-party data centres due to transitioning as much of our hosting needs as possible into the cloud during the 2020-25 regulatory control period (**RCP**).
Option selected	Section 4 of this business case details the assessment process and related cost benefit analysis for each option. Option 2 – Measured Move Cloud, has been selected as the preferred option because it represents the lowest long-term cost to customers and is the most appropriate investment required to achieve the expenditure objectives and satisfy the drivers. In addition, it represents the lowest overall risk rating for the following reasons: • All options enable the efficient delivery of distribution services through maintaining our IT Infrastructure. • Option 1 does not provide the flexibility and scalability to meet business and customer demand for peak loads without upfront capex (which may still be insufficient). Nor is it in-line with the industry and vendor shift to providing SaaS, which will lead to us maintaining a largely out of date platform by the end of the 2020-25 RCP. • Option 3 has a high level of risk due to transitioning a far higher volume of our hosting needs to the cloud and reliance on a single data centre to provide a high-level of availability (ie no geographic redundancy). • By contrast, Option 2: – Maximises the asset life of our IT Infrastructure and presents an acceptable level of risk.

Topic	Detail
	– Represents the most efficient option by minimising the costs of refreshing our IT infrastructure with the lowest total expenditure (**totex**[2]) for the 2020-25 RCP. – Provides the ability to be flexible and scalable in meeting peak demand for IT services and being responsive to business and customer needs (eg by supporting peak demand for online real-time outage information during storms). – Appropriately aligns our approach to replacing IT infrastructure with vendor and industry trends. – Is an efficient substitution of capex for opex. Option 2 also provides the best fit with our Digital Strategy 2018-2025[3], and the aims of the Future Operating Model[4].
Estimated cost	The totex for Option 2 over the 2020-25 RCP is **$35.3 million**, an 8% reduction on our totex of $38.2 million for our IT infrastructure refresh in the 2015-20 RCP. This includes: • forecast capex of **$28.5 million**[5]; and • forecast step change in opex[6] of **$6.9 million**. This step change in opex is a capex to opex substitution for $7.7 million of additional capex that would otherwise need to be spent on IT hardware refresh and on-premise software upgrades.
Estimated benefits	The benefits of proceeding with Option 2 are: • Ensures IT infrastructure is current and operational to maintain service levels to customers by providing staff with access to reliable systems. • Utilises cloud hosting to enable us to flexibility scale to be more responsive to peak customer needs by only paying for capacity when needed. • Minimises cyber security risks which, in turn, reduces risks of power system disruption and threats to security and privacy of personal information of our customers and enables us to comply with our regulatory obligations. • Reduces risks to adverse organisational impact and increased costs due to minimising: – operational support needs; and – downtime associated with infrastructure failure or performance degradation. • Requires the lowest totex for the 2020-25 RCP and provides an efficient substitution of capex with opex, both in the long-term interests of our customers.
Risks of not proceeding	Not proceeding with the IT infrastructure refresh presents an overall **Extreme** level of risk due to increases in the following risks: • faults, instability and reduced performance of IT services will directly impact upon our ability to deliver distribution services and provide a reliable and safe electricity supply; • increasing likelihood of cyber security risks may put the distribution network at risk and result in information loss and non-compliance with regulatory obligations;

[2] Totex in the context of this business case represents the total capex plus opex step change.
[3] Digital Strategy 2018-2025.
[4] SA Power Networks Future Operating Model 2016–2031.
[5] All dollar values in this document are in Dec 2017 dollars and exclude corporate overheads.
[6] Opex increase compared to base year, minus opex benefits.

Topic	**Detail**
	• lack of support from suppliers resulting in inability to maintain our IT infrastructure if there is a failure; • increased complexity and associated costs to support and maintain the IT environment; • being unable to recover from IT outages in a timely manner that will directly impact business ability to service customers; and • adapting to future business and customer needs without significantly increasing costs. For further detail on risk assessment and the benefits associated with reducing the identified risks, refer to Section 2.2.
Regulatory framework	This expenditure is required in order to achieve each of the following capex objectives: • clause 6.5.7(a)(1) [Meet or manage the expected demand for standard control services]; • clause 6.5.7(a)(2) [Comply with all applicable regulatory obligations or requirements]; • 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], and the corresponding opex objectives in clause 6.5.6(a) of the NER. The forecast capex and opex also meet the capex and opex criteria by: • ensuring the efficient and effective operation and management of the network and delivery of network services to customers; • minimising the costs associated with IT services required to meet the expenditure objectives; • adopting processes which are prudent and consistent with good electricity industry practice; and • applying historical costs and approaches as a realistic expectation of efficient cost inputs.
Supporting evidence	The forecast expenditure for the 2020-25 RCP have been developed having regard to historic IT infrastructure refresh costs and updated forecasts on an asset class basis and are in line with supplier changes to support arrangements to ensure critical assets are kept within support. We considered multiple options for the use of cloud hosting through commissioning a detailed hosting strategy assessment. This assessment lead to the proposal to adopt a hybrid hosting model that has a lower totex than the other options considered. Refer to Section 5 **-** Supporting evidence for further detail.
Customer and stakeholder engagement	We engaged with the Consumer Consultative Panel (**CCP**) in relation to the need to move to higher usage of cloud hosting services at an IT Deep Dive workshop in June 2018. The CCP were interested in understanding the details related to costs in particular noting that participants at that workshop were broadly comfortable with this

Topic	Detail
	proposed expenditure but sought reassurance that it represented the best price for the work.[7] We have considered these comments as part of this business case. In particular, we considered and explored a large number of options to determine the most prudent and efficient way forward.

[7] Think Human, *Information Technology Deep Dive Workshop Report*, 28 June 2018, version 1.

2 Drivers

2.1 Introduction

IT infrastructure is the critical foundation for IT services that support business operations and enables the delivery of distribution services efficiently.

Business critical services provided by our IT infrastructure enable us to:

- distribute and regulate power across the network;
- meet all regulatory obligations and requirements (including those imposed by (amongst others) the Australian Energy Regulator (**AER**) and Australian Tax Office);
- monitor and analyse network performance in real time, and identify/correct network faults;
- maintain the network and supporting assets;
- provide a safe working environment for field staff;
- connect and disconnect customers;
- bill customers and retailers;
- manage and supervise staff and contractors;
- pay staff, contractors and suppliers;
- maintain backup systems, data storage;
- plan for and track our impact on the environment; and
- monitor and report on our Balanced Scorecard key performance indicators and achieve the objectives in our Corporate Plan.

Our IT Infrastructure consists of both:

- **Hosting Services** - those IT infrastructure services hosted in a data centre directly related to server-based computing, associated networking and data storage. Examples of Infrastructure refresh for hosting services include:
  - refresh and updates of server assets and IT network core assets; and
  - capacity upgrades for data storage.
- **Network Connectivity and Supporting Services** - those infrastructure components that provide network connectivity to hosting services, supporting management and platform capabilities on top of the hosting services, and support resiliency of our IT infrastructure. Examples of IT infrastructure refresh activities for these components include:
  - refresh of IT network assets located outside of data centres that provide connectivity from our offices and depots into our hosting services and the Internet; and
  - Platform Software upgrades and updates (eg patching server operating systems or upgrading database management software).

Refer to Appendix A - IT Service Stack Visualisation for a depiction of our IT Service Stack highlighting the components of our IT infrastructure in the context of our organisation.

During the 2010-15 regulatory control period (**RCP**), we explored options for reducing the complexity and cost of providing IT infrastructure services through executing our Data Centre Hosting Strategy[8]. This strategy has moved us away from owning our own data centres towards co-location services operating infrastructure we own, effectively a 'private cloud'. We currently maintain this ‘private cloud’ across two third-party data centres.

To meet customer and organisation needs for reliability and availability, our applications are deployed across both third-party data centres. Both sites are active and use data replication between them to support business continuity for critical services. The data centres are sized to ensure that if either fails, the

[8] Data Centre Hosting Strategy developed in 2014 and submitted as part of the regulatory proposal for the 2015-20 RCP.

other can deliver the critical services required by our organisation to service our customers at agreed service levels. This results in an investment in assets across both data centres to enable our Business Continuity Plan to be applied during an IT infrastructure outage. We have had several outages of this nature since implementing our current hosting solution and due to this industry standard design have been able to maintain service with minimal impact to our customers and the business. This has delivered a reliable hosting environment since the beginning of the 2015-20 RCP.

A failure or outage of IT infrastructure has a direct, and significant, impact on our ability to operate and maintain our electricity network. This will negatively affect our service levels and our ability to provide efficient distribution services to customers.

As an example, when a car drives into a pole and causes an outage on the electricity network, the business requires the use of 20 distinct IT services to ensure power is safely restored and associated business processes are efficiently managed. Each of these IT services is delivered on IT infrastructure that:

- hosts the application;
- provides connectivity from both office and field locations to the application;
- stores and manages the relevant data and information; and
- ensures all the above are provided securely, reliably and with an appropriate level of availability to minimise impacts to customers.

When IT infrastructure is not current and operational, we are unable to make appropriate use of these IT service leading to significant impacts to customers, and increased risk in managing and operating the electricity network. Refer to Appendix B – IT services used when car hits a pole for a visualisation of this scenario.

2.2 Issues and risks associated with not proceeding

The growing risks and issues we need to address relate, in the main, to our hosting strategy. Most assets that compromise our current hosting environment will be at the end of their useful life in the early years of the 2020-25 RCP. Retaining our current approach to managing our IT infrastructure service will require a significant increase in capex to ensure the reliability of these business-critical assets.

Maintaining physical data centres requires us to predict and provision **capacity** for peak demand to ensure we can meet customer and business needs. Increased digitisation results in ongoing capacity growth leading to a continued increase in the data centre footprint as more hardware is purchased to expand the private cloud to meet customer and business demand. This leads to a growing IT infrastructure footprint which requires ongoing refresh and additional support overheads. This approach to managing capacity requires significant capital-intensive projects to meet growth needs which introduces greater costs and risks for customers and the business. A key risk is the inability to be cost efficient in scaling to meet peak demand for IT services (eg our IT infrastructure was unable to support the peak demand experienced from our customers seeking information from our online outage reporting during the state-wide power outage in late September 2016). We can either over-invest upfront to meet demand forecasts or make more efficient investment decisions and carry the risk of being unable to meet peak load for IT services at critical times.

In recent times, the IT industry has explored new ways of managing hosting services using cloud computing. The Australian Government has also recognised the importance of exploring cloud options stating that[9]:

> *…agencies must now adopt cloud where it is fit for purpose, provides adequate protection of data and delivers value for money.*

[9] Australian Government, Department of Finance, *Australian Government Cloud Computing Policy: Smarter ICT Investment*, version 3.0, October 2014, page 4, available at, https://www.finance.gov.au/sites/default/files/australian-government-cloud-computing-policy-3.pdf.

This industry trend has led to many software applications provided by vendors moving to a SaaS model. Some applications used within our SAP suite will only be available via SaaS after their next product upgrade early in the 2020-25 RCP. For more details on cloud computing refer to Appendix C: What is Cloud Computing?

In addition to industry trends, we have a changing business environment. Some of the key changes we are experiencing that pose issues and risks to consider in the assessment of our hosting services are:

- Customers demand more real-time services and information related to electricity supply.
- We have an increasing need for data on our ageing assets to manage the security and reliability of electricity supply in a prudent and efficient manner.
- We have increased our staff mobility and need to ensure adequate support and performance for staff from where ever they do their work.
- The network of the future is driving increasing need for flexibility in the delivery of IT services.

Given the looming end-of-life replacement needs for our current hosting environment, IT industry trends and our changing business environment, we need to assess if data centres should remain as our primary method for providing prudent and efficient hosting services. Based on this need we commissioned a hosting strategy for the 2020-25 RCP with the objective to:

- identify the most efficient and prudent option for managing our hosting needs whilst managing operational risks and meeting demands of vendors who are moving to SaaS;
- meet growing server and storage capacity requirements; and
- address the need for our IT infrastructure to be able to efficiently and prudently scale up or down on demand, whilst remaining stable, such as in the lead up to and during major storm events and the subsequent return to normal operations.

The outcomes of the hosting strategy review are elaborated in Section 4.

Other than the risks of failure or performance degradation, there is no additional risk or issue in how we currently refresh the Network Connectivity and Supporting Services aspects of our IT infrastructure. We can address issues and risks with our hosting Services with negligible impact on Network Connectivity and Supporting Service refresh approach.

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

The primary risk is “*Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment”*, with the risk rating assessed as Extreme.

The results of the risk assessment of not proceeding with any planned activity in respect of the IT infrastructure (**the Do Nothing scenario**) are presented in Table 1: Risks of Not Proceeding.

Table 1: Risks of Not Proceeding

Risk ID	Risk Domain	Risk Description: ***Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:*** Consequence Description:	Likelihood	Consequences	Risk Rating
1	Reliability	• Business losing capability to manage electricity network resulting in increased number of outages, and duration of outages, for customers. • Increase in cyber security incidents resulting in malevolent people having access to our network control systems where they could impact network operations, and in non-compliance with regulatory obligations.	Almost Certain	Moderate	High
2	Financial	• Inability of our people to use IT systems to (examples and not inclusive): – connect and disconnect customers; – bill customers; – pay staff, contractors and suppliers; and – use efficient methods/systems for core business functions resulting in reductions to business productivity. • Higher IT opex to resolve failures / issues. • Security breaches (refer Reputation risk below) may lead to significant litigation costs.	Almost Certain	Moderate	High
3	Health & Safety	• Business unable to manage critical and life support customers could result in fatalities, regulatory and financial consequences, adverse reputational outcomes. • Inability to manage switching activities could result in fatalities, regulatory and financial consequences, adverse reputational damage.	Possible	Moderate	Medium
4	Reputation / Customer Service	• Visible and direct impact to customers utilising applications supported by our IT infrastructure resulting in a negative impact to reputation and increase in customer complaints (eg our registered electricians appointment booking application for connections). • Increase in cyber security incidents resulting in our organisation, and customers, private data being compromised. May also lead to malevolent people having access to our network control systems where they could impact network operations and non-compliance with regulatory obligations.	Almost Certain	Moderate	High
5	Regulatory	• Breaching security and privacy legislation and not meeting regulatory supply requirements and Australian Energy Market Operator (**AEMO**) obligations.	Almost Certain	Major	Extreme
6	Organisational	• Increase in frequency and duration of critical IT system outages as discussed above that will require the use of business continuity plans and specific management, for increasing periods of time, until services can be restored.	Almost Certain	Major	Extreme

Inherent Risk Summary	
The overall inherent risk rating for our IT Infrastructure without proactive maintenance:	Extreme

2.3 Detailed description of drivers

The key drivers for this business case are the following:

1. Maintain reliable IT services to enable efficient delivery of distribution services

With our heavy reliance on IT services, the need for reliable IT infrastructure to support the efficient delivery of distribution services has never been greater. When systems unexpectedly fail or suffer a performance impact, we lose access to critical capability for managing the network, productivity decreases, and our business efficiency drops rapidly impacting our ability to maintain our network and deliver services to customers.

Our organisation's responsiveness to our customers is critically dependent upon our IT infrastructure remaining operational, secure and fit for purpose. To remain responsive to customers, our staff mobility has significantly increased in the 2015-20 RCP. IT infrastructure provides the critical enabling connectivity and hosting-based services to enable our staff to work from wherever they perform their roles in the community. Our IT infrastructure also enables our customers to access online information and online applications (eg Outage Maps and Booking a Connection) whenever they need it.

2. Maintain IT infrastructure in an efficient manner while managing risk

We mitigate the IT services failure and outage risk through an annual investment program that has been designed to efficiently and prudently refresh our end-of-life IT infrastructure assets whilst mitigating various risks. This investment program has an internal governance group that forecasts expenditure needs using asset refresh cycles that are based on the risk and impact of failure of particular asset classes and types. Additional risk factors considered include, security patching, compatibility and migration paths for applications.

Our asset refresh cycles are generally in line with or exceed the Australian Tax Office (**ATO**) 'useful life' definitions and where support is available, we deem the risk acceptable. We also go beyond relevant vendor recommendations for replacement where possible. By way of example, server infrastructure has an asset life of four years according to the ATO. However, our typical forecast methodology for server replacements is from five to seven years and, as a general principle, we seek to maintain assets for as long as practicable and prudent, including by using extended support arrangements. In general, we seek to extend the life of assets while vendors are still offering security updates and support, but not beyond that time[10].

3. Manage cyber security risks

Managing risks associated with cyber security require our IT infrastructure to be kept current to support the latest updates and provide sufficient performance to meet application and operating system needs. Platform software updates and upgrades need to be maintained in-line with vendor recommendations and release cycles to minimise the likelihood of breaches.

Our regulatory obligations with respect to cyber security are increasing with the establishment of new government bodies such as the Critical Infrastructure Centre (**CIC**) and passing of the *Security of Critical Infrastructure Act 2018* (**SCI Act**). The CIC will provide increased scrutiny and oversight of critical infrastructure security including the electricity, gas, water and ports sectors. The CIC administers the SCI Act as well as new critical infrastructure system and data control obligations imposed by other regulatory bodies under the advice of the CIC such as the Foreign Investment Review Board (**FIRB**).

[10] The IT Asset Management Plan defines the framework for the management of IT assets aligned to the SA Power Networks Asset Management Policy.

4. Manage our response to Industry Driven Cloud Adoption

Over the last decade, cloud computing has become a more prevalent hosting alternative to the use of traditional data centres. Services, as opposed to owning assets, are steadily becoming the standard IT architectural approach for consuming IT capability. The availability of cloud services offers an opportunity for organisations to deliver services more efficiently, as well as providing services that are more responsive to customer and business needs. The use of new technologies is always a consideration as we seek to remain prudent and efficient in managing our network.

Increasingly, applications are being offered only in cloud hosting environments by vendors or models with on-premise deployments are beginning to attract higher costs. At the time of preparing this business case the following application services, that are utilised within our business from an on-premise implementation, will only be offered via SaaS from the early part of the 2020-25 RCP:

- SAP Mobile Platform (maintenance ends December 2020);
- SAP Enterprise Portal (maintenance ends December 2020); and
- SAP Gateway (maintenance ends December 2022).

These are known examples where the adoption of cloud services will not be an option.

As the use of cloud hosting in industry and vendor products increases, there will be a rising need to integrate with services that are only available in the cloud. Not preparing for the use of cloud hosting services will increase the risks of compatibility issues, IT environment complexity, and associated costs to maintain existing levels of service.

5. Maintain services whilst responding to change and peak demands

Our business environment is undergoing change whose impact requires consideration as we plan our IT infrastructure needs for the 2020-25 RCP. There is a need for increasing flexibility and scalability of services to efficiently meet peaks in demand for IT services and associated infrastructure.

These changes are detailed in our Future Operating Model[11] and Digital Strategy[12].

The list below summarises some of the key aspects from these strategies that are relevant to this business case:

- Customers are demanding more real time services and information related to their electricity supply.
- We have an increasing need for data on our ageing assets to manage the security and reliability of electricity supply in a prudent and efficient manner.
- We have increased our staff mobility to be more responsive to customer and business needs. In addition, our workforce is transitioning, and we need to retain, augment and share the skills and experiences of our knowledgeable workforce.
- Energy policy is evolving at a fast pace requiring increased customer energy data.
- We're one of the first DNSPs that will be moving to a distributed energy world where complex interactions will require smarter technology.
- Technology capabilities are accelerating producing new opportunities, but also pressures to keep up with the pace of change.

As outlined in the strategies, these changes will be addressed through the following:

[11] SA Power Networks – Future Operating Model 2016-2031

[12] Digital Strategy 2018-2025

- New capabilities to develop and deliver services which transform the way we work, what customers value, and create great experiences for customers.
- New support systems and better customer data to enable us to deliver new services efficiently and effectively.
- New partnerships and collaborations with manufacturers, suppliers, developers, local and state government and communities.
- A new cultural focus not just on delivering a great service as we supply electricity to our customers, but on delivering necessary technology foundations, seeing new opportunities and responding in a timely and agile way.

These changes, and our approach to addressing them, require that our IT infrastructure, as the foundation for the delivery of IT services, can handle increased volumes of data and has the flexibility to keep pace with the latest capabilities and manage increasingly integrated cloud environments.

In addition to the need for increasing **flexibility** in this changing environment, **scalability** of services to efficiently meet peaks in demand for IT services also becomes a critical need (eg during periods of high customer interactions like severe weather events). To maintain services to customers we must ensure the business has sufficient storage capacity, computing power and network capacity in the most appropriate hosting service solution. Too little capacity will result in poor response and low productivity, and impact services provided to our customers. Too much capacity can unnecessarily increase complexity, decrease manageability, and waste both time and money. Given many licensing fees are tied to server size, software licensing costs alone can bring significant savings when our IT infrastructure is sized appropriately.

From a customer perspective, the severe weather events experienced during the 2015-20 RCP, most notably the storm leading to the state-wide outage on 28 September 2016, led to a significant peak in use of our online outage reporting systems and maps. Figure 1: Online Outage Systems Sessions September 2016 below shows a peak of sessions on that day of greater than 300,000 compared to a typical average of less than 1000.

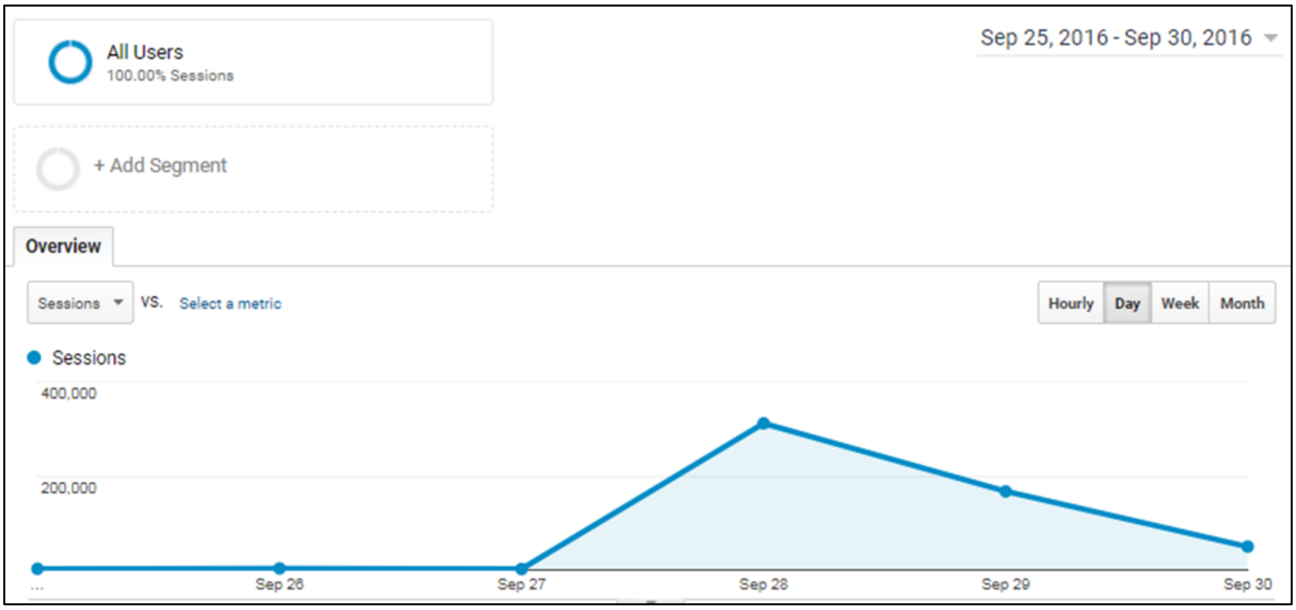


Figure 1: Online Outage Systems Sessions September 2016

This is a key example of the need for us to have the ability to scale and manage our capacity to meet significant fluctuations in customer demand. Whilst this level of demand is more likely to occur once a decade than once a year, we do see similar order of magnitude spikes in demand in the two to four annual storm events we experience every year. After the state-wide outage on 28 September 2016, we moved the hosting of this service to be cloud based where we can scale the environment quickly and efficiently to meet the needs of customers and reduce the need to over invest in capacity up front.

More holistically, our current hosting environment for all IT services requires upfront forecasting and investment in capacity. Through analysis of historic trends and assumptions on future use we predict required capacity needs and provision capacity we believe will be needed, upfront. To manage lead-times and minimise repeat labour effort we typically purchase and install this capacity once on an annual basis which can be months to a year in advance of when the capacity is required. This approach results in:

- potential over-investment upfront due to purchasing equipment to support capacity we may not use; and
- runs the risks of not having sufficient capacity to meet peaks and rapid changes in demand that can eventuate.

From the start of the 2015-20 RCP to end of December 2017, the organisation's need for backup and storage have increased significantly. These increases are driven by increased digitisation of information and our reliance on this information to manage the network (eg photos of network asset defects to improve work scoping). These increases directly translate to increased future expenditure forecasts.

Table 2 below details these increased backup and storage requirements.

Table 2: Jan 2015 - Backup and storage requirements as at Dec 2017

Infrastructure to Support Organisation Usage	Jan 2015	Dec 2017
Primary Storage	[redacted]	[redacted]
Backup Storage	[redacted]	[redacted]

Compute requirements (server-based memory usage) also increased by approximately [redacted] year on year during the same period. These growths need to be supported across both of our current third-party data centres. Evidence of our increasing capacity needs is in Section 5.2.4 Capacity increases.

Not exploring approaches that improve the flexibility and scalability of our IT Infrastructure in this environment of increasing change will increase the risk of being unable to maintain service to our customers in a responsive, prudent and efficient manner.

[13] Significant increases to backup requirements are driven by both volume of digitisation and ensuring data can be restored quickly when needed.

3 Scope

3.1 In-Scope

This business case covers all relevant expenditure to ensure our IT infrastructure environment is current and supportable. As our IT infrastructure comprises two types of services, options were considered separately for each:

- **Hosting Services** - those IT infrastructure services hosted in a data centre directly related to server-based computing, associated networking and data storage.
- **Network Connectivity and Supporting Services** - those infrastructure components that provide network connectivity to hosting services, supporting management and platform capabilities on top of the hosting services, and support resiliency of our IT infrastructure.

3.1.1 Hosting Services

Under our business as usual infrastructure program, this includes the equipment and labour costs for:

- Refresh and updates to Server assets
- Capacity upgrades for storage / backup / compute where not transitioned to IaaS
- Refresh and updates to the core/backbone IT network assets as part of our hosting solutions
- Capacity upgrades for IT network core.

Additionally, with the potential adoption of cloud technologies it includes:

- Capex for:
  - Project costs to transitioning any of data centre hosting to use cloud services
  - Project and capital costs for establishing and upgrading capacity for connectivity to cloud services.

- Opex step change for:
  - any hosting services that are transitioned to 'as a Service' hosting models eg IaaS; and
  - connectivity costs related to accessing cloud services.

3.1.2 Network Connectivity and Supporting Services Infrastructure

This program includes:

- Refresh, updates and capacity upgrades for IT network assets that provide connectivity into our hosting services, eg:
  - Non-core network assets in depots, offices, remote sites etc
  - Wi-Fi networks and wireless access points.
- Updates and Upgrades to Platform Software including:
  - Converged Infrastructure (Flexpod / NetApp) – pre-validated data centre platforms consisting of storage, compute and network components as one asset
  - Operating Systems
    - Windows – preparation / images only
    - Unix / Linux – preparation images only
  - Database Management Systems
    - Oracle
    - SQL Server
    - SAP HANA
  - Middleware & Services
    - MS Active Directory
    - Backup (CommVault)
    - Desktop as a Service (Citrix)
  - Client Operating System Management components (due to dependencies with supporting platform software)
    - Microsoft Windows Client

        - Device profile management (RES)
        - SCCM
    - Infrastructure Management components
        - Monitoring Tools for capacity and performance.
- IT Resiliency and Disaster Recovery capability
    - Identification of required corrective actions to maintain resiliency
    - Implementation of prioritised corrective actions.

3.2 Out of Scope

The following are explicitly out of scope of this business case:

- Opex relating to maintaining and supporting our infrastructure environments including:
    - Support costs for infrastructure assets
    - Licensing costs for Platform Software
    - Internal support costs
- Capex relating to specific upgrades of server operating systems from the in-scope preparation activities. These upgrades will be performed through application upgrade activities as covered by our IT Applications Business Case.
- Expenditure relating to the telecommunications network.
- IT infrastructure costs for enabling new business capability, such costs are covered within estimates for projects that deliver such capability.

4 Options assessment

4.1 Overview of options considered

The following are key factors in assessing options for this business case:

- We have a significant refresh of our assets in the data centres looming in the early part of the 2020-25 RCP due to most assets being commissioned in 2014. We will sweat the assets past their vendor recommended replacement dates, but they will still need replacement to manage our risk.
- The vendor and industry driven cloud adoption required consideration as some capabilities will only be offered in the cloud.
- We must maintain services in our dynamic and changing environment, specifically to support peak demand and rising capacity needs without over capitalising in advance of the demand materialising.
- We must be able to manage the continuously increasing risk profile of operating our IT infrastructure environment, including cyber security risks.
- The inherent risk of not refreshing our IT Infrastructure is Extreme (refer Section 2.2) and as such the 'Do Nothing' option has not been considered in detailed analysis.

These factors were the appropriate triggers for assessing alternatives to our business as usual (**BAU**) approach for refreshing our IT infrastructure.

We have structured our options analysis[14] for this business case as follows:

- Section 4.2 - Options assessment for Hosting Services: sets out a review of options for meeting the key factors above related to our IT infrastructure in third party data centres (ie hosted in the data centres)
- Section 4.3 **-** Options assessment for Network Connectivity and Supporting Services Infrastructure: sets out a review of options for maintaining and managing the risks of our infrastructure components not considered in the hosting services options.
- Section 4.4 **-** Summary of options assessment for IT Infrastructure Refresh**:** sets out a combined view of options for our Infrastructure Refresh, holistically including detailed options assessment and selection of our preferred option.

4.2 Options assessment for Hosting Services

4.2.1 Options considered

We moved some of our IT infrastructure into two third-party data centres in 2014. Most of these assets will reach their end-of-life early in the 2020-25 RCP.

We have explored how these hosting services can be provisioned. The options for our hosting services were developed in conjunction with an advisory consultancy, BDO Australia[15], who has expertise in cloud hosting. BDO worked closely with our internal subject matter experts in the development of our hosting options and associated financial modelling.

An extensive process was undertaken to consider appropriate hosting solutions. The various scenarios considered were put through preliminary assessments before three options were explored further with detailed cost modelling and analysis. This process is detailed in Appendix E: Hosting Strategy review.

The table below outlines the detailed options that were assessed.

[14] Our IT infrastructure comprises two types of services; Hosting Services and Network connectivity and Supporting Services, thus we conducted separate options assessments for each service.

[15] https://www.bdo.com.au/en-au/home

Table 3: Hosting options considered

Option	Description
Hosting Services Base Case	We have modelled a theoretical financial 'Base Case' for our hosting services against which each option can be compared to demonstrate any: • opex step change; and • foregone capex, for each of the options below. It is not a viable option we can implement as it does not meet the drivers detailed in this business case, but it is necessary to explain the financial differences between each option explored.
Hosting Option 1 – Business as Usual	This option acknowledges the need to adapt to changes in hosting needs but retains our two third-party data centres as the basis for our hosting service needs. This consists of continuing to refresh the assets associated with our hosting service as we do today, but transitioning to SaaS for any applications where the vendor will no longer provide an on-premise solution.
Hosting Option 2 – Measured Move to Cloud	This option takes a more proactive shift to adopting the use of cloud services to meet our drivers. It connects our private cloud hosting (our two third-party data centres) to external cloud hosting solutions to form a hybrid cloud. This implementation of a hybrid cloud requires a smaller scale up-front spend on infrastructure and will take a cloud first approach to hosting considerations.
Hosting Option 3 – Aggressive Move to Cloud	This option takes an aggressive approach to adopting cloud services for our hosting needs. It creates a hybrid cloud deployment based on a single data centre connected with external cloud services. Applications and services would be deployed across both private and public cloud with availability of applications balanced across the hybrid cloud.

The following sub-sections outlines high-level details for each option. Detailed assumptions and costs for each option are available in the cost models in Appendix F: Cost models.

4.2.2 Costs, benefits and risks of Hosting Services Base Case

For the purpose of evaluating our hosting service options in the context of the regulatory framework for opex, a theoretical base case scenario has been considered to enable comparison of the feasible options relative to the regulatory base year 2018/19. This is necessary to ensure that opex changes and substituted capex calculations reflect changes occurring subsequent to the 2018/19 base year and not just incremental changes commencing in 2020/21.

This scenario is identical to our business as usual approach (Option 1 below), however it incorporates a **theoretical** scenario whereby the SAP infrastructure platform software, identified as moving to SaaS in Option 1 after the regulatory base year 2018/19, continues to be provided as on-premise managed infrastructure platform software.

This option is ***not feasible***, as SAP are only going to provide these services via SaaS in the future and we must either move with them or undertake a costlier project to identify and replace the capability.

The costs for this option reflects the required capex were we to maintain our current approach to hosting services without change. That is:

- capex for refreshing our hosting infrastructure as we do today; plus
- capex for application upgrades/updates/patches for the infrastructure platform software moving to SaaS as if were we able to host them on-premise.

Costs

This theoretical option requires a theoretical total of **$21.191 million** in capex for the 2020-25 RCP.

Table 4: Hosting services base case cost for the 2020-25 RCP ($million, Dec $2017)

Cost Type	2020/21	2021/22	2022/23	2023/24	2024/25	Total 2020-25 RCP
Capex	0.661	14.930	2.048	1.776	1.776	**21.191**
Opex Step Change	0.000	0.000	0.000	0.000	0.000	**0.000**
TOTAL THEORECTICAL EXPENDITURE	**0.661**	**14.930**	**2.048**	**1.776**	**1.776**	**21.191**

Note: Totals may not exactly match the sums of individual costs due to rounding

There is no analysis on the risks and (dis)advantages of this option as it is not feasible.

4.2.3 Costs, benefits and risks of Hosting Option 1 – Business as Usual

Option 1 acknowledges the need to adapt to changes in hosting needs but maintains our current approach to managing operational risks by keeping infrastructure, that we own and manage, current and operational to enable the delivery of current services. It retains the existing private cloud hosting in our two third-party data centres as the basis for our hosting requirements. The caveat to this is to adopt SaaS where vendors move services to this model and do not provide an alternative. Capital costs associated with refreshing infrastructure apply the same prudent and efficient approach to sweating assets whilst maintaining risk and service delivery requirements.

Key aspects of this option are:

- Adopting cloud services only where required eg driven by vendor roadmap(s) where they are not providing alternatives
  - Three SAP applications will move to SaaS under this option:
    - SAP Mobile Platform
    - SAP Enterprise Portal
    - SAP Gateway
- Connectivity included to allow use of cloud only where required
- Continue with two third-party data centres
- Ongoing capital purchases for capacity growth
- In-line with our IT Asset Management Plan, refresh data centre based infrastructure (after sweating assets where possible) with like for like, continuing the organic approach of our hosting environment

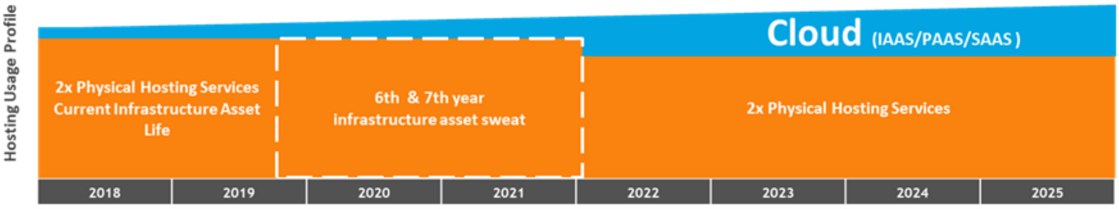

Hosting Usage Profile
Cloud (IAAS/PAAS/SAAS)
2x Physical Hosting Services Current Infrastructure Asset Life
6th & 7th year infrastructure asset sweat
2x Physical Hosting Services
2018
2019
2020
2021
2022
2023
2024
2025

Figure 2: Hosting Option 1, Business as Usual, Roadmap

Summary of roadmap activities:

- 2018 and 2019 – Continued data centre based approach with ongoing organic cloud growth

- 2018 and 2019 – Establish cloud governance model
- 2019 – Extension of compute infrastructure support warranties to 6th and 7th year (if possible)
- 2020 – Deployment of SAP SaaS services
- 2021 – Implementation of cloud connectivity and transition of selected applications
- 2021 – Purchase and implement replacement infrastructure
- 2022 to 2025 – Operation of hybrid cloud hosting platforms with a private cloud, data centre hardware, first approach.

Costs

This option requires **$20.631 million** in forecast capex for the 2020-25 RCP and forecast opex that reflects a **$1.277 million** step change compared to the 2018/19 base year.

Table 5: Hosting services: Option 1 Business as Usual cost ($million, Dec $2017)

Cost Type	2020/21	2021/22	2022/23	2023/24	2024/25	Total 2020-2025
Capex	0.621	14.800	1.918	1.646	1.646	**20.631**
Opex Step Change[16]	0.026	0.026	0.408	0.408	0.408	**1.277**
TOTAL COST[17]	**0.648**	**14.826**	**2.326**	**2.054**	**2.054**	**21.908**

Note: Totals may not exactly match the sums of individual costs due to rounding

NB: This opex step change is an inefficient capex to opex substitution of -**$0.717 million** (Dec $2017) when compared with the Base Case. Extrapolating out to include the 2025-30 RCP, this substitution becomes an inefficient capex to opex substitution of **-$2.107 million**.

Advantages / Benefits

- Minimal transition project effort and costs.
- Minimal increase to operating expenditure.
- Maintains the efficient delivery of energy services and manages the risks of IT infrastructure failure.

Disadvantages

- Need to purchase capacity ahead of time to meet customer and business needs with usage and non-usage of resources then needing to be managed.
- High capital investment in our IT infrastructure is not in line with the general industry shift by vendors towards providing SaaS resulting in us hosting a largely out of date platform at the end of the 2020-25 RCP
- High reliance on third-party data centres which may constrain future solution options.
- Will continue a focus for our IT staff on keeping our technology stack current instead of shifting the focus to driving value to the business through flexible and timely use of services.
- Does not align to Digital Strategy and the needs of our customers and business as detailed in our Future Operating Model as it does not provide agility and scalability of core IT services.

[16] Additional opex from cloud network connectivity and SaaS costs.

[17] Capex plus incremental increase in opex (compared to 2018/19 base year and adjusted for benefits from moving to SaaS).

Risks

Option 1 has been assessed against the Do Nothing scenario (presented in Section 2.2 - Issues and risks associated with not proceeding) to identify residual risk consequences.

Table 6: Hosting services: Option 1 Business as Usual risk analysis

Risk ID	Risk Domain	Risk Description		Likelihood	Consequences	Risk Rating
		Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:	**A hosting approach that continues to focus on a capital intensive refresh of on-premise hardware may lead to:**			
		Consequence Description				
1	Reliability	• Business losing capability to manage electricity network resulting in increased number of outages, and duration of outages, for customers. • Increase in cyber security incidents resulting in malevolent people having access to our network control systems where they could impact network operations and non-compliance with regulatory obligations.	• An inability to efficiently scale critical IT services to meet peak demands experienced during certain conditions (including avalanche) resulting in longer duration of outages for customers.	Possible	Moderate	Medium
2	Financial	• Inability of our people to use IT systems to (examples and not inclusive): – Connect / disconnect customers – Bill customers – Pay staff, contractors and suppliers – Use efficient methods/systems for core business functions resulting in reductions to business productivity • Higher IT opex to resolve failures / issues • Security breaches (refer Reputation risk below) may lead to significant litigation costs	• Inability to scale efficiently to meet peak loads resulting in higher upfront expenditure for capacity. • Inability to repurpose storage increases that will be required for significant application upgrades. • Increased integration complexity between a mostly on-premise environment and increasing volume of cloud services and third-party data sources resulting in increased project costs and increased support complexity/costs	Possible	Moderate	Medium

Risk ID	Risk Domain	Risk Description Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:	Risk Description A hosting approach that continues to focus on a capital intensive refresh of on-premise hardware may lead to:	Likelihood	Consequences	Risk Rating
		Consequence Description				
3	Health & Safety	• Business unable to manage critical and life support customers could result in fatalities, regulatory and financial consequences, adverse reputational outcomes. • Inability to manage switching activities could result in fatalities, regulatory and financial consequences, adverse reputational damage	• N/A	Rare	Moderate	Low
4	Reputation / Customer Service	• Visible and direct impact to customers utilising systems supported by our IT Infrastructure resulting in a negative impact to reputation and increase in customer complaints. • Increase in cyber security incidents resulting in our organisation, and customers, private data being compromised and non-compliance with regulatory obligations.	• An inability to efficiently scale critical IT services to meet peak demands for customer facing systems resulting in an inability to provide services to customers.	Likely	Minor	Medium
5	Regulatory	• Breach of security and privacy legislation and other regulatory obligations and requirements, including those imposed by regulators such as AEMO.	• Minimal impact to cyber security risks due to cloud providers certifying at a high level	Unlikely	Major	Medium

Risk ID	Risk Domain	Risk Description		Likelihood	Consequences	Risk Rating
		Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:	**A hosting approach that continues to focus on a capital intensive refresh of on-premise hardware may lead to:**			
		Consequence Description				
6	Organisational	• Increase in frequency and duration of critical IT system outages as discussed above that will require the use of business continuity plans and specific management, for increasing periods of time, until services can be restored.	• Inability to scale efficiently to meet peaks of infrastructure usage, such as a proof of concept for new technology, or application upgrade scenarios, resulting in increased complexity and effort to manage such scenarios • Increased integration complexity between a mostly on-premise environment and increasing volume of cloud services and third-party data sources resulting in increased support complexity.	Almost Certain	Minor	High

Residual Risk Summary	
The overall risk rating for this option is:	High

4.2.4 Costs, benefits and risks of Hosting Option 2 – Measured Move to Cloud

Option 2 reflects a smaller scale capital investment in IT infrastructure that we own and manage (compared to Option 1) and a more deliberate, but gradual, move to using infrastructure and systems owned by service providers but managed by us (referred to as IaaS). This option involves moving approximately thirty percent of non-critical applications, two of the critical applications and all SAP modules (other than those noted exceptions) to an IaaS model. Like Option 1, this option includes the transition of three SAP components to SaaS, but also transitions one critical application (Splunk) to SaaS. This implementation of a balanced hybrid cloud requires a smaller scale up-front spend on infrastructure and uses a cloud first approach to hosting.

Key aspects of this option are:

- Measured move to cloud and providing compatible platforms for both legacy and new applications.
- Reduce infrastructure footprint in two third-party data centres leading to a reduction in capex.
- Incremental capacity growth via cloud which also enables on–demand capacity to meet peak demands.
- Refresh reduced infrastructure footprint at the 2020-25 RCP.
- Cloud first approach for new and ongoing delivery of our IT hosting needs where prudent and efficient requiring an uplift in opex.

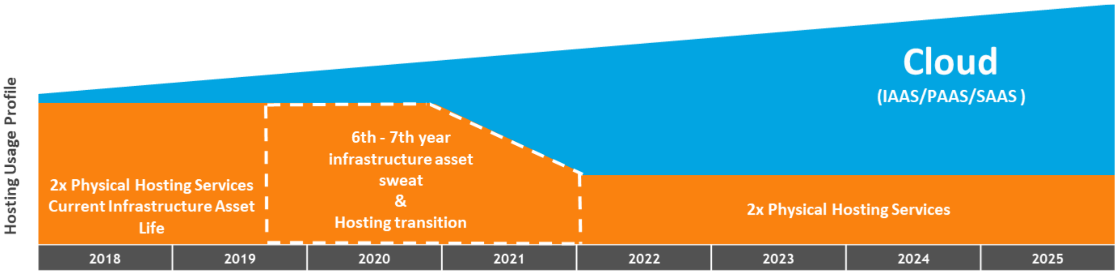

Hosting Usage Profile
Cloud
(IAAS/PAAS/SAAS)
2x Physical Hosting Services Current Infrastructure Asset Life
6th - 7th year infrastructure asset sweat & Hosting transition
2x Physical Hosting Services
2018
2019
2020
2021
2022
2023
2024
2025

Figure 3: Hosting Option 2, Measured Move to Cloud, Roadmap

Summary of roadmap activities:

- 2018 and 2019 – Continued data centre based approach with ongoing organic cloud growth
- 2018 ongoing – Establish cloud governance model
- 2019 – Extension of compute infrastructure support warranties to 6th and 7th year (if possible)
- 2020 – Deployment of SAP SaaS services
- 2020 – Selection/finalisation of cloud vendor(s)
- 2021 – Enhance cloud connectivity
- 2021 – Re–architect and transition applications aligned to any change in hosting platforms
- 2021 – Refresh and implement reduced infrastructure footprint for two third-party data centres
- 2022 to 2025 – Operation of hybrid cloud hosting platforms with a cloud first approach

Costs

This option requires **$13.464 million** in forecast capex for the 2020-25 RCP and forecast opex increase that reflects a **$6.860 million** step change compared to the 2018/19 base year.

Table 7: Hosting services: Option 2 Measured Move to Cloud cost ($million, Dec $2017)

Cost Type	2020/21	2021/22	2022/23	2023/24	2024/25	Total 2020-2025
Capex	2.668	8.878	0.820	0.549	0.549	**13.464**
Opex Step Change[18]	0.904	1.125	1.560	1.608	1.663	**6.860**
TOTAL COST[19]	**3.572**	**10.003**	**2.381**	**2.156**	**2.212**	**20.323**

Note: Totals may not exactly match the sums of individual costs due to rounding

[18] Additional opex from cloud network connectivity and SaaS / IaaS costs

[19] Capex plus incremental increase in opex (compared to 2018/19 base year and adjusted for benefits).

This option foregoes $7.727 million in capex compared with the Base Case. When compared to the opex step change this results in an efficient capex to opex substitution of **$0.867 million** when compared with the Base Case. Extrapolating out to include the 2025-30 RCP, this efficient capex to opex substitution becomes **$1.866 million.**

This option includes capex for transitioning services to the cloud in both the 2020-25 and 2025-30 RCPs. Once these transition costs are complete, the ongoing costs for hosting will become even more efficient.

Advantages / Benefits

- Maintains the efficient delivery of distribution services and manages the risks of IT infrastructure failure
- Efficient capex to opex substitution.
- Improved agility and adaptability to customer and business needs.
- Reduced risk of applications changing beyond the hosting platforms ability to support.
- Provision of agile and scalable hosting platforms as needs change, reduction in scale and effort of infrastructure projects when compared with Option 1.
- Allows incremental non-capital-intensive capacity growth, storage upgrade needs will reduce.
- Provide greater ability via on-demand capacity to manage peak demands aligned to business needs, such as during severe weather events.
- Does not over commit to cloud services, maintaining on-premise solutions for predictable demand and a preference for cloud services for exceptions and where cost-benefit analysis is compelling.
- Aligns to our Digital Strategy and the needs of our Future Operating Model by providing agility and scalability of core IT services.
- Avoids potential higher future cost for the inevitable transition of hosting services to the cloud.

Disadvantages

- Requires transition costs (included in cost estimates) and project risks to establish and migrate to cloud services.
- Ongoing opex increases.
- Increased reliance on cloud service providers who may financially fail or increase costs unfairly.
- Retains both private cloud hosting environments and associated costs and risks.

Risks

Option 2 has been assessed against the Do Nothing scenario (presented in Section 2.2 - Issues and risks associated with not proceeding) to identify residual risk consequences.

Table 8: Hosting services: Option 2 Measured Move to Cloud risk analysis

Risk ID	Risk Domain	Risk Description		Likelihood	Consequences	Risk Rating
		Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:	**A hosting approach that adopts a measured move to the cloud and retains 2 physical third-party data centres may lead to:**			
		Consequence Description				
1	Reliability	• Business losing capability to manage electricity network resulting in increased number of outages, and duration of outages, for customers. • Increase in cyber security incidents resulting in malevolent people having access to our network control systems where they could impact network operations and non-compliance with regulatory obligations.	• Increased exposure to service provider issues resulting in outages with critical applications.	Possible	Moderate	Medium
2	Financial	• Inability of our people to use IT systems to (examples and not inclusive): – Connect / disconnect customers – Bill customers – Pay staff, contractors and suppliers – Use efficient methods/systems for core business functions resulting in reductions to business productivity • Higher IT opex to resolve failures / issues. • Security breaches (refer Reputation risk below) may lead to significant litigation costs.	• Unexpected hidden costs in services moved to the cloud due to the complexity of the pricing options and models. • Unexpected impacts in training and skill requirements that increase IT support opex.	Likely	Minor	Medium

Risk ID	Risk Domain	Risk Description		Likelihood	Consequences	Risk Rating
		Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:	**A hosting approach that adopts a measured move to the cloud and retains 2 physical third-party data centres may lead to:**			
		Consequence Description				
3	Health & Safety	• Business unable to manage critical and life support customers could result in fatalities, regulatory and financial consequences, adverse reputational outcomes. • Inability to manage switching activities could result in fatalities, regulatory and financial consequences, adverse reputational damage	• N/A	Rare	Moderate	Low
4	Reputation / Customer Service	• Visible and direct impact to customers utilising systems supported by our IT Infrastructure resulting in a negative impact to reputation and increase in customer complaints. • Increase in cyber security incidents resulting in our organisation, and customers, private data being compromised.	• Increased exposure to service provider issues resulting in outages with customer facing applications.	Possible	Minor	Low
5	Regulatory	• Breach of security and privacy legislation and other regulatory obligations and requirements, including those imposed by regulators such as AEMO obligations.	• Minimal impact to cyber security risks due to cloud providers certifying at a high level.	Unlikely	Major	Medium
6	Organisational	• Increase in frequency and duration of critical IT system outages as discussed above that will require the use of business continuity plans and specific management, for increasing periods of time, until services can be restored.	• IT support teams impacted by learning curve of new skills in support services resulting in impact to IT services.	Likely	Minor	Medium

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

4.2.5 Costs, benefits and risks of Hosting Option 3– Aggressive Move to Cloud

Option 3 contemplates a hybrid cloud deployment based on a single data centre connected with external cloud services. Applications and services would be deployed across both private and public cloud with availability of applications balanced across the hybrid cloud. Compared to Option 2, a far higher proportion of IaaS in an accelerated timeframe. This option reflects a high level of maturity in cloud adoption and application compatibility with cloud (ie applications must be compatible with both private and public cloud hosting and must also be cloud aware to meet availability requirements).

Key aspects of this option are:

- Aggressive shift to cloud first with significant change to delivery of IT services
- Reduce to one data centre
- Leverage cloud on–demand for capacity growth
- Refresh reduced infrastructure footprint at next reset
- Cloud first approach for new and ongoing delivery of our IT hosting needs

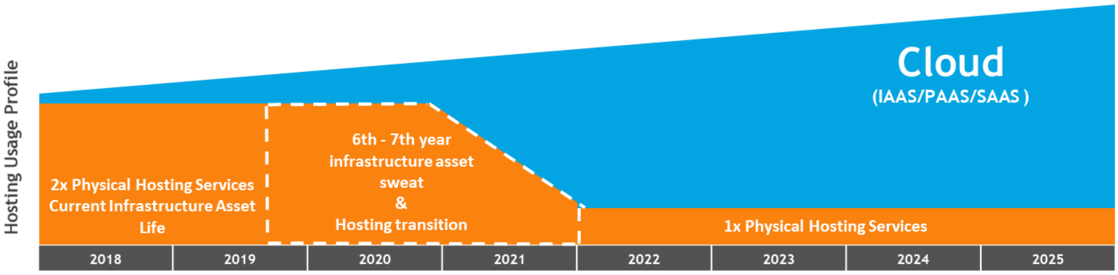

Hosting Usage Profile
Cloud
(IAAS/PAAS/SAAS)
2x Physical Hosting Services
Current Infrastructure Asset Life
6th - 7th year infrastructure asset sweat
&
Hosting transition
1x Physical Hosting Services
2018
2019
2020
2021
2022
2023
2024
2025

Figure 4: Hosting Option 3, Aggressive Move to Cloud, Roadmap

Summary of roadmap activities:

- 2018 and 2019 – Continued data centre based approach with ongoing organic cloud growth
- 2018 ongoing – Establish cloud governance model
- 2019 – Extension of compute infrastructure support warranties to 6th and 7th year (if possible)
- 2020 – Deployment of SAP SaaS services
- 2020 – Selection/finalisation of cloud vendor(s)
- 2021 – Enhance cloud connectivity
- 2021 – Re–architect and transition applications aligned to any change in hosting platforms
- 2021 – Refresh and implement reduced infrastructure footprint for single data centre
- 2022 to 2025 – Operation of hybrid cloud hosting platforms with a cloud first approach

Costs

This option requires **$13.990 million** in forecast capex for the 2020-25 RCP and forecast opex increase that reflects a **$11.053 million** step change compared to the 2018/19 base year.

Table 9: Hosting services: Option 3 Aggressive Move to Cloud cost ($million, Dec $2017)

Cost Type	2020/21	2021/22	2022/23	2023/24	2024/25	Total 2020-2025
Capex	6.126	7.511	0.353	0.000	0.000	**13.990**
Opex Step Change[20]	0.937	1.926	2.565	2.725	2.900	**11.053**
TOTAL COST[21]	**7.063**	**9.438**	**2.918**	**2.725**	**2.900**	**25.043**

Note: Totals may not exactly match the sums of individual costs due to rounding

[20] Additional opex from cloud network connectivity and SaaS / IaaS costs

[21] Capex plus incremental increase in opex (compared to reveal year 2018/19 and adjusted for benefits)

This option foregoes $7.201 million in capex compared with the Base Case. When compared to the opex step change this results in an inefficient capex to opex substitution of **-$3.852 million** when compared with the Base Case. Extrapolating out to include the 2025-30 RCP this becomes an inefficient capex to opex substitution of -**$6.609 million.**

The capex for this option is higher when compared to Option 2 due to increased transition costs for this option.

Advantages / Benefits

- Maintains the delivery of distribution services and manages the risks of IT infrastructure failure.
- Improved agility and adaptability to customer and business needs (greater than Option 1).
- Reduced risk of applications changing beyond the hosting platforms ability to support.
- Provision of agile and scalable hosting platforms as needs change, reduction in scale and effort of infrastructure projects when compared with Option 1.
- Allows incremental non-capital-intensive capacity growth, storage upgrade needs will reduce (reduced further than Option 1).
- Provide greater ability via on-demand capacity to manage peak demands aligned to customer and business needs, such as during severe weather events.
- Reduces our private cloud infrastructure footprint to a single data centre.
- Aligns to our Digital Strategy and the needs of our customers and business as set out in our Future Operating Model by providing agility and scalability of core IT services.

Disadvantages

- Inefficient capex to opex substitution of $3.852 million over the 2020-25 RCP.
- Requires significant transition costs (included in cost estimates, and higher than Option 1) and project risks to establish and migrate to cloud services, far higher than Option 1 and potentially undeliverable during the 2020-25 RCP without impacting other aspects of the IT program.
- Opex increases (more than Option 1).
- Increased reliance on cloud service providers who may financially fail or increase costs unfairly.
- IT resiliency will require far more complex application re-architecting to function between on-premise and cloud deployed applications.

Risks

Hosting Option 3 has been assessed against the Do Nothing scenario (presented in Section 2.2 - Issues and risks associated with not proceeding) to identify residual risk consequences.

Table 10: Hosting services: Option 3 Aggressive Move to Cloud Risk Analysis

Risk ID	Risk Domain	Risk Description		Likelihood	Consequences	Risk Rating
		Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:	**A hosting approach that adopts an aggresive move to the cloud and retains only 1 physical data centre may lead to:**			
		Consequence Description				
1	Reliability	• Business losing capability to manage electricity network resulting in increased number of outages, and duration of outages, for customers. • Increase in cyber security incidents resulting in malevolent people having access to our network control systems where they could impact network operations and non-compliance with regulatory obligations.	• Increased exposure to being impacted by other users of shared hosting services (eg recent O365 performance issues due to another tenant running a resource consuming script) resulting in impacts applications critical for managing the network.	Possible	Minimal	Low
2	Financial	• Inability of our people to use IT systems to (examples and not inclusive): – Connect / disconnect customers – Bill customers – Pay staff, contractors and suppliers – Use efficient methods/systems for core business functions resulting in reductions to business productivity. • Higher IT opex to resolve failures / issues. • Security breaches (refer Reputation risk below) may lead to significant litigation costs.	• Unexpected hidden costs in services moved to the cloud due to the complexity of the pricing options and models (higher likelihood than option 2). • Less exposure to issues related to asset life. • Increased exposure to being impacted by other users of shared hosting services (eg recent O365 performance issues due to another tenant running a resource consuming script) resulting to productivity impacts	Likely	Minor	Medium

Risk ID	Risk Domain	Risk Description		Likelihood	Consequences	Risk Rating
		Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:	**A hosting approach that adopts an aggresive move to the cloud and retains only 1 physical data centre may lead to:**			
		Consequence Description				
3	Health & Safety	• Business unable to manage critical and life support customers could result in fatalities, regulatory and financial consequences, adverse reputational outcomes. • Inability to manage switching activities could result in fatalities, regulatory and financial consequences, adverse reputational damage.	• N/A	Rare	Moderate	Low
4	Reputation / Customer Service	• Visible and direct impact to customers utilising systems supported by our IT infrastructure resulting in a negative impact to reputation and increase in customer complaints. • Increase in cyber security incidents resulting in our organisation, and customers, private data being compromised. May also lead to malevolent people having access to our network control systems where they could impact network operations and non-compliance with regulatory obligations.	• Increased exposure to service provider issues resulting in outages with customer facing applications.	Possible	Minor	Low
5	Regulatory	• Breach of security and privacy legislation and other regulatory obligations and requirements, including those imposed by regulators such as AEMO obligations.	• Minimal impact to cyber security risks due to cloud providers certifying at a high level.	Unlikely	Major	Medium

Risk ID	Risk Domain	Risk Description		Likelihood	Consequences	Risk Rating
		Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:	**A hosting approach that adopts an aggresive move to the cloud and retains only 1 physical data centre may lead to:**			
		Consequence Description				
6	Organisational	• Increase in frequency and duration of critical IT system outages as discussed above that will require the use of business continuity plans and specific management, for increasing periods of time, until services can be restored.	• Higher project risks for the transition effort due to volume of work to be complete; and the complexity of shifting some applications that may need significant re-architecting to work in the cloud. • Increased impacts to IT Operating Model (**IToM**) and teams due to volume and increased pace of change.	Almost Certain	Moderate	High

Residual Risk Summary	
The overall risk rating for Hosting option 3 is:	High

4.3 Options assessment for Network Connectivity and Supporting Services Infrastructure

4.3.1 Options considered

The options for the Network Connectivity and Supporting Service components of our IT infrastructure[22] are aligned to our IT Asset Management Plan and have considered the following key factors:

- asset classes and their useful lives;
- capabilities required to support the efficient delivery of distribution services;
- vendor costs for equipment and services; and
- labour assumptions based on historic project actuals and considerations for future servicing strategies of vendors.

The table below outlines the options assessed.

Table 11: Network Connectivity and Support Services Options Considered

Option	Description
Option 1 – Industry Standard Refresh	Based on industry and vendor recommendations, proactive plans asset replacements or upgrades before they become unusable based on useful life recommendations from the industry and vendors.
Option 2 – Business as Usual (BAU)	Represents our current approach to replacing and/or upgrading our IT infrastructure assets – an ongoing, rolling program that proactively keeps our infrastructure components current and operational. Plans asset refresh based on useful life typically longer than industry and vendor recommendations based on our own experience with balancing cost and risk within our environment.

The following sub-sections outline high-level details for each option. Detailed assumptions, costs and risks for each option are available in the cost models in Appendix F: Cost models**.**

4.3.2 Costs, benefits and risks Network Connectivity and Supporting Services Option 1 – Industry Standard Refresh

Option 1 uses refresh cycles and approaches based on industry and vendor recommended refresh cycles. This option focuses on prioritising the mitigation of risk by keeping our environment as current as possible. Refresh lifecycles are based on ATO definitions of useful life for hardware assets and vendor recommendations and frequency of updates/upgrades for platform software. This applies an IT resiliency approach driven by ensuring all critical services are assessed and enhanced at least once every two years.

Table 12: Option 1 – industry standard refresh activities below summarises key aspects of this option by IT infrastructure component:

[22] Refer to Section 3.1.2 for examples of network connectivity and supporting services assets.

Table 12: Option 1 – industry standard refresh activities

Infrastructure Component	Description
Network Connectivity	Refresh the following on a 5-year lifecycle: • Routers, switches, cloud-bridges in depots/offices Wi-Fi devices and wireless access points
Platform Software	The following refresh activities for our platform software: • Annual firmware upgrades • Windows Server O/S Upgrades every 3 years • Unix / Linux Upgrade every 3 years • Patching of all platform software when provided by vendors • Upgrading Oracle client/server in-line with vendor release cycles • Upgrading SQL Server in-line with vendor release cycles • Upgrading SAP HANA in-line with vendor release cycles • Commvault (backup software) updates annually • Updating Active Directory every 4 years • Updating/Upgrading CITRIX every 6 months • Packaging and testing updates to Windows O/S (and related management and productivity applications) every 6 months in-line with Microsoft's new windows servicing strategy.
IT Resiliency	The following activities to review and update our IT resiliency assets: • 1 large failover • Review and enhancements for 12 critical services each year • Review and enhancements for all SAP Resiliency measures at least once every two years

Costs

This option requires **$21.358 million** in forecast capex for the 2020-25 RCP.

Table 13: Option 1 – Industry standard refresh cost ($million, Dec $2017)

Cost Type	2020/21	2021/22	2022/23	2023/24	2024/25	Total 2020-2025
Capex	4.973	4.838	4.144	3.805	3.598	**21.358**
Opex Step Change	0.000	0.000	0.000	0.000	0.000	**0.000**
TOTAL COST	**4.973**	**4.838**	**4.144**	**3.805**	**3.598**	**21.358**

Note: Totals may not exactly match the sums of individual costs due to rounding

NB: Costs differences for this option are best considered over the 10-year period from 2020 to 2030. For example, refresh of network assets on a five vs a seven-year cycle still applies to the 2020-25 RCP once under both this option, and Option 1.

Advantages / Benefits

- Customers not exposed to significant ongoing impacts.
- Maintains the delivery of distribution services and manages the risks of Infrastructure failure.
- Reduces risk related to IT infrastructure failure, or under performance, across all domains to a 'Low' or 'Medium' level of risk.

Disadvantages

- Significant capex required, especially over the longer term (ie $42.67 million over the 2020-30 period)

Risks

Option 1 has been assessed against the Do Nothing scenario (presented in Section 2.2 - Issues and risks associated with not proceeding) to identify residual risk consequences.

Table 14: Option 1 – Industry standard refresh risk analysis

Risk ID	Risk Domain	**Risk Description:** **Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:** **Consequence Description:**	Likelihood	Consequences	Risk Rating
1	Reliability	• Business losing capability to manage electricity network resulting in increased number of outages, and duration of outages, for customers. • Increase in cyber security incidents resulting in malevolent people having access to our network control systems where they could impact network operations and non-compliance with regulatory obligations.	Possible	Moderate	Medium
2	Financial	• Inability of our people to use IT systems to (amongst other things): ○ Connect / disconnect customers ○ Bill customers ○ Pay staff, contractors and suppliers ○ Use efficient methods/systems for core business functions resulting in reductions to business productivity. • Higher IT opex to resolve failures / issues. • Security breaches (refer Reputation risk below) may lead to significant litigation costs.	Possible	Moderate	Medium
3	Health & Safety	• Business unable to manage critical and life support customers could result in fatalities, regulatory and financial consequences, adverse reputational outcomes. • Inability to manage switching activities could result in fatalities, regulatory and financial consequences, adverse reputational damage.	Rare	Moderate	Low

Risk ID	Risk Domain	**Risk Description:** **Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:** **Consequence Description:**	**Likelihood**	**Consequences**	**Risk Rating**
4	Reputation / Customer Service	• Visible and direct impact to customers utilising systems supported by our IT infrastructure resulting in a negative impact to reputation and increase in customer complaints. • Increase in cyber security incidents resulting in our organisation, and customers, private data being compromised.	Possible	Minor	Low
5	Regulatory	• Breach of security and privacy legislation and other regulatory obligations and requirements, including those imposed by regulators such as AEMO.	Unlikely	Major	Medium
6	Organisational	• Increase in frequency and duration of critical IT system outages as discussed above that will require the use of business continuity plans and specific management, for increasing periods of time, until services can be restored.	Possible	Minor	Low

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

4.3.3 Costs, benefits and risks of Network Connectivity and Supporting Services Option 2 – Business as Usual

Option 2 maintains our current approach to refreshing our Network Connectivity and Support Service Infrastructure using refresh cycles and approaches based on our experience in managing our environment. This option seeks the most prudent and efficient approach by sweating assets and delaying upgrades / updates to an acceptable level of risk and management to reduce cost. Refresh lifecycles are based on our IT Asset Management Plan taking into consideration vendor recommendations but using our experiences and risk profiles to ensure we remain prudent and efficient with our asset replacements.

Table 15: Option 2 - Business as usual refresh activities below summarises key aspects of this option by Infrastructure component:

Table 15: Option 2 - Business as usual refresh activities

Infrastructure Component	Description
Network Connectivity	Refresh the following on a 7-year lifecycle: • Routers, switches, cloud-bridges in depots/offices Refresh the following on a 5-year lifecycle: • Wi-Fi devices and wireless access points
Platform Software	Following refresh activities for our platform software: • Flexpod/Netapp/Vmware/ESX annual firmware upgrades • Windows Server O/S updates twice yearly by adopting new windows servicing strategy • Unix / Linux Upgrade every 6 months to a year • Patching of all platform software, sweating timeframes where possible • Upgrading Oracle client/server on alternate years • Upgrading a third of SQL Server databases each year • Upgrading SAP HANA in-line with vendor release cycles • Commvault (backup software) updates annually • Explore and upgrade work for moving to AzureAD (over updating AD in-line with vendor release cycles) • Updating/Upgrading CITRIX every 6 months • Packaging and testing updates to Windows O/S (and related management and productivity applications) every 6 months in-line with Microsoft's new windows servicing strategy
IT Resiliency	The following activities to review and update our IT resiliency assets: • 1 large failover per year • Review and enhancements for 3 critical services each year • Review and enhancements for all SAP Resiliency measures at least once every three years

Costs

This option requires **$15.004 million** in forecast capex for the 2020-25 RCP.

Table 16: Option 2 - Business as usual refresh costs ($million, Dec $2017)

Cost Type	2020/21	2021/22	2022/23	2023/24	2024/25	Total 2020-2025
Capex	2.511	2.493	3.333	3.469	3.197	**15.004**
Opex Step Change	0.000	0.000	0.000	0.000	0.000	**0.000**
TOTAL COST	**2.511**	**2.493**	**3.333**	**3.469**	**3.197**	**15.004**

Note: Totals may not exactly match the sums of individual costs due to rounding

Advantages / Benefits

- Customers not exposed to significant ongoing impacts.
- Maintains the efficient delivery of energy services and manages the risks of IT infrastructure failure.
- Risks related to IT Infrastructure reduced to acceptable levels.
- Reasonable level of expenditure based on historical spend.

Disadvantages

- Does not maximise risk mitigation on likelihoods of IT infrastructure failure and recoverability.

Risks

Option 2 has been assessed against the Do Nothing scenario (presented in Section 2.2 - Issues and risks associated with not proceeding) to identify residual risk consequences.

Table 17: Option 2 - Business as usual refresh risk analysis

Risk ID	Risk Domain	**Risk Description:** **Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:** **Consequence Description:**	Likelihood	Consequences	Risk Rating
1	Reliability	• Business losing capability to manage electricity network resulting in increased number of outages, and duration of outages, for customers. • Increase in cyber security incidents resulting in malevolent people having access to our network control systems where they could impact network operations and non-compliance with regulatory obligations.	Possible	Minor	Low
2	Financial	• Inability of our people to use IT systems to (amongst other things): ○ Connect / disconnect customers ○ Bill customers ○ Pay staff, contractors and suppliers ○ Use efficient methods/systems for core business functions resulting in reductions to business productivity • Higher IT opex to resolve failures / issues. • Security breaches (refer Reputation risk below) may lead to significant litigation costs.	Possible	Moderate	Medium
3	Health & Safety	• Business unable to manage critical and life support customers could result in fatalities, regulatory and financial consequences, adverse reputational outcomes. • Inability to manage switching activities could result in fatalities, regulatory and financial consequences, adverse reputational damage.	Rare	Moderate	Low

Risk ID	Risk Domain	**Risk Description:** **Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:** **Consequence Description:**	Likelihood	Consequences	Risk Rating
4	Reputation / Customer Service	- Visible and direct impact to customers utilising systems supported by our IT infrastructure resulting in a negative impact to reputation and increase in customer complaints. - Increase in cyber security incidents resulting in our organisation, and customers, private data being compromised and non-compliance with regulatory obligations.	Likely	Minor	Medium
5	Regulatory	- Breach of security and privacy legislation and other regulatory obligations and requirements, including those imposed by other regulators such as AEMO.	Unlikely	Major	Medium
6	Organisational	- Increase in frequency and duration of critical IT system outages as discussed above that will require the use of business continuity plans and specific management, for increasing periods of time, until services can be restored.	Likely	Minor	Medium

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

4.4 Summary of options assessment for IT Infrastructure Refresh

4.4.1 Options considered

As outlined in section 4.1 - Overview of options , the analysis of options for our Infrastructure refresh considered distinct options for both Hosting Services and Network Connectivity and Supporting Services Infrastructure.

This section brings together the options from the distinct analysis to summarise and select a holistic option for ensuring our IT infrastructure services are kept current and within support.

Given it requires significantly more expenditure to adopt an Industry Standard approach, with no significant impact to risk levels, for Network Connectivity and Supporting Services, we have selected the BAU option as the preferred option.

Thus, our holistic IT Infrastructure Refresh options combine the Network Connectivity and Supporting Services BAU option with the three Hosting Services options.

Each Hosting Service option explored represents an implementation of a hybrid cloud to varying degrees. Holistic benefits of hybrid cloud hosting approaches that are relevant across the options are:

- improved agility and adaptability to meet changing business needs with scalable hosting platforms;
- reduced risk of applications changing beyond the hosting platforms ability to support;
- prudent and efficient hosting costs through incremental, non-capital intensive, capacity growth; and
- greater ability to manage peak demands aligned to customer and business needs.

Table 18: IT Infrastructure refresh summary options and costs ($million, Dec $2017)

Option	Description	Cost Summary (2020-25 RCP)	
IT Infrastructure Refresh **Option 1 – Business As Usual**	A holistic business as usual approach for refreshing our Infrastructure combining sections: **4.2.3 - Costs, benefits and risks of Hosting Option 1 – Business as Usual** and **4.3.3 - Costs, benefits and risks of** Network **Connectivity and Supporting Services Option 2 –** Business **as Usual**		
		Capex	35.634
		Opex Step Change	1.277
		Total Costs[23]	**36.911**
IT Infrastructure Refresh **Option 2 – Measured Move to Cloud**	Extends our business as usual approach for refreshing our IT infrastructure to an approach that moves aspects of our hosting services to the cloud under SaaS and IaaS. Combines sections: **4.2.4 - Costs, benefits and risks of Hosting Option 2 – Measured Move to Cloud** and **4.3.3 - Costs, benefits and risks of Network Connectivity and Supporting Services Option 2 – Business as Usual**		
		Capex	28.467
		Opex Step Change	6.860
		Total Costs[23]	**35.327**

[23] Capex plus incremental increase in opex (compared to reveal year 2018/19 and adjusted for benefits).

Option	Description	Cost Summary (2020-25 RCP)	
IT Infrastructure Refresh **Option 3 – Aggressive Move to Cloud**	Similar to Option 2 but with a larger scope and more rapid transition to using the cloud for our hosting services to support decommissioning the use of one of our two existing third-party data centres. Combines sections: **4.2.5 - Costs, benefits and risks of Hosting Option** 3**– Aggressive Move to Cloud** and **4.3.3 - Costs, benefits and risks of Network Connectivity and Supporting Services Option 2 – Business as Usual**		
		Capex	28.994
		Opex Step Change	11.053
		Total[23]	**40.047**

A breakdown of capex and opex step changes and capex to opex substitutions compared to the theoretical base case, by option, is provided in Table 19.

Table 19: Opex step changes and capex to opex substitutions by option over the 5-year and 10-year cash flow periods

IT Infrastructure Refresh Options	2020-25 RCP				10-year period, 2020-2030[24]			
	Capex[25]	Opex step change [26]	Totex[27]	Capex/ opex trade-off[28]	Capex	Opex step change	Totex	Capex/ opex trade-off
Base Case[29]	36,194	-	-	-	71,081	-	71,081	-
Option 1: Business as Usual	35,634	1,277	36,911	**(717)**	69,871	3,317	73,188	**(2,107)**
Option 2: Measured Move to Cloud	28,467	6,860	35,327	**867**	51,145	18,070	69,215	**1,866**
Option 3 - Aggressive Move to Cloud	28,994	11,053	40,047	**(3,852)**	49,231	28,458	77,690	**(6,609)**

An option by option analysis is not included here given the previous sections 4.2 and 4.3 provide detailed options assessments.

[24] Combines the "theoretical base case" for Hosting Services with the base case for the Network Connectivity and Supporting Services Option 2 – Business as Usual.

[25] Represents the total capex associated with the proposed option over the cash flow period 1 July 2020 to 30 June 2025.

[26] Represents the total opex step change (new opex minus opex benefits) associated with the proposed option over the cash flow period 1 July 2020 to 30 June 2025.

[27] Represents the total cash flow, capex plus opex step change opex, over the period from 1 July 2020 to 30 June 2025.

[28] The efficiency of the capex to opex substitution expressed as totex (total capex 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 (ie +'ve is efficient).

[29] The period from 1 July 2020 to 30 June 2030.

4.4.2 Summary benefits and risks of each option

The overall cost, benefit and risk assessment for our holistic Infrastructure options is summarised in **Table 20: Overall advantages, benefits, disadvantages and risks of the options considered** below.

Table 20: Overall advantages, benefits, disadvantages and risks of the options considered for IT Infrastructure Refresh

Option	Advantages / Benefits	Disadvantages / Risks	Overall risk rating
IT Infrastructure Refresh Option 1: Business as Usual	Customers not exposed to significant ongoing impacts. Maintains efficient delivery of distribution services and manages the risks of IT infrastructure failure. Minimal transition project effort and cost to shift services to the cloud.	Inefficient capex to opex substitution. IT infrastructure may still fail, but the likelihoods and consequence are reduced through refresh of end of life equipment. Retains current issues with lack of flexibility / scalability. Capacity planning still based on upfront planning and capex. Does not align to our Digital Strategy and needs of customers and the business as set out in the Future Operating Model which leads to a high level of risk across Financial and Organisational domains due to a largely out of date hosting platform at the end of the 2020-25 RCP driving increasing support complexity and project costs.	High
IT Infrastructure Refresh Option 2: Measured Move to Cloud	Customers not exposed to significant ongoing impacts. Maintains efficient delivery of distribution services and manages the risks of IT infrastructure failure. Efficient capex to opex substitution. Lowest overall NPV and cost over two reset periods (2020-2030). Greater flexibility, agility and scalability which will allow us to more efficiently and prudently meet the demands of our customer and operate and maintain our network.	Retains a footprint in the two existing third-party data centres. Transition project and uplift in opex required.	Medium

Option	Advantages / Benefits	Disadvantages / Risks	Overall risk rating
	Align to our Digital Strategy and needs of customers and the business as set out in our Future Operating Model.		
IT Infrastructure Refresh Option 3: Aggressive Move to Cloud	Similar to Option 2 but with a higher level of flexibility, agility and scalability. Reduces our private cloud infrastructure footprint to a single data centre.	Inefficient capex to opex substitution. Requires significant transition project effort / cost and risks. Opex increases (more than Option 1). Complexity of application support and IT resiliency becomes significantly more complex with the loss of one data centre as applications need to operate seamlessly between on-premise and cloud models.	High

4.4.3 Options assessment

A summary of the costs and benefits associated with the holistic IT Infrastructure Refresh options is set out in Table 21.

Section 4.4.4 provides the commentary and the discussion of the selected option, Option 2.

A summary of risk assessments for all options is provided in Appendix G.

Table 21: IT infrastructure refresh cost-benefit analysis over the 10-year period from 1 July 2020 to 30 June 2030, $000's, Dec $2017

Option	10-year analysis				2020-25 RCP totex[30]	Overall Risk Rating	Ranking
	Total capex	Total opex step change[31]	Totex[32]	NPV[33]			
Option 1: Business as Usual	69,871	3,317	73,188	(63,851)	36,911	High	2
Option 2: Measured Move to Cloud	51,145	18,070	69,215	(60,457)	35,327	Medium	1
Option 3: Aggressive Move to Cloud	49,231	28,458	77,690	(68,027)	40,047	High	3

We note that:

- All option costs were supported by detailed cost models and key assumptions, based on industry-standard estimation methods.
- Cost estimates were based on both current analysis and historical costs of similar projects.
- External estimates were sought for all vendor-related costs, especially costs related to cloud hosting which included assessing costs from multiple cloud hosting vendors.
- The costs have been validated with IT operational management and IT infrastructure subject matter experts for reasonableness and completeness.

4.4.4 Option selected

Option 2 – Measured Move to Cloud, has been selected as our holistic IT Infrastructure Refresh option because:

- a Do Nothing option is not prudent as it would increase risk of failure of distribution services to customers and the business to Extreme levels;
- it has the most efficient cost for achieving the expenditure objectives (including the lowest cost and lowest NPV);
- it enables the drivers identified in Section 2 to be addressed;

[30] Represents the total expenditure, capex plus new opex minus opex benefits, required within the 2020-25 RCP.

[31] Represents the total opex step change (new opex minus opex benefits) associated with the proposed option over the cash flow period 1 July 2020 to 30 June 2030.

[32] Represents the total cash flow, capex plus opex step change, over the period from 1 July 2020 to 30 June 2030.

[33] NPV of the proposed expenditure over the period from 1 July 2020 to 30 June 2030, based on discount rate of 2.89%.

- it maintains efficient delivery of distributions services and manages the risks of IT infrastructure failure;
- it prudently allows SA Power Networks to maintain its current risk profile rather than see it increase by continuing to rely on IT infrastructure assets that are not supported and past the end of their useful life;
- in contrast to Option 1:
  - provides a flexible and scalable Hosting Service to respond to business changes and vendor/industry driven cloud adoption;
  - reduces the scale and effort of future IT infrastructure refresh projects;
  - aligns to our Digital Strategy 2018-2025 and the aims of the Future Operating Model; and
  - minimises organisational and financial risks associated with delaying cloud adoption; and
- in contrast to Option 3:
  - avoids a high level of project risk due to the increased scope of transition; and
  - avoids organisational risks associated with maintaining IT resiliency between applications hosted on-premise with high availability provided from the cloud.

A more detailed description of the selected option is set out in Section 7.

5 Supporting evidence

5.1 IT Infrastructure recurrent expenditure in previous RCPs

Given its foundational nature for the operation of the business and provision of distribution services to our customers, recurrent expenditure on IT infrastructure has been accepted in the past by the AER.

Our total actual/estimated expenditure for our recurrent IT Infrastructure Refresh program in the 2015-20 RCP is **$38.230 million**. This is an increase of $1.5 million on the 2015-2020 allowance for IT Infrastructure, reflecting the increased demand for reliable IT services from customers and across the business.

Our selected option for the 2020-25 RCP is forecasting capex plus a step change in opex that combined will total **$35.327 million**. This represents an 8% reduction in expenditure compared with our 2015-20 RCP actual/estimated expenditure.

5.2 IT infrastructure asset lifecycles

The lifecycles for IT infrastructure assets used to forecast costs in this business case are based on our IT Asset Management Plan[34] which is a framework for ensuring IT assets are prudently managed throughout the entire asset lifecycle. These lifecycles are typically based upon vendor and industry recommendations, with our own experience informing risk in our environment to sweat assets where possible past the 'standard' definition of their useful life to ensure efficiency and prudency. Our objective is to find the right balance of cost and risk to meet business service levels.

A summary of our refresh approach for the IT infrastructure assets is as follows:

Table 22: Asset lifecycle standards for selected assets

Infrastructure Component	Description	Asset Class - Refresh Cycle
Data Centre / Hosting Services	IT infrastructure assets that provide the server-based processing and storage for the organisation, including supporting IT network connectivity to and within the data centre environments. We currently maintain IT infrastructure in two third-party data centres to meet high availability requirements and support business continuity.	Storage / Backup capacity – upgraded annually based on forecast needs. Server based infrastructure – small updates annually based on business need; large scale refresh every 5 to 7 years (sweat assets if risk manageable). Data Centre based Core IT Network equipment (eg load balancers – small updates annually based on business need, large scale refresh every 5-7 years).
Network Connectivity	IT network assets based outside the core third-party data centres to support the entire business with optimised connectivity to hosting services. Without	Switches / Router – typically refreshed every 5-7 years in line with vendor support agreements.

[34] SAPN, IT Asset Management Plan 2019-2023

	these assets we would otherwise need to pay for a carrier service (eg NBN).	Wi-Fi assets – refreshed every five years given uplift in wi-fi usage.
Platform Software	Updates and upgrades to platform software – software processes and services which can be built upon to provide business applications and services. This includes operating systems, databases, middleware technology and centralised management and monitoring, such as: • Windows Server • Linux • VMware • CITRIX Avanti • Active Directory • CommVault • Oracle • SQL Server	Patches / Updates – annually as needed to maintain security and performance. Major upgrades – planned as significant projects based on vendor release cycles, support arrangements and appropriate business case justifications.
IT Resiliency Program	Program of work that identifies and implements updates to IT infrastructure to minimise frequency and duration of IT outages.	Annual investment to keep resiliency and disaster recovery capability tuned to support business continuity needs. Full failover (test to our backups) every year, with 3 critical services assessed and enhanced.

5.2.1 Ongoing journey for prudent and efficient IT infrastructure services

Given the recurrent cost associated with our IT infrastructure service, we continually review and investigate options to ensure we are as efficient as possible whilst maintaining reliability and availability.

A high-level view of this journey is:

- Pre-2015 – owning and running our IT infrastructure assets.
- 2015 to current – utilising private cloud through the use of two third-party data centres (in which we continued to own the IT assets).
- Current – exploring the use of cloud hosting services as opposed to owning our own IT infrastructure hosting assets.

Vendor roadmaps and the prevalence of cloud hosting are driving significant change and reducing the relevance of maintaining 'private cloud' and on-premise hosting solutions. Cloud hosting solutions offer the opportunity for increasing efficiencies, flexibility, reliability whilst reducing costs that we cannot ignore given the size of our IT infrastructure footprint.

5.2.2 Gartner predictions on data centres

By 2025, 80% of enterprises will have shut down their traditional data centre, versus 10% today.[35]

This prediction is based on Gartner[36] analyst's views of IT services needing to be more agile in meeting needs of business and delivering services closer to customers. The article highlights the radical changes in the IT industry impacting how services are delivered and indicates data centre use for hosting services will be relegated to legacy needs.

Industry commentary on this prediction speculates that this shift may occur even faster[37] than the end of the 2020-25 RCP.

The trends indicated within the article, and industry commentary on the article, are in-line with our hosting strategy review and desired outcomes.

5.2.3 Independent input into our Hosting Strategy

As mentioned earlier in this business case, to ensure an objective and independent review of cloud hosting, we engaged with BDO Australia to prepare our Hosting Strategy and perform a detailed cost benefit analysis of the use of cloud hosting. Our internal subject matter experts provided BDO Australia with data and costs on our current environment. After this analysis, we further validated our assumptions and costs for the cloud hosting options with different service providers and SAP. Appendix E: Hosting Strategy review summarises the relevant details of the hosting strategy and includes attachments with details from the review.

5.2.4 Capacity increases

The graphs below demonstrate our increasing growth in capacity needs in the 2015-20 RCP.

[redacted]

Figure 5: Prime Storage Growth across both data centres

[35] Dave Cappuccio, Gartner, *The Data Center is Dead*, 26 July 2018, <https://blogs.gartner.com/david_cappuccio/2018/07/26/the-data-center-is-dead/>.

[36] Gartner are the world's leading IT research and advisory company with over 40 years of experience.

[37] Matt Asay, TechRepublic, *Gartner predicts the data center is toast: They might be right*, 27 July 2018, <https://www.techrepublic.com/article/gartner-predicts-the-data-center-is-toast-they-might-be-right/>.

[redacted]

Figure 6: Backup Storage Growth

Much of this growth has been driven by the increased use in our business of digital technologies for managing our ageing asset base. The list below outlines some of the key areas of growth:

- Increased structured data collection, integration and analytics on our assets as part of our Assets and Work program (this has driven the ability to efficiently defer over $205 million in repex in the 10-year period from 2015 to 2025).
- Photographs, video and LIDAR data related to our assets.
- General uplift in storage of information and documentation for business purposes.

In addition to the increase in the amount of data, it is worth noting that many of these data formats are increasing in size as technology improvements drive higher degrees of resolution/precision (eg photo file sizes are much larger than they were even five years ago).

5.2.5 Other DNSPs

The following is a summary of proposals by other DNSPs in their recent regulatory proposals that relate to the use of cloud hosting. In general, most DNSPs are intending to commence the use of cloud hosting services at some level in their next RCP:

- Essential Energy are planning to use SaaS, IaaS and PaaS as a primary alternative to traditional long-cycle capital investments.[38]
- TasNetworks have assumed 'No significant move to externally hosted services (cloud).'[39]
- EvoEnergy are taking an 'appropriate infrastructure' approach to hosting needs and acknowledge that cloud solutions provide a number of benefits that need to be considered through formal assessments.[40]

[38] Essential Energy, 2019-24 Regulatory Proposal, Supporting Document 12.1.16a: Essential Energy ICT Plan – Financial Years 2020-2024, v1.1, April 2019: Essential Energy 1.1.16a ICT Plan FY 20-24 – 20180430 – Public.

[39] TasNetwroks, 2019-24 Regulatory Proposal, Supporting Document 2322: IT Infrastructure Core Services – Investment Evaluation Summary: TN-IT Core Services 2422-Public.

[40] Evoenergy, 2019-24 Regulatory Proposal, Appendix 5.9: ICT expenditure proposal, 29 January 2018: Evoenergy – Appendix 5.9 ICT expenditure proposal-29 January 2018_Public.

- Endeavour Energy are proposing a cloud enablement program to further leverage cloud services.[41]
- AusGrid are intending to deploy cloud technologies across a number of their business areas.[42]

5.2.6 Cloud Case Study: Proof of Concept for Data Analytics

To improve our ability to provide services to customers we have been exploring the use of data analytics technologies. An in-flight proof of concept has been used to explore potential benefits in the use of predictive analytics related to the low voltage network. Given the volume of data and processing required, significant storage and processing capability was required to conduct the proof of concept.

A traditional approach to deploying new hardware and purchasing software licensing would have cost $[redacted] to $[redacted] in IT infrastructure hardware plus additional software costs. Timelines for procurement and installation of the equipment would have delayed starting the proof of concept by multiple weeks to months.

Using a SaaS model, we were able to commence the proof of concept as quickly as possible for an approximate cost of [redacted]

The proof of concept ran for approximately 6 months for a total hosting service cost of approximately $[redacted] This represents [redacted] of the cost of hosting services had we used our traditional approach to IT infrastructure.

Irrespective of the potential value of the capabilities explored, the IT Infrastructure Refresh approach for the proof of concept demonstrates the value of using cloud hosting services.

[41] Endeavour Energy, 2019-24 Regulatory Proposal, Supporting Document 10.27: ICT Investment Plan, February 2018: Endeavour Energy – 10.27 ICT Investment Plan – February 2018 - Public.

[42] Ausgrid, 2019-24 Regulatory Proposal, Attachment 5.18: ICT Technology Plan, April 2018: Ausgrid – Attachment 5.18 0 ICT Technology Plan – April 2018 - Public.

6 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 the 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 and comply with applicable regulatory obligations and requirements*** - The proposed expenditure is necessary as the effective operation of IT services, of which IT infrastructure is the foundation, is critical to the effective operation of the electricity network and management of network outages and meeting our regulatory obligations.

- ***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.

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 Infrastructure Refresh:
  - supports the efficiency and effectiveness of the operation and management of the network and the delivery of network services to customers;
  - takes advantage of cost efficiencies offered by cloud hosting services; and
  - helps to minimise operational costs.

- ***Prudent*** – The IT Infrastructure Refresh:
  - adopts processes which are prudent and consistent with the needs of other DNSPs in Australia and good electricity industry practice; and
  - considers appropriate sweating of IT infrastructure assets where risk is manageable.

- ***Realistic expectation of the demand forecast and cost inputs*** – The forecast expenditure for the 2020-25 RCP:
  - uses historic costs and bottom up estimating as the basis for costs; and
  - is based on independent advice, combined with multiple quotes, used to forecast cloud hosting costs.

7 Detailed description of selected option

7.1 Target state

Option 2 will give rise to a reduction of hosting infrastructure in the third-party data centres to approximately [redacted] of current (2017/18) usage, with allowances for organic growth. By 2022 we will have adopted a strong cloud position capable of delivering against the drivers of this business case. This is depicted in **Figure 7: Option 2 Target State** below.

[redacted]

🟧 Datacentre 🟦 Cloud

Figure 7: Option 2 Target State

All reviews validated that the two key cloud providers, [redacted], have valid platforms suitable for hosting IaaS workloads. All financial modelling utilised [redacted] pricing based on published price list availability and options which was later validated with requests for quotation (**RFQs**) on aspects of the service.

The new target state is expected to utilise the reduced data centre footprint set out in Table 22.

Table 23: Current and future state data centre rack capacity

Category	Current State	Future State	Differential
Racks	[redacted]	[redacted]	[redacted]
Approx. Rack Unit Capacity	[redacted]	[redacted]	[redacted]
Approx. Rack Units Utilised	[redacted]	[redacted]	[redacted]
Rack Unit % Utilisation	[redacted]	[redacted]	[redacted]

7.2 Establishing cloud services

To include external cloud services in the IT hosting infrastructure there are a number of key activities that must be performed to prepare for operating the hosting environment. These activities will be undertaken in preparation for adopting IT Infrastructure Refresh Option 2.

Governance

Operating a larger hybrid cloud will require maturation of our current governance model. The new governance model will include new areas for control and reporting while remaining agile to deliver maximum benefits from cloud services.

The key activities which will be undertaken include the following:

- **Governance group** – identify stakeholders required to build an effective cloud governance model.
- **Undertake risk assessment** – identify risks and ensure appropriate mitigations are in place.
- **Policies** – create policies, cloud standards and processes to achieve effective governance.
- **Cloud vendor selection** – define standards and application alignment criteria to select appropriate vendor.
- **Reporting framework** – define the reporting framework for the governance group and to executive management.
- **Implement** – deploy cloud governance and corresponding areas to the business and establish in to operations.

Network

Our current connectivity to cloud services [redacted]. This connectivity is unlikely to provide the necessary capacity and scalability for the hybrid cloud deployment. To create the new hybrid cloud hosting environment, additional connections will be made.

The connectivity must be scalable to allow us to grow over time and remain agile to meet hosting requirements. The identified critical path for creating the cloud connectivity involves the following steps:

- Identify and select a cloud connection aggregator service.
- Extend our data centre connectivity to cloud aggregator.
- Establish and deploy cloud network standards.

Security

Extending the security perimeter and establishing new standards for cloud deployed applications will require a shift in the current deployment. Based on the current deployment and approach, a re-design will be required prior to establishing the selected cloud presence.

Key elements identified for this deployment to be achieved are as follows:

- Identify hybrid cloud security approach and standards.
- Align standards with governance and networking standards.
- Establish security presence across hybrid cloud.

Application re–architecting

Critical to achieving the benefits that IaaS offers, will be the re–architecting of applications. This will align applications to customer and business needs and assist in achieving a prudent and efficient outcome from our hybrid cloud deployment.

Resource deployment and availability

As SAP is approximately [redacted] of the current infrastructure usage, it is the best example for the required changes in application architecture and its move to cloud provides the best example of the efficiencies of this architecting.

Currently critical SAP workloads are deployed in an active/active availability architecture. This means the capacity to run all production workloads must exist in both third-party data centres consuming power and increasing costs/overheads. Re-architecting introduces an active/standby availability which also allows scaling up to a larger instance when required. We note that:

- Host configuration is based on the "Warm Standby + DEV/QA" DR option.
- DEV/QA host is co–hosting the DEV/QA instances together with PROD secondary instance (without preload option).
- Additional hosts/instances can be started on–demand during projects or testing exercises.

By utilising IaaS we can see a marked change in our normal operations.:

[redacted]

Figure 8: IaaS Availability Model

Figure 8: IaaS Availability Model above illustrates only the production instance utilising compute and memory, while the underlying data is replicated to an alternate availability zone. The high availability metrics are still achieved using automated business continuity rules but delivers a greater cost efficiency during normal operations.

High Availability and Disaster Recovery

In the current private cloud hosting model, we must purchase all capacity for compute, memory and storage for replication and high availability as well as test workloads. Cloud platforms, particularly IaaS, offer significant benefits in running a more dynamic environment.

By re-architecting and operating a single production instance and a combined development and quality assurance (Dev/QA) instance, only the capacity required is used at any given time. Data is continuously replicated over availability zones from production but not loaded into memory.

[redacted]

Figure 9: IaaS during BCP event

During a BCP or DR event the DEV /QA instances will be shutdown to free resources for the production instance. The production instance will then take-over DEV/QA resources, once the take-over is complete the DEV/QA instance can be started as a new to host bring the environment back to normal operations.

7.3 Migration Roadmap

The migration plan depicted in **Figure 10: Migration Roadmap** below shows the high-level moves from data centre to cloud across the application groups.

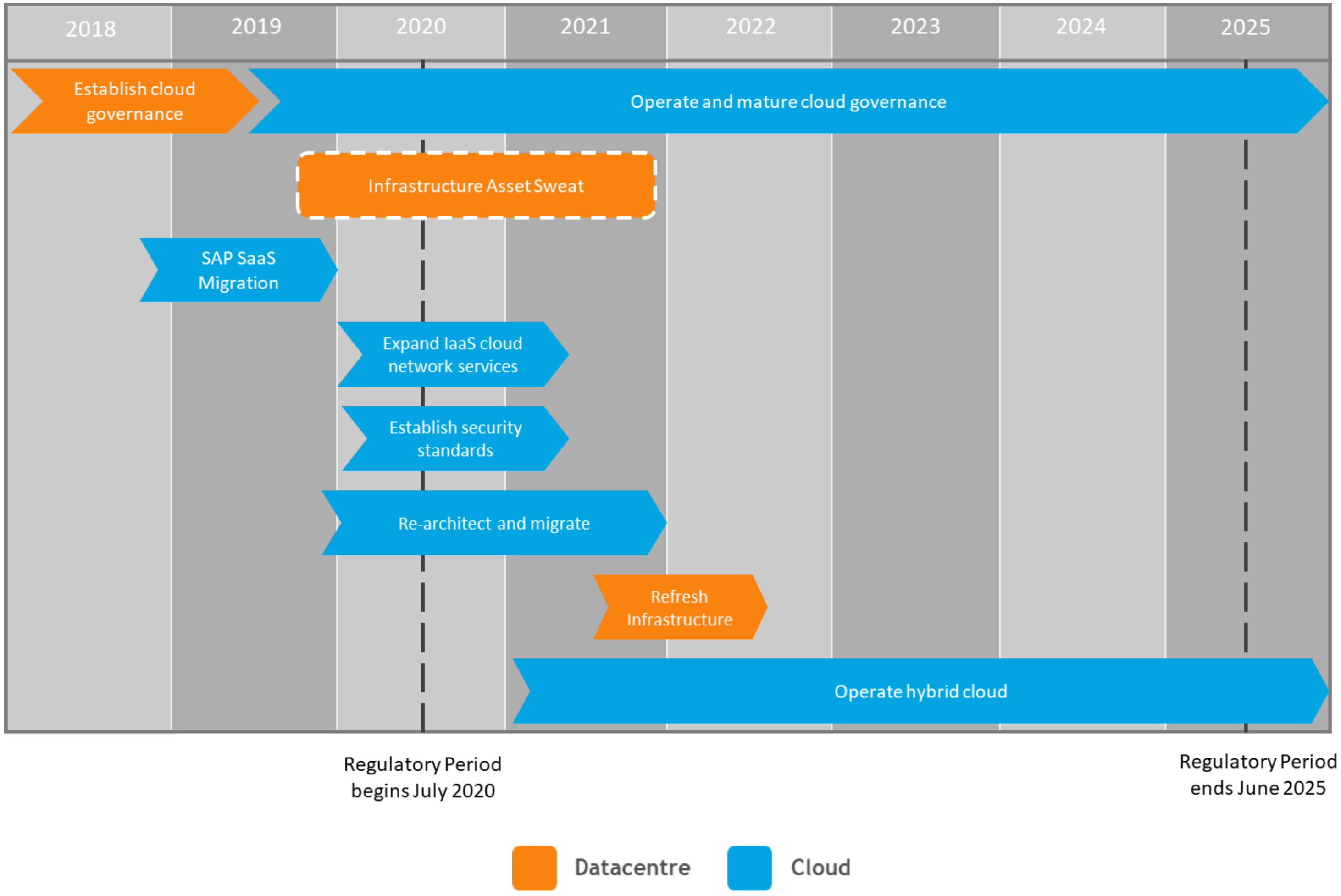

2018
2019
2020
2021
2022
2023
2024
2025
Establish cloud governance
Operate and mature cloud governance
Infrastructure Asset Sweat
SAP SaaS Migration
Expand IaaS cloud network services
Establish security standards
Re-architect and migrate
Refresh Infrastructure
Operate hybrid cloud
Regulatory Period begins July 2020
Regulatory Period ends June 2025
Datacentre
Cloud

Figure 10: Migration Roadmap

7.4 Migration

Migration - [redacted]

With over [redacted] of resources in the hosting environment used by [redacted] and proven hosting roadmaps on IaaS and SaaS, this is the largest opportunity for us to lower capital infrastructure costs and bring a high level of agility to the hosting environment.

[redacted]

Figure 11 - [redacted] Application Migration Summary

Migration – Critical Applications

The nature of the Critical applications means that each application was assessed individually. Those applications selected for either IaaS or SaaS solutions have internal strategies supporting this approach. [redacted] and [redacted] have been identified as legacy environment which are likely to be retired during the next reset period meaning IaaS will offer the opportunity to "turn off" the hosting and achieve a saving which is not possible in a purchase hosting infrastructure model.

[redacted]

Figure 12 - Critical Application Migration Summary

Migration – Non–Critical Applications

The approach selected for Non–Critical applications (**NC Apps**) moves these in percentages. While accuracy is lost in using these types of averages and percentages it allows the strategy to adapt to the changing nature of the application landscape. As all migrations for NC Apps are targeted at IaaS, there is a large amount of flexibility to adapt which applications will migrate, and how, during detailed planning.

Table 24: No. of applications by complexity

	Approx. # of Apps to migrate	% of Total classified non–critical apps
Low Complexity	[redacted]	[redacted]
Medium Complexity	[redacted]	[redacted]
High Complexity	[redacted]	[redacted]

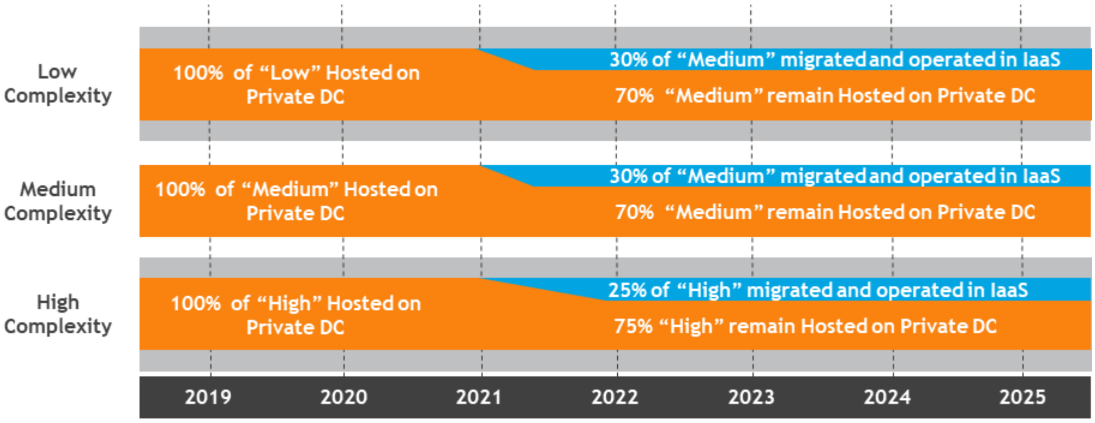

Low Complexity
100% of "Low" Hosted on Private DC
30% of "Medium" migrated and operated in IaaS
70% "Medium" remain Hosted on Private DC
Medium Complexity
100% of "Medium" Hosted on Private DC
30% of "Medium" migrated and operated in IaaS
70% "Medium" remain Hosted on Private DC
High Complexity
100% of "High" Hosted on Private DC
25% of "High" migrated and operated in IaaS
75% "High" remain Hosted on Private DC
2019
2020
2021
2022
2023
2024
2025

Figure 13 - Non-Critical Application Hosting Summary

7.5 Network Connectivity and Supporting Services

Option 2's approach to refresh these components of our IT infrastructure is unchanged from our business as usual approach.

Glossary

Acronym / Abbreviation	Definition
AER	Australian Energy Regulator
ASIC	Australian Securities and Investments Commission
AEMO	Australian Energy Market Operator
ATO	Australian Tax Office
BAU	business as usual
BCP	Business Continuity Planning
BW	Business Warehouse
capex	capital expenditure
CCP	Consumer Consultative Panel
CIC	Critical Infrastructure Centre
CRM	Customer Relationship Managment [system]
Click	Click Scheduling software
DBYD	Dial Before You Dig
DNSP	Distribution Network Service Provider
FIRB	Foreign Investment Review Board
DR	Disaster Recovery
GIS	Geographic Information Systems
HEC	SAP HANA Enterprise Cloud
HR	Human Resources
IaaS	Infrastructure as a Service
IT	Information Technology
IToM	IT Operating Model
NC Apps	Non–Critical applications
NEM	National Electricity Market
NER	National Electricity Rules
NPV	Net Present Value
OMS	Outage Management System
opex	operating expenditure
PaaS	Platform as a Service
PSS	Protection Settings System Redevelopment
RCP	Regulatory Control Period
repex	replacement expenditure
RFQ	requests for quotation
RIN	Regulatory Information Notice
SaaS	Software as a Service
SAP	Systems Applications Products [enterprise resource planning software platform]

Acronym / Abbreviation	Definition
SAPN	SA Power Networks
SCI Act	Security of Critical Infrastructure Act 2018

A. Appendix A – IT Service Stack Visualisation

Figure 14: IT Service Stack below is a depiction of our IT Service Stack in the context of our organisation. The two aspects of our IT Infrastructure Refresh that this business case explores options for are highlighted in:

- orange for our Hosting Services; and
- green for our Network Connectivity and Supporting Services.

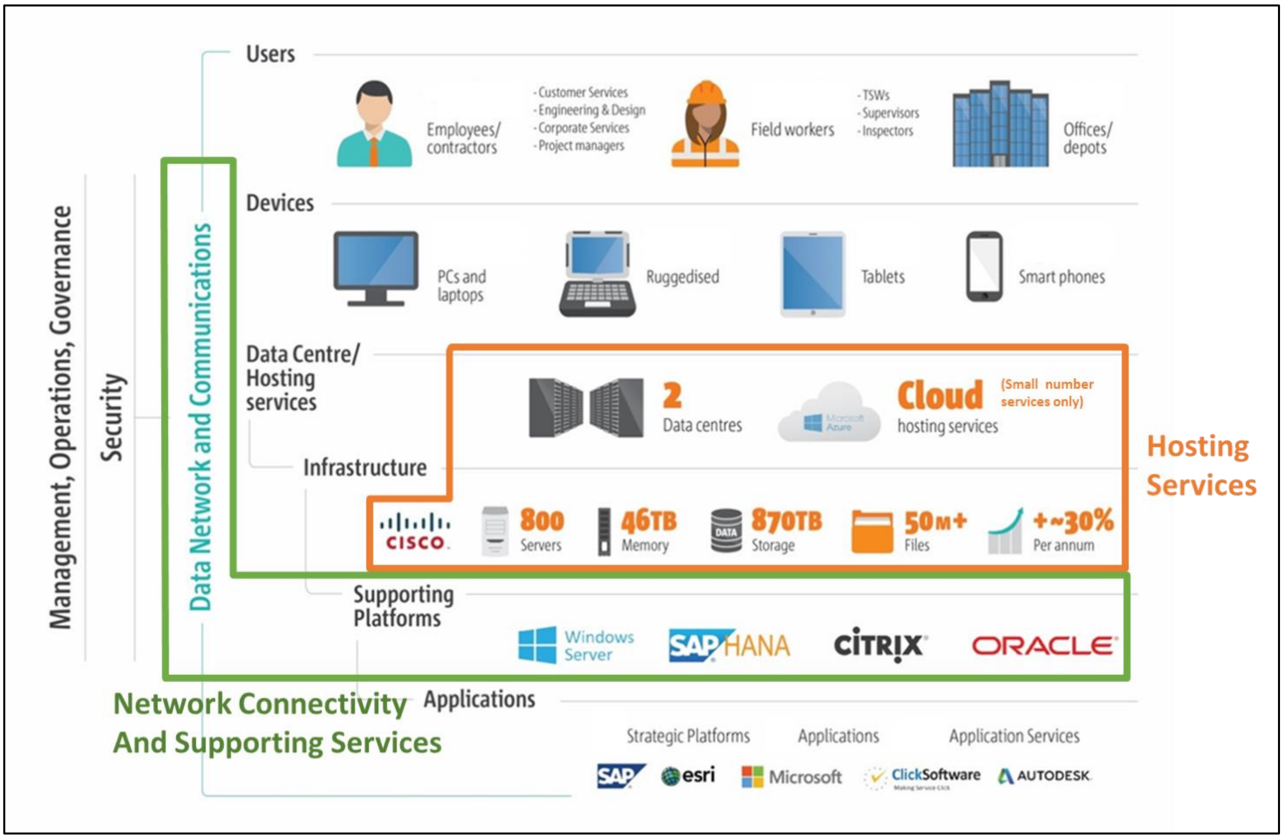
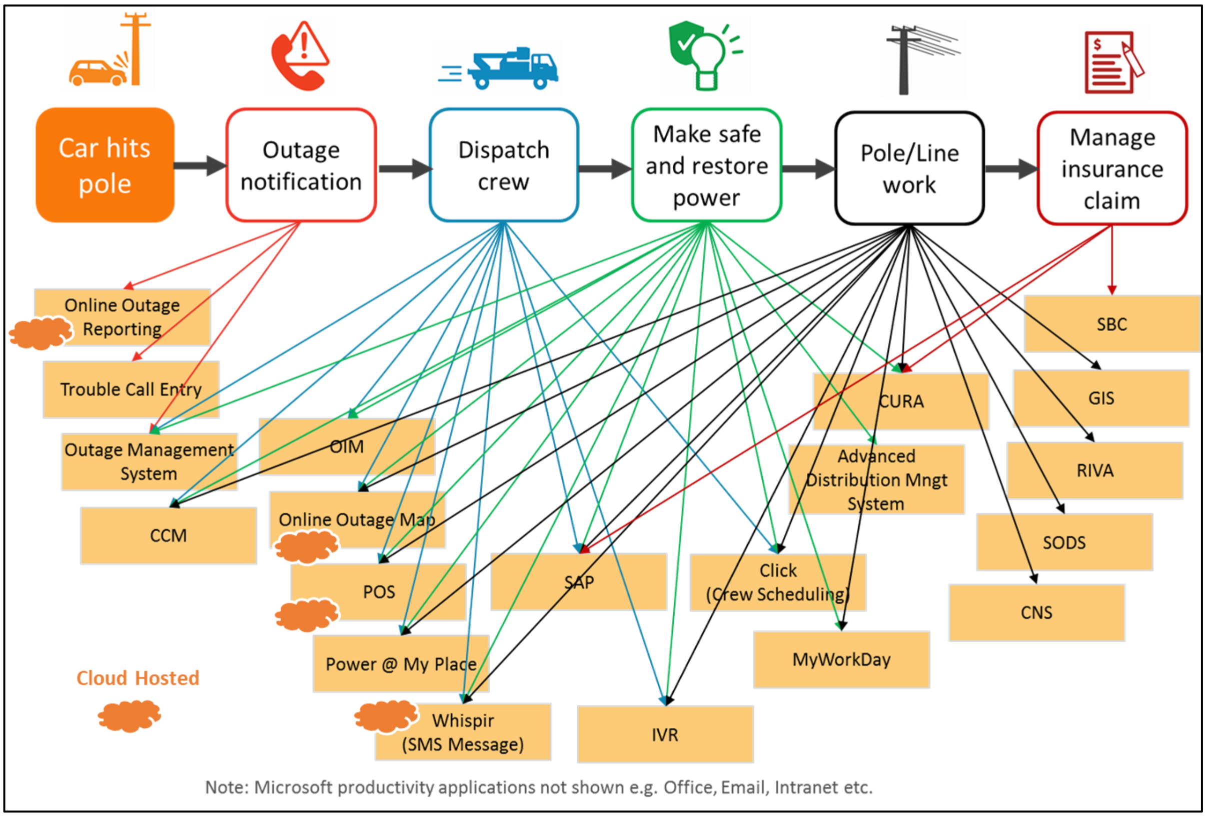


Figure 14: IT Service Stack

B. Appendix B – IT services used when car hits a pole

Our IT Infrastructure Refresh provides all the underlying hosting, data storage, connectivity and enabling technology that delivers IT services used operate our business and maintain the electricity network. By way of example, Figure 15: IT services used when car hits a pole below depicts the numerous IT services that are used to manage the restoration to service and associated business outcomes when a car drives into an electricity pole and causes an outage.



Note: Microsoft productivity applications not shown e.g. Office, Email, Intranet etc.

Figure 15: IT services used when car hits a pole

C. Appendix C: What is Cloud Computing?

The following is an excerpt from the current NIST (National Institute of Standards and Technology, United States) Definition of Cloud Computing:[43]

> *Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (eg, networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics, three service models, and four deployment models.*

C.1 Essential Characteristics:

On-demand self-service. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.

Broad network access. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (eg mobile phones, tablets, laptops, and workstations).

Resource pooling. The provider's computing resources are pooled to serve multiple consumers using a multi-tenant model, with different physical and virtual resources dynamically assigned and reassigned according to consumer demand. There is a sense of location independence in that the customer generally has no control or knowledge over the exact location of the provided resources but may be able to specify location at a higher level of abstraction (eg country, state, or data centre). Examples of resources include storage, processing, memory, and network bandwidth.

Rapid elasticity. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

Measured service. Cloud systems automatically control and optimise resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (eg storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service.

C.2 Service Models:

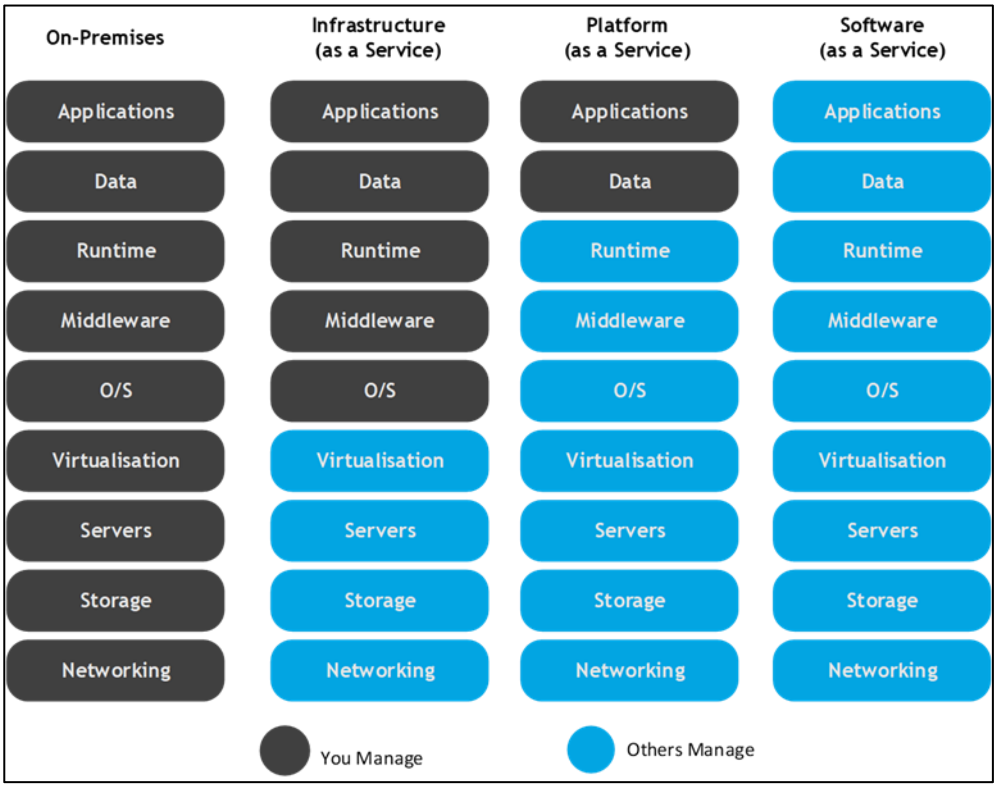
Software as a Service (SaaS). The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (eg web-based email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure (including network, servers, operating systems, storage, or even individual application capabilities) with the possible exception of limited user-specific application configuration settings.

Platform as a Service (PaaS). The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.

[43] NIST Definition of Cloud Computing, Special Publication 800-145 September 2011.

Infrastructure as a Service (IaaS). The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited control of select networking components (eg host firewalls).

Figure 16: Hosting Types, who manages below illustrates who manages the various aspects of IT services stack under each of these models, and on-premise through a data centre.



On-Premises	Infrastructure (as a Service)	Platform (as a Service)	Software (as a Service)
● Applications	● Applications	● Applications	🔵 Applications
● Data	● Data	● Data	🔵 Data
● Runtime	● Runtime	🔵 Runtime	🔵 Runtime
● Middleware	● Middleware	🔵 Middleware	🔵 Middleware
● O/S	● O/S	🔵 O/S	🔵 O/S
● Virtualisation	🔵 Virtualisation	🔵 Virtualisation	🔵 Virtualisation
● Servers	🔵 Servers	🔵 Servers	🔵 Servers
● Storage	🔵 Storage	🔵 Storage	🔵 Storage
● Networking	🔵 Networking	🔵 Networking	🔵 Networking

● You Manage 🔵 Others Manage

Figure 16: Hosting Types, who manages

C.3 Deployment Models

Private cloud. The cloud infrastructure is provisioned for exclusive use by a single organisation comprising multiple consumers (eg business units). It may be owned, managed, and operated by the organisation, a third-party, or some combination of them, and it may exist on or off premises.

Community cloud. The cloud infrastructure is provisioned for exclusive use by a specific community of consumers from organizations that have shared concerns (eg mission, security requirements, policy, and compliance considerations). It may be owned, managed, and operated by one or more of the organisations in the community, a third-party, or some combination of them, and it may exist on or off premises.

Public cloud. The cloud infrastructure is provisioned for open use by the general public. It may be owned, managed, and operated by a business, academic, or government organisation, or some combination of them. It exists on the premises of the cloud provider.

Hybrid cloud. The cloud infrastructure is a composition of two or more distinct cloud infrastructures (private, community, or public) that remain unique entities, but are bound together by standardised or proprietary technology that enables data and application portability (eg cloud bursting for load balancing between clouds).

D. Appendix D – 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 fora 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

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted] [redacted]

[redacted]

[redacted] [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[44] These are the known changes at the time of analysis. The probability of more is high.

[redacted] [redacted]

[redacted]

		[redacted]	
	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted] [redacted]

[redacted]

[redacted]

	[redacted]	
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

F. Appendix F: Cost models

The following documents containing our cost models are available on request.

1. Document: IT Infrastructure Hosting Services - Option 1 BAU

2. Document: IT Infrastructure Hosting Services - Option 2 Measured Move to Cloud

3. Document: IT Infrastructure Hosting Services Option 3 Aggressive Move to Cloud

4. Document: IT Infrastructure Refresh (con and sprting serv) - Option 1 – Industry Standard Refresh

5. Document: IT Infrastructure Refresh (con and sprting serv) - Option 2 – BAU

6. Document: IT Infrastructure Summary Options Consolidation and Comparison

G. Appendix G: Risk assessment

A comparison of Hosting options on the Inherent risk rating is identified below. The risk assessment for Network Connectivity and Supporting Services has a medium risk which does not affect the overall residual risk rating.

Risk Id	Risk Domain	**Risk Description** **Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:**	**Likelihood**	**Consequence**	**Risk Rating**	**Residual**	**Residual**	**Residual Risk**	**Residual**	**Residual**	**Residual Risk**	**Residual**	**Residual**	**Residual Risk**
			Do Nothing			**Option 1**			**Option 2**			**Option 3**		
		Overall Risk Rating	**Extreme**			**High**			**Medium**			**High**		
1	Reliability	• Business losing capability to manage electricity network resulting in increased number of outages, and duration of outages, for customers. • Increase in cyber security incidents resulting in malevolent people having access to our network control systems where they could impact network operations and non-compliance with regulatory obligations.	Almost Certain	Moderate	High	Possible	Moderate	Medium	Possible	Moderate	Medium	Possible	Minimal	Low
2	Financial	• Inability of our people to use IT systems to (examples and not inclusive): – Connect / disconnect customers – Bill customers – Pay staff, contractors and suppliers – Use efficient methods/systems for core business functions resulting in reductions to business productivity • Higher IT opex to resolve failures / issues Security breaches (refer Reputation risk below) may lead to significant litigation costs	Almost Certain	Moderate	High	Possible	Moderate	Medium	Likely	Minor	Medium	Likely	Minor	Medium

Risk Id	**Risk Domain**	**Risk Description** **Failure of IT infrastructure components, due to assets past their useful life and/or not kept current, secure and supported within the environment may lead to:**	**Likelihood**	**Consequence**	**Risk Rating**	**Residual**	**Residual**	**Residual Risk**	**Residual**	**Residual**	**Residual Risk**	**Residual**	**Residual**	**Residual Risk**
			Do Nothing			**Option 1**			**Option 2**			**Option 3**		
3	Health & Safety	• Business unable to manage critical and life support customers could result in fatalities, regulatory and financial consequences, adverse reputational outcomes • Inability to manage switching activities could result in fatalities, regulatory and financial consequences, adverse reputational damage	Possible	Moderate	Medium	Rare	Moderate	Low	Rare	Moderate	Low	Rare	Moderate	Low
4	Reputation / Customer Service	• Visible and direct impact to customers utilising applications supported by our IT Infrastructure resulting in a negative impact to reputation and increase in customer complaints (eg our registered electricians appointment booking application for connections) • Increase in cyber security incidents resulting in our organisation, and customers, private data being compromised. May also lead to malevolent people having access to our network control systems where they could impact network operations and non-compliance with regulatory obligations.	Almost Certain	Moderate	High	Likely	Minor	Medium	Possible	Minor	Low	Possible	Minor	Low
5	Regulatory	• Breach of security and privacy legislation and other regulatory obligations and requirements, including those imposed by regulators such as AEMO.	Almost Certain	Major	Extreme	Unlikely	Major	Medium	Unlikely	Major	Medium	Unlikely	Major	Medium
6	Organisational	Increase in frequency and duration of critical IT system outages as discussed above that will require the use of business continuity plans and specific management, for increasing periods of time, until services can be restored.	Almost Certain	Major	Extreme	Almost Certain	Minor	High	Likely	Minor	Medium	Almost Certain	Moderate	High