Technology Document ICT Program Brief TAM Infrastructure

2023-27 Transmission Revenue Reset

PUBLIC

Submitted: 29 October 2020

Table of Contents

1 Document Background

1.1 Purpose of this document

The purpose of this document is to outline a business case for a proposed program of work that will form part of AusNet Services' Technology TRR submission.

1.2 References

Document	Version	Author
Digital Utility Strategy	V1.3	S Scanlon
Infrastructure Roadmap Initiatives	V1	AusNet Services
FY21 Electricity Transmission Business Plan	V0.3	A Hill
TRR Technology Strategy	V0.21	S Scanlon
Technology Asset Management Policy	V0.4	A Pedler

1.3 Document History

Date	Version	Comment	Person
21/10/2020	V1.0	Published	S Scanlon

1.4 Approvals

Position	Date
Technology Leadership Team	

2 Executive summary

2.1 Program summary

The table below provides a summary of the program discussed in this brief. Additional information is provided throughout the brief.

Table 2-1 Summary table

Key objective(s) of the program	The objectives of the Infrastructure Technology Asset Management (TAM) program is to mitigate operational and security risks by ensuring AusNet Services meets lifecycle and capacity obligations, and optimises Data Centre (DC) infrastructure assets, including platforms, hardware and licenses, so that they remain up to date, robust, scalable and continue to meet customer expectations, service obligations of business and regulatory requirements.						
Key benefits	• Enables continued delivery of safe & reliable electrical services to customers with the least possible disruption, also meeting regulatory compliance and strategic business objectives • Prudent mitigation of key operational risks by ensuring systems are up to date and supported by vendors • Value for customers through controlled capex expenditure through effective lifecycle management to manage a growing asset base • Appropriate risk management over the life of assets to ensure costs of delivering technology services are managed • Removes potential security vulnerabilities through ensuring security patching is up to date, thereby reducing the risk of unauthorised access leading to data loss or loss of service to customers						
Cost allocation	Electricity Distribution	49%	Electricity Transmission	30%			
	Gas Distribution	21%					
Program type	**Recurrent**	☒					
	Non-Recurrent	☐					
	Client Devices	☐					
Program timings	Program duration:	5 years					
Expenditure forecast	**($m)**	**FY2023**	**FY2024**	**FY2025**	**FY2026**	**FY2027**	**Total**
	CAPEX	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$19.54
	OPEX	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$0.77
	Electricity Transmission Cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$20.30**
	Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$53.46
Estimated life of system	The expected life of systems are three to seven years, including servers, software & license, hardware compliance.						

Program Brief

Customer Engagement	This program has been proposed as part of AusNet Services Electricity Distribution Price Reset (EDPR) submission and this brief pertains to the TRR allocation of these costs. As part of the EDPR process, we have held deep dive workshops with stakeholders including the Customer Panel, on ICT. In that engagement we described the importance and need for ICT expenditure to meet our customers' evolving needs and to support compliance with regulatory and legal obligations. Material associated with all our deep dives is available on AusNet Services' website. A key theme of our engagement with the Customer Forum was the need for us to provide clarity on what we were proposing and what the expected customer benefits were. This information has been also presented to the Customer Advisory Panel (CAP) We acknowledge the feedback received from both sessions and have taken it into consideration when proposing the most appropriate option for this business case.

AusNet Services is required to deliver safe and reliable electricity services with the least possible disruptions to customers. IT infrastructure assets and systems underpin all operations at AusNet Services. To ensure the continued reliability of operations and in turn the delivery of electricity to customers, AusNet Services' infrastructure must remain up to date, be robust, scalable and agile to the changing demands of the business, regulatory and customer requirements.

Therefore, the objectives of the program are to serve these needs, including:

- Business improvements that will enhance efficiency and reduce opex; and
- Replacement of End-of-Life and Out-of-Support Hardware and Software to avoid infrastructure failure, disruption to customers, and increased opex.

The TAM Infrastructure technology program has identified these key initiatives to enable continuity of systems operations:

- Operating system version upgrades and license refresh,
- Hardware Assets Lifecycle refresh, including servers, field mobility iPads, etc.
- Application Hosting Initiatives (AHI) Server refresh, and
- AusNet On Demand Platform (AoD) refresh.

This investment enables AusNet Services to avoid systems failure in AusNet Services' technology environments;

- Ensure AusNet Services meets its Lifecycle and Capacity obligations throughout FY2023-2027,
- Mitigate known operational risks and issues,
- Reduce effort for supportability of legacy infrastructure and applications, and
- Maintain the technology environment in a vendor supported state.

Program Brief

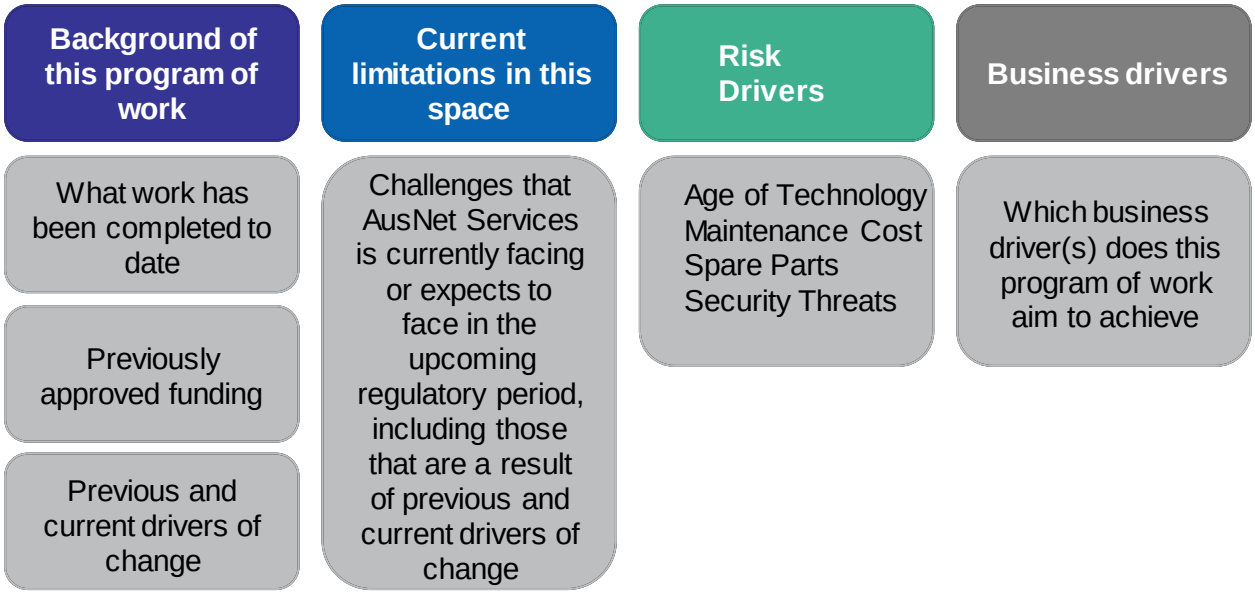
Alignment with AER ICT expenditure assessment framework

In accordance with the AER - Guidance Note - Non-network ICT capex assessment approach for electricity distributors (28 November 2019), we have categorised this program as recurrent expenditure, on the basis that it relates to ongoing refresh of AusNet Services' Data Centre (DC) infrastructure assets, including platform, hardware and licenses, so that they remain up to date, robust, scalable and continue to meet service obligations of business and regulatory requirements. This is a cost that must be incurred periodically. As such, we have not undertaken NPV analysis in support of the project. However, consistent with AusNet Services' internal practices, we have developed a detailed business case for the chosen option.

3 Context

This chapter provides an overview of the context in which this program of work is operating within, and the figure below lists out key areas to be discussed.

Figure 3-1 Key areas of the context to be discussed



3.1 Background

The TAM Infrastructure program provides lifecycle refresh of infrastructure assets, end user assets and shared platforms (e.g. data centre facilities and IT equipment). It is made up of specific assets requiring replacement during the regulatory period.

The proposed expenditure on lifecycle refreshes secure the platform's support and technology spending in a controlled manner so that capacity, performance and service levels can be maintained through the next period. By ensuring these systems continue to be supported by suppliers, AusNet Services gains access to the expertise required to resolve incidents, as well as patches for security vulnerabilities and bug fixes as they are available.

Critical assets (i.e. SCADA) will need to remain on premise through the 2023-27 period; hence, AusNet Services needs to maintain current data centre (DC) assets.

The TAM program forms AusNet Services' recurrent Technology investment to ensure lifecycle currency and capacity management.

3.2 Current limitations

Specific assets replaced during the regulatory period are driven by the application demand (i.e. capacity, performance, etc.) and volume demands of the business at the point in time (e.g. number of employees).

Within any year, capacity, lifecycle and operational enhancement changes are required for business systems to meet the following needs:

- Probabilistic risk avoidance, mitigating the following risk category types:
  - Legal & compliance
  - Regulation
  - Health & Safety
  - Reputation.

- Identification of business improvements which will allow us to manage the cost of delivering technology services at an acceptable level of risk over the life of the assets.
- Minimise the risk of system failure and disruption to customer services.
- Minimise security threats of unauthorised access.

Therefore, lifecycle refreshes and enhancements in the FY2023–27 period will be of particular importance as they will provide stability and dependability of the infrastructure and compliance with regulatory and vendor support requirements. If lifecycle refreshes are not carried out, AusNet Services could be impacted by service failures in an unsupported environment, representing a critical risk to the distribution of electricity to customers. To ensure this does not occur, lifecycle initiatives have to be implemented in a timely manner.

The infrastructure requirements for additional and new demand (i.e. new applications hosted in the data centre) is not part of the TAM infrastructure lifecycle refreshment. As noted above, this aligns with the definition of recurrent expenditure in the AER's Consultation paper – ICT Expenditure Assessment.

3.3 Technology risk drivers

All TAM expenditure initiatives identified and proposed by AusNet Services reflect the least cost service delivery strategy for technology infrastructure over time at the maximum level of risk that the business and customer services they support can reasonably tolerate:

1. **Technology risk increases over time.** Hardware failures follow a pattern of fail in the first months of operation, stable operation for a number of years, and exponential increase in failures after the end of life as defined by the manufacturer. This failure curve is known as the 'bathtub curve'[1]. Extending the life of technology after the vendor end of life date increases business and service performance risk as the likelihood of failure increases.
2. **As technology ages the cost of maintenance increases.** Equipment vendors will provide cost effective support until a point is reached where their costs increase. Vendors need to provide internal capability to support both old and new products, where the old products are used by a decreasing customer base. This cost is passed on to the customer and often exceeds the cost of deploying and maintaining new technology.
3. **Spare parts become unavailable.** Technology relies on a supply chain of components and suppliers, which are subject to component lifecycle management. After a number of years, a manufacturer will be unable to source component parts making it impossible to produce spare parts. Reliable access to spare parts is then compromised and the risk of unserviceable outages increases.
4. **The price-performance of technology infrastructure continues to improve over time**, lowering the total cost of delivering like-for-like services. Failing to refresh infrastructure locks in higher costs and lower service capabilities.
5. **Security.** AusNet Services' DC assets need to be protected against cyber security threats. Ongoing patching is required to remove vulnerabilities which allow for unauthorised access leading to major business disruption or loss of critical information. When technology is no longer supported by a manufacturer no new patches are made available to address security vulnerabilities. The risk of unauthorised access leading to data loss, loss of service, or non-compliance with regulatory requirements, increases over time.

[1] *Basic terms and models used for reliability evaluation*, National Institute of Standards and Technology at https://itl.nist.gov/div898/handbook/apr/section1/apr124.htm and *Software Reliability,* Jiantao Pan (Carnegie Mellon University) at https://users.ece.cmu.edu/~koopman/des_s99/sw_reliability/

3.4 Business drivers

In the face of significant industry disruption resulting in a period of substantial uncertainty and increasing complexity across the industry, AusNet Services has selected four key business drivers which set the direction for the business.

These business drivers are:

- Maintaining current service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid;
- Updating and implementing new technologies to enable AusNet Services to respond to changes within the growing renewable generation market;
- Complying with new obligations; and
- Delivering improvements requested by our customers regarding sustainability and cost.

All expenditure programs identified and proposed by AusNet Services will have regard to the business drivers and can be directly linked to at least one of these initiatives. This research has also been further validated through the ICT deep drive presented to the customer forum.

This program of work is most relevant to the following business drivers;

- **'Maintaining current service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid'**, as it contributes to increased effectiveness and capability in managing and maintaining a robust technology environment.
- **'Updating and implementing new technologies to enable AusNet Services to respond to changes within the growing renewable generation market'**, as it allows for flexibility in maintaining infrastructure assets in line with its lifecycle, allowing the business to continue to operate efficiently and limit system outages. System outages cause delays and increase the cost of operating the business.

3.5 Approach to developing expenditure forecast

For each program brief, a consistent approach is used to develop programs of work and the associated expenditure forecast for the regulatory period FY2023-2027.

A full overview of the approach can be found in section 3.2 of the "*AusNet Services – Transmission Revenue Review – Technology Strategy Document*".

To develop each program of work and associated expenditure, the following steps were taken:

- Needs analysis to identify areas of the network and business processes that require investment over the upcoming regulatory period,
- Bottom up discussion with business and technology architects and delivery leads to develop options to address the investment need, including scope, key objectives, and drivers influencing the requirement for the programs,
- Consideration of different options to achieve the objectives of the program and analysis of their relative costs, benefits and risks, and
- Top down view to ensure that the Technology Strategy investment portfolio represents prudent and efficient expenditure for the upcoming period, relative to AusNet Services' previous expenditure and also benchmarked against other comparable Transmission businesses.

4 Options

4.1 Overview

This section provides an overview of a select number of options that may feasibly alleviate the current limitations as addressed in section 3.2. Each option represents a combination of initiatives within the program of work.

Table 4-1 Brief overview of the options

Brief overview of each of the options	
Option 1	Minimise Capex Investment This option refers to “sweating the assets”, which does not adopt a proactive approach to ensure continued vendor support and mitigation of operational risks. Key initiatives include: • Operating Systems version and license refresh • Application Hosting Initiative Platform and Server Refresh • AoD Refresh • Service Now platform buildout & GRC for security and IT
Option 2 (Recommended)	Business as Usual and tactically leverage existing on-premise infrastructure assets to mitigate operational and security risks. Key initiatives include: • All option 1 capex initiatives during transition period • Hardware Lifecycle Refresh, including Air Conditioners (AC) for Data Centers, Backup storage, Network Attached Storage (NAS), field mobility iPads & UPS for specific Data Centers
Option 3	[C-I-C]

4.2 Option #1 Sweat Hardware Assets

This option involves extending the life of existing hardware assets and requires that AusNet Services does not adopt a proactive approach to improving infrastructure hardware assets impacted by capacity and lifecycle constraints when failing out of vendor support.

This option presents a high risk of system failure with critical consequences likely to result in non-compliance with regulations or business objectives. Therefore, this option is not recommended.

Program Brief

Alignment to objectives

Table 4-2 Objectives analysis of option 1

Objective	Outcome	Comments
Mandatory requirements, including safety, legal, regulatory and technical compliance	Partial	Partially aligned as this option involves the adoption of significant risks and system failure could result in the following critical risk category types: a. Legal & Compliance b. Reputation c. Regulation d. Health & Safety
Business improvements that will improve efficiency and manage costs and risk over time	Partial	Partially aligned as it may seem to be a lower upfront expenditure option. However, a higher risk environment would lead to an unsupported operating environment, potentially higher long-term support costs and lower productivity in business.
Replacement of End-of-Life and Out-of-Support Hardware and Software to avoid infrastructure failure, customer disruption and increased operational expenditure	✕	Not aligned as infrastructure assets failure will result in disruption to customers and increased operational expenditure.

Costs

The direct cost of option 1 addresses platform and license maintenance requirements excluding hardware assets refresh.

Table 4-3 Costs of option 1

($m)	FY2023	FY2024	FY2025	FY2026	FY2027	Total
Capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$13.07
Opex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$0.54
Electricity Transmission Cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$13.61**
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$40.71

Importantly, the costs in the table above do not include the costs associated with critical system failure - either to AusNet Services or its customers. Such costs have not been modelled but are related to safety obligations/initiatives, regulatory, compliance and/or reputational costs. The risk of incurring these costs, which may be significant, is higher under this option than options 2 or 3.

Benefits

Sweating assets can save AusNet Services investment expenditure, with a saving of $6.5m compared to option 2.

However, this apparent saving can be easily offset by the risk of system failure and increased capex due to change of environment. For example, avoiding refreshes now would require greater investment in the future should an unsupported system failure occur. This will allow us to manage the cost of delivering technology services at an acceptable level of risk over the life of the assets.

Risks

There are several risks associated with this option, as highlighted in the table below. Based on the consequence and likelihood of each risk, we have rated each of the individual risks blue, green, yellow, orange or red (order of severity). See Below in
Table 5-3, we have identified techniques or actions to mitigate the risks identified for this option.

Table 5-3 Option 2 risks and mitigation actions

	Risk	Rating	Mitigation
R2.1	Lower operational risk due to system failure	D	Lifecycle maintenance as per manufacturer's specification.
R2.2	Increased cost and complexity of maintaining datacenter centric infrastructure assets.	E	Lifecycle maintenance as per manufacturer's specification Continue optimizing on premise data centre to move towards cloud based services
R2.3	Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	D	This is a common risk across all business areas

Attachment 1 – Risk level matrix for additional information on this rating system.

Table 4-4 Risks of option 1

	Risks	Consequence	Likelihood	Risk rating
R1.1	Hardware that is out of support and has gone end of life places the business at risk in the event there is a hardware failure, firmware issue or BIOS issue.	Level 2. Business impact in the form of productivity loss.	Likely	C
R1.2	Unsupported systems may fail, and no support or maintenance services will be available to call upon.	Level 2. Customer / community affected by loss of service.	Likely	C

R1.3	Increased cost and complexity of maintaining Data Centre infrastructure assets.	Level 1. An impact that would have otherwise required minor management attention.	Likely	D
R1.4	Reduced or loss of employee productivity and business functions.	Level 1. Impact of event absorbed through normal activity.	Likely	D
R1.5	Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	Level 1. An impact that would have otherwise required minor management attention.	Possible	E

Overall, we consider this option is rated medium risk.

Alignment to mitigation of key risk drivers

As discussed in Section 3.3, there would be no alignment in respect of maintaining Vendor support of current assets with security benefits.

Table 4-5 Alignment to key risk drivers of option 1

Risk Driver		Achieved by
Technology risk increases over time	X	N/A
Cost of maintenance increases as technology ages	X	N/A
Spare parts unavailable	X	N/A
Availability of new technology	X	N/A
Security	X	N/A

Alignment to business related drivers of expenditure

As discussed in Section 3.4, there are four Transmission business drivers that AusNet Services has identified and is focussing on over the next regulatory period. In summary, the business drivers are not directly relevant to this option.

4.3 Option #2 Lifecycle Refresh (RECOMMENDED)

This option involves carrying out the TAM lifecycle refresh initiatives to ensure the AusNet Services' business environment is supported and industry and/or legal obligations are met. Costs, benefits, mitigated risks and customer related drivers of expenditure are explored further below.

Note; this program relates to electricity transmission, which normally is 30% of the overall corporate capital investment of circa $48.5M over a five-year period. However, in the next TRR period (2023-27)

additional capital of $1M pa has been identified for specific transmission systems and data centre (DC) infrastructure that will need lifecycle and capacity upgrades in the period.
For example:

- Lifecycle replacements within both Data Centre SCADA rooms of air conditioners and UPS
- Lifecycle refresh of infrastructure supporting the transmission network planning and management systems

Our policy for the frequency with which individual assets are refreshed is aligned to our Technology Asset Management Policy and is dependent on the business criticality of the services they support and the risk of their failure with age.

Alignment to objectives

Table 4-6 Objectives analysis of option 2

Objective		Comments
Mandatory requirements, including safety, legal, regulatory and technical compliance; and	✓	Lifecycle maintenance, as per manufacturer's specification. Reliable and vendor supported system contributes to mitigate the operational and security risks
Business improvements that will improve efficiency and reduce Operational Expenditure; and	✓	Mitigate the risk of system failure and disruption to business operations.
Replacement of End-of-Life and Out-of-Support Hardware and Software to avoid infrastructure failure and increased operational expenditure	✓	Lifecycle maintenance delivers more efficient technology, so subsequent refreshes have lower capital costs

Costs

Infrastructure assets that will be required to be refreshed within TAM include storage and compute appliances, security operational tools and licensing. Lifecycle refreshes include Database, Virtualisation Software, Environment Management and other shared platform based refreshes.

As business applications are retired and replaced, platform consolidation ensures that there is not a myriad of legacy environments being maintained and that available compute, storage and other capacities are leveraged efficiently to support demand. Platform consolidation provides for good management and maintenance of shared platforms and infrastructure and is not specific to a single TRR period.

Program Brief

ServiceNow (SNOW) is a service management tool and central source of truth for infrastructure assets and shared platforms (i.e. the CMDB). This provides evidence on the level of capacity management, ensures that infrastructure has appropriate monitoring in place and is delivering data to capacity management.

Table 4-7 Costs of option 2

($m)	FY2023	FY2024	FY2025	FY2026	FY2027	Total
CAPEX	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$19.54
OPEX	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$0.77
Electricity Transmission Cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$20.30**
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$53.46

Benefits

Lifecycle maintenance delivers more efficient, stable technology at lower risk. In addition, there are other benefits listed as below:

Table 4-8 Benefits of option 2

Benefits
Reduced likelihood and subsequently avoided cost of critical system failure and increase in support/maintenance costs. Improved system and customer information security compared to option 1. Conservatively future proofing against potential changes in adjacent systems that may require an up to date systems to function and ensuring that AusNet has the ability to adapt to alternative technologies can reduce the cost to serve and in doing so, lower prices for customers.

Risks

There are risks associated with this option, as highlighted in the table below. Based on the consequence and likelihood of each risk, we have rated each of the individual risks blue, green, yellow, orange or red (order of severity). See Below in
Table 5-3, we have identified techniques or actions to mitigate the risks identified for this option.

Table 5-3 Option 2 risks and mitigation actions

	Risk	Rating	Mitigation
R2.1	Lower operational risk due to system failure	D	Lifecycle maintenance as per manufacturer's specification.
R2.2	Increased cost and complexity of maintaining datacenter centric infrastructure assets.	E	Lifecycle maintenance as per manufacturer's specification Continue optimizing on premise data centre to move towards cloud based services
R2.3	Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	D	This is a common risk across all business areas

Attachment 1 – Risk level matrix for additional information on this rating system.

Table 4-9 Risks of option 2

	Risks	Consequence	Likelihood	Risk rating
R2.1	Lower operational risk due to system failure	Level 2 business impact in the form of productivity loss.	Possible	D
R2.2	Increased cost and complexity of maintaining datacenter centric infrastructure assets.	Level 1. An impact that would have otherwise required minor management attention.	Possible	E

R2.3	Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	Level 2. An impact that would have otherwise required minor management attention over several days.	Possible	D

Overall, we consider this option is rated Low.

Alignment to mitigation of key risk drivers

As discussed in Section 3.3, this option is fully aligned in respect to reducing technology risk and providing a stable environment.

Table 4-10Alignment to key risk drivers of option 2

Risk Driver		Achieved by
Technology risk increases over time	✓	By maintaining critical systems in line with their supplier lifecycle maintenance requirements.
Cost of maintenance increases as technology ages	✓	Staying in Vendor support window is more efficient and cost effective than getting customised vendor support.
Spare parts unavailable	✓	Maintaining infrastructure assets in line with its lifecycle ensures spare parts availability reducing down time.
Availability of new technology	✓	Obtain efficiency by replacing obsolete technology
Security	✓	Critical lifecycle refresh remedies the vulnerabilities and ensure the security and reliability of the network

Alignment to business related drivers of expenditure

As discussed in Section 3.4, there are four Transmission business drivers that AusNet Services has identified and is focussing on over the next regulatory period. The table below highlights how this option

will input into the initiatives where relevant. Where we consider that a business driver is not directly relevant to the option, 'N/A' is applied.

Table 4-11 Business related drivers of option 2

Business drivers	How this program achieves this
Maintaining current service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid;	Refreshing current applications and upgrading where prudent. Allow for increased effectiveness and capability in managing and maintaining a robust technology environment
Updating and implementing new technologies to enable AusNet Services to respond to changes within the growing renewable generation market;	Maintaining infrastructure assets in line with its lifecycle allows the business to continue to operate efficiently and limit system outages. System outages cause delays and increase the cost of operating the business
Complying with new obligations	N/A
Delivering improvements requested by our customers regarding sustainability and cost.	Operation risks are mitigated. Therefore, continuity and reliability of supply is maintained, which contributes to brand and reputation.

4.4 Option #3 Strategic Migration to Cloud

[C-I-C]

Alignment to objectives

Table 4-12 Objectives analysis of option 3

Objective		Comments
Mandatory requirements, including safety, legal, regulatory and technical compliance; and	✓	[C-I-C]
Business improvements that will improve efficiency and reduce Operational Expenditure; and	✓	[C-I-C]
Replacement of End-of-Life and Out-of-Support Hardware and Software to avoid infrastructure failure and increased operational expenditure	✓	[C-I-C]

Costs

[C-I-C]

Table 4-13 Costs of option 3

($m)	FY2023	FY2024	FY2025	FY2026	FY2027	Total
Capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$26.86
Opex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$4.74
Electricity Transmission Cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$31.60
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$89.01

Benefits

[C-I-C]

Table 4-14 Benefits of option 3

Benefits
[C-I-C]
[C-I-C]
[C-I-C]
[C-I-C]
[C-I-C]

[C-I-C]

Risks

There are several risks associated with this option, as highlighted in the table below. Based on the consequence and likelihood of each risk, we have rated each of the individual risks blue, green, yellow, orange or red (order of severity). See Below in
Table 5-3, we have identified techniques or actions to mitigate the risks identified for this option.

Table 5-3 Option 2 risks and mitigation actions

	Risk	Rating	Mitigation
R2.1	Lower operational risk due to system failure	D	Lifecycle maintenance as per manufacturer's specification.
R2.2	Increased cost and complexity of maintaining datacenter centric infrastructure assets.	E	Lifecycle maintenance as per manufacturer's specification Continue optimizing on premise data centre to move towards cloud based services
R2.3	Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	D	This is a common risk across all business areas

Attachment 1 – Risk level matrix for additional information on this rating system.

Table 4-15 Risks of option 3

	Risks	Consequence	Likelihood	Risk rating
R3.1	[C-I-C]	[C-I-C]	Possible	D
R3.2	[C-I-C]	[C-I-C]	Possible	D
R3.3	[C-I-C]	[C-I-C]	Possible	D

[C-I-C]

Alignment to mitigation of key risk drivers

As discussed in Section 3.3, this option is fully aligned in respect to reducing technology risk and providing a stable environment.

Table 4-16 Alignment to key risk drivers of option 3

Risk Driver		Achieved by
Technology risk increases over time	✓	[C-I-C]
Cost of maintenance increases as technology ages	✓	[C-I-C]
Spare parts unavailable	✓	[C-I-C]
Availability of new technology	✓	[C-I-C]
Security	✓	[C-I-C]

Alignment to business related drivers of expenditure

As discussed in Section 3.4, there are four Transmission business drivers that AusNet Services has identified and is focussing on over the next regulatory period. The table below highlights how this option will input into the initiatives where relevant. Where we consider that a business driver is not directly relevant to the option, 'N/A' is applied.

Table 4-17 Business related drivers of option 3

Business drivers	How this program achieves this
Maintaining current service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid;	Refreshing current applications and upgrading where prudent.
Updating and implementing new technologies to enable AusNet Services to respond to changes within the growing renewable generation market;	[C-I-C]
Complying with new obligations	[C-I-C]
Delivering improvements requested by our customers regarding sustainability and cost.	[C-I-C]

5 Assessment and recommended option

5.1 Assessment of the options

To identify a recommended option for this program of work, we have selected a number of criteria to assess each of the options. We consider that these criteria represent a comprehensive view of each option, in achieving AusNet Services' customer and business objectives as well as requirements of the AER in ensuring that any expenditure is both prudent and efficient.

The table below summarises our assessment of each of the options against the criteria.

Table 5-1Summary table of the assessment of the options

	Option 1	Option 2	Option 3
Alignment to objectives	Does not achieve objectives	Aligned with program objectives	Aligned with program objectives
Costs ($m)	$13.61	$20.30	$31.60
Overall risk rating	Medium	Low	Low
Alignment to technology risk drivers	Low alignment (1/5)	High alignment (5/5)	High alignment (5/5)
Alignment to business related drivers of expenditure	No alignment (0/4)	High alignment (3/4)	High alignment (3/4)

5.2 Recommended Option – Risk Mitigation

Based on this assessment, Option 2 is the recommended option, as it reflects a prudent level of expenditure that will progress AusNet Services towards its objective of efficient and effective operations while maintaining current reliability levels and reducing potential opex costs relating to system failures if no action taken.

However, the implications for the continuity of operations while moving towards cloud-based services should be a key consideration in future design decisions.

Because option 2 and option 3 meet the objectives at a similar level of risk but option 3 comes with a substantially higher transition risk, option 2 represents a more prudent transitional approach as AusNet Services pursues a long term migration from on-premise infrastructure to the cloud.

Table 5-2 Confirmation of scope of recommended option

In scope	Out of scope	Dependencies
[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]

Below in
Table **5-3**, we have identified techniques or actions to mitigate the risks identified for this option.

Table 5-3 Option 2 risks and mitigation actions

	Risk	Rating	Mitigation
R2.1	Lower operational risk due to system failure	D	Lifecycle maintenance as per manufacturer's specification.
R2.2	Increased cost and complexity of maintaining datacenter centric infrastructure assets.	E	Lifecycle maintenance as per manufacturer's specification Continue optimizing on premise data centre to move towards cloud based services
R2.3	Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	D	This is a common risk across all business areas

6 Attachment 1 – Risk level matrix

The figure below shows the risk level matrix to which we have assessed each of risks within the options. Risks of highest concern are rated red, whereas those of lowest concern are rated blue.

Figure 6-1

Likelihood	Consequence 1	2	3	4	5
Almost Certain	C	C	B	A	A
Likely	D	C	B	B	A
Possible	E	D	C	B	A
Unlikely	E	D	D	C	B
Rare	E	E	D	C	C

Consequence Rating	
5	Catastrophic
4	Major
3	Moderate
2	Minor
1	Insignificant

Overall Risk Rating	
A	Extreme
B	High
C	Medium
D	Low
E	Very Low