

AusNet

Electricity Distribution Price Review FY2027 to FY2031 (EDPR 2027-31)

Business case: Technology Asset Management - Infrastructure

Date: January 2025



Table of contents

1. Executive summary	3
2. Context	5
2.1 Categories of ICT infrastructure	5
2.2 Drivers of investment	5
2.3 Historical performance	5
2.4 Historical recurrent expenditure	7
3. Needs identification	8
3.1 Strategy in the 2027-31 period	8
3.2 Needs identification	8
4. Options consideration	9
4.1. Assessment approach	9
4.2. Risk and cost analysis of alternative strategies	9
4.2.1 Option 1 – Actively manage without vendor support	10
4.2.2 Option 2 – Perform lifecycle refreshes (recommended option)	11
Appendix A – Line by line assessment	13

Document history

DATE	VERSION	COMMENT	PERSON
30/09/2024	V1.0	Initial draft business case for review	
22/11/2024	V2.0	Revised business case incorporating input	
5/12/2024	V3.0	Updated for final review	
20/12/2024	V4.0	Final business case document	

Related documents

DOCUMENT	VERSION	AUTHOR
Technology Asset Management (TAM) Applications Business Case	V4.0	AusNet Services
Technology Strategy and Investment Plan	V3.0	AusNet Services
AusNet EDPR 2027-31 Digital Program NPV Model	V3.0	AusNet Services

Approvals

POSITION	DATE
Digital & Technology – Strategy, Regulatory and Partner Management	December 2024
Digital & Technology – Architecture	December 2024
Distribution – Strategy and Regulation	December 2024

1. Executive summary

ICT infrastructure includes compute servers, storage servers, telecommunications and end user devices. Infrastructure is required to operate AusNet's technology systems and applications. These systems and applications enable AusNet's capability to safely and reliably operate our network assets in real time, securely provide customer information and accurate billing, efficiently plan and maintain our network assets, and efficiently run our business.

This business case relates to "Technology Asset Management" (TAM): recurrent capex on ICT infrastructure housed 'on premise' in our Richmond and Rowville data centres. It excludes recurrent operating expenditure on ICT infrastructure housed in the cloud. The infrastructure is predominantly for Operating Technology (OT) related to critical electricity network infrastructure. As an integrated business, it is essential that our electricity transmission ICT infrastructure is supported 'on premise' due to the criticality of transmission services to all Victorian customers, and this provides an opportunity to securely and cost effectively house ICT infrastructure related to our distribution network including ADMS and DERMS.

Over the last regulatory period, AusNet sought to migrate some of our ICT infrastructure to the cloud where there were opportunities to prudently and more cost effectively support the applications. This included our legacy data and analytics capabilities that would be downsized over time. However, our experience in some instances was that migrating infrastructure which required significant data and processing speed resulted in poor latency and was not cost effective. As a result, we have now balanced our infrastructure between on premises and the cloud, based on the requirements of specific applications.

With our current mix of on-premise and cloud ICT infrastructure assessed as optimal, our strategy in the 2027-31 period is to pursue efficiency opportunities in our data centres. This includes enhanced virtualisation to further improve agility and exploit scale economies across applications where possible, together with moving the datacentres toward a private cloud architecture over time.

The recurrent expenditure in this business case is to replace end of life hardware such as compute and storage servers, refurbish data centre facilities such as air conditioners, replace end of life telecommunications infrastructure, and undertake refresh of end use devices such as computers.

We assessed two options for recurrent infrastructure capex. Option 1 was to actively manage risks by operating infrastructure beyond vendor support or end of life, and taking the risk of managing systems ourselves. Option 2 was consistent with our current practices to refresh infrastructure at the end of vendor support or end of life.

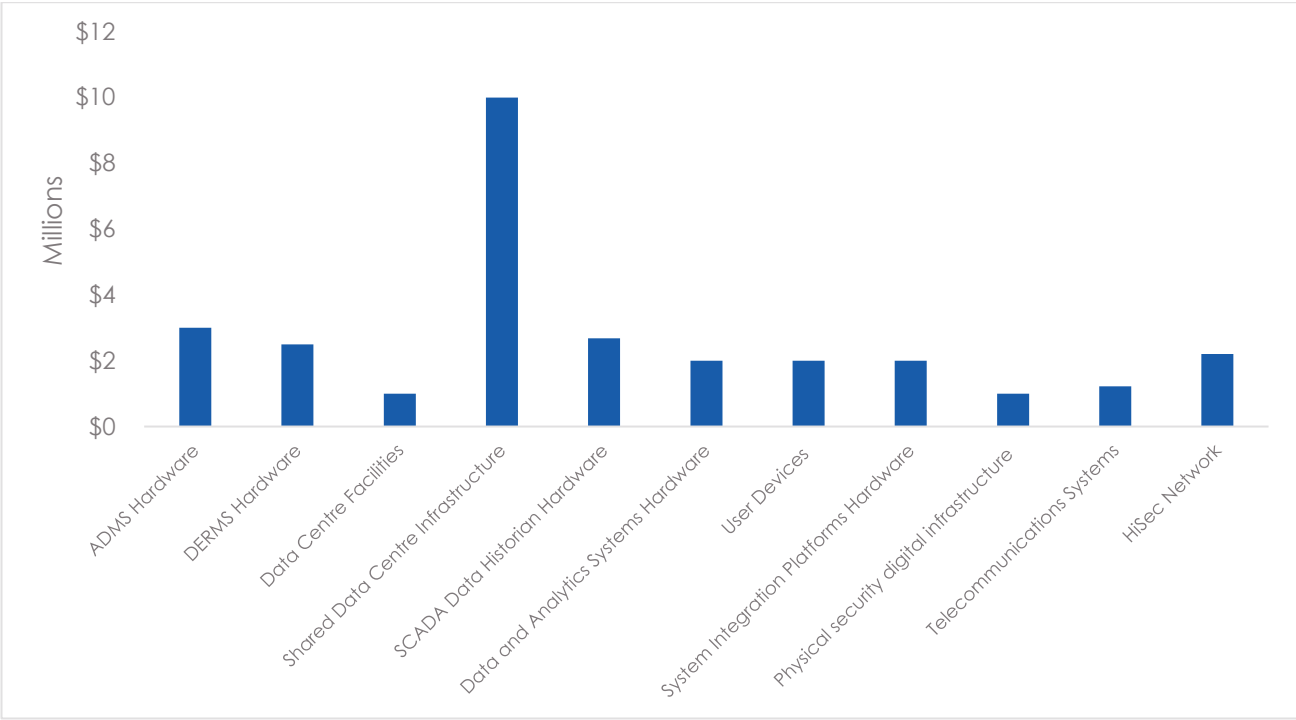
Option 2 was preferred on the basis that it entailed significantly less risk. We also undertook a line-by-line assessment of infrastructure items to confirm the ongoing business need for the infrastructure and whether there were any alternative solutions.

We consider that the expenditure is efficient and prudent because:

- We have settled on an optimal mix of on-premise and cloud ICT infrastructure to support our applications and systems.
- We have identified strategies to fine tune the operation of data centres including the potential for private cloud architecture, and continue to pursue potential efficiencies in end user devices.
- We have a sound procurement process that extracts 'best value' for our investments from vendors in terms of costs and performance.
- In terms of options analysis, we have undertaken risk analysis of options including actively managing risks. We found that the current policy to refresh infrastructure in line with vendor recommendations is the preferred option based on mitigating key risks. We also have undertaken a line-by-line assessment of our ICT infrastructure to assess if there are opportunities to replace on failure or provide current capability through a new system.
- Our forecast capex is remaining consistent despite an increase in demand for compute and storage services for existing applications and systems, demonstrating that we are progressively implementing productivity improvements in infrastructure technologies.

The proposed program for the 2027-31 regulatory period is \$29.6 million (\$ real 2024). **Figure 1** identifies forecast recurrent capex on each infrastructure asset. Shared data centre infrastructure is the most material component, comprising about 40 per cent of the proposed program.

Figure 1 – Proposed capex on current applications infrastructure and systems (\$m, real 2024)



2. Context

Digitalisation has provided an opportunity for AusNet to improve the efficiency of our services, and to provide enhanced customer experience. ICT infrastructure is the foundation of our ICT capabilities providing the necessary processing speed to apply and retrieve data, storage of information, networks to communicate information, and laptops and other end user devices to enable our organisation's work.

ICT infrastructure is a critical enabler of our ecosystem of ICT applications and systems. The applications provide a critical support function to deliver distribution services to our customers reliably and efficiently.

2.1 Categories of ICT infrastructure

The scope of this business case relates to ICT infrastructure on premises used to support our applications and systems. ICT infrastructure includes:

- **Data centre facilities** – Data centres are physical facilities that houses IT infrastructure for building, running and delivering applications and services. We have two data centres on premises in Richmond and Rowville that are used to support the operating technology applications and systems for AusNet's transmission and distribution electricity networks.
- **Servers** – Servers are housed in racks in a data centre. Compute servers provide the necessary computing power and resources to run AusNet's applications and systems for end users. Storage servers provide a centralised location for storing and retrieving information, making it accessible to authorized users from various locations.
- **Network infrastructure** – This includes cables, switches, routers, and firewalls that connect servers to each other and to end-user devices. They enable data movement and connectivity across the system.
- **End user devices** – This includes equipment used directly by our staff to perform their work activities including laptops, mobile and landline phones, field devices and printers. In a modern workplace, this suite of digital tools are required to perform our underlying functions effectively and efficiently. Generally, these assets have a supported life of about 3 to 5 years.

2.2 Drivers of investment

The overarching driver for investment is to ensure our ICT infrastructure is functional and operational to support our applications and systems. Unlike software, ICT infrastructure assets such as servers and network communications are largely generic and, with appropriate virtualisation and management software, can support multiple applications and systems.

We scale our infrastructure to meet the demands for processing and storage for all our applications and systems, purchasing sufficient racks, servers, and communication networks to deliver adequate performance. When we purchase infrastructure from vendors, we generally enter into a maintenance support agreement which effectively provides a warranty for the expected life of the asset. We may be provided with the opportunity to purchase extended support.

At the end of the support period, there is a higher risk that the asset will fail in service. Applications and systems would not be able to operate at required performance until the infrastructure is replaced, ultimately giving rise to significant risks in AusNet's ability to deliver its network and support functions.

Similar to other networks, AusNet seeks to refresh and replace its infrastructure within the support periods offered by vendors, leading to periodic cycles of renewal investment.

2.3 Historical performance

AusNet's ICT management has matured over the last decade. The section "Evolution of ICT at AusNet Services" on page 12 of the ICT Strategy for our 2016-2020 EDPR¹ provides historical background on journey that we were undertaking, with our current proposal Technology Strategy and Investment Plan detailing the next stages that we planned to fully transform the ICT delivery organisation. This is set out in **Figure 2** below

¹ <https://www.aer.gov.au/system/files/AusNet%20Services%20-%20Appendix%207E%20-%20ICT%20Strategy%20-%20April%202015.pdf>

Figure 2 – ICT infrastructure journey

	2006-2010	2011-2015	2016-2020	2021-2025
Business environment	Stable & predictable	Changing	Uncertain and more complex	Major disruption
AusNet IT Theme	Maintain IT	Manage IT	Modernise Business Tools	Enable Business Transformation
Initiatives	<ul style="list-style-type: none"> Support inherited (fragmented) IT environment Limited IT infrastructure consolidation & modernisation 	<ul style="list-style-type: none"> Formal service management IT Infrastructure modernisation Initial IT application modernisation 	<ul style="list-style-type: none"> Finish IT application modernisation Pilot business deployment of new capabilities Retire legacy IT environment 	<ul style="list-style-type: none"> Full-scale rollout of new IT-enabled business model Condition-responsive electricity network management Electricity capex deferral Realtime, optimised electricity business decision making
Benefits	<ul style="list-style-type: none"> Continuity of IT services 	<ul style="list-style-type: none"> Risk-managed IT Secure IT Reliable IT 	<ul style="list-style-type: none"> Flexible IT Controlled IT cost 	<ul style="list-style-type: none"> Controlled business costs Dynamic business environment managed

We are on course to progress this transformation in the current FY2022-26 period, having managed, modernised and evolved our ICT capability in line with established practices over the last 20 years. As a commodity service, infrastructure management is largely a recurrent cost – scaled to meet the increasing performance and data needs of the business. There are limited opportunities to radically transform how we provision the service; rather adjusting and optimising the current model, in particular which business services are delivered on premise and which in the cloud given that AusNet is required to maintain datacentres for its transmission business.

AusNet's ICT infrastructure architecture has evolved with technology improvements and business needs. In the 2016-21 period, we consolidated our ICT infrastructure to two data centres. The decision to host operating technology infrastructure on premises largely relates to the cyber-security needs of our transmission network. It was economical to leverage the data centres to host the infrastructure that similarly supports distribution network applications and systems.

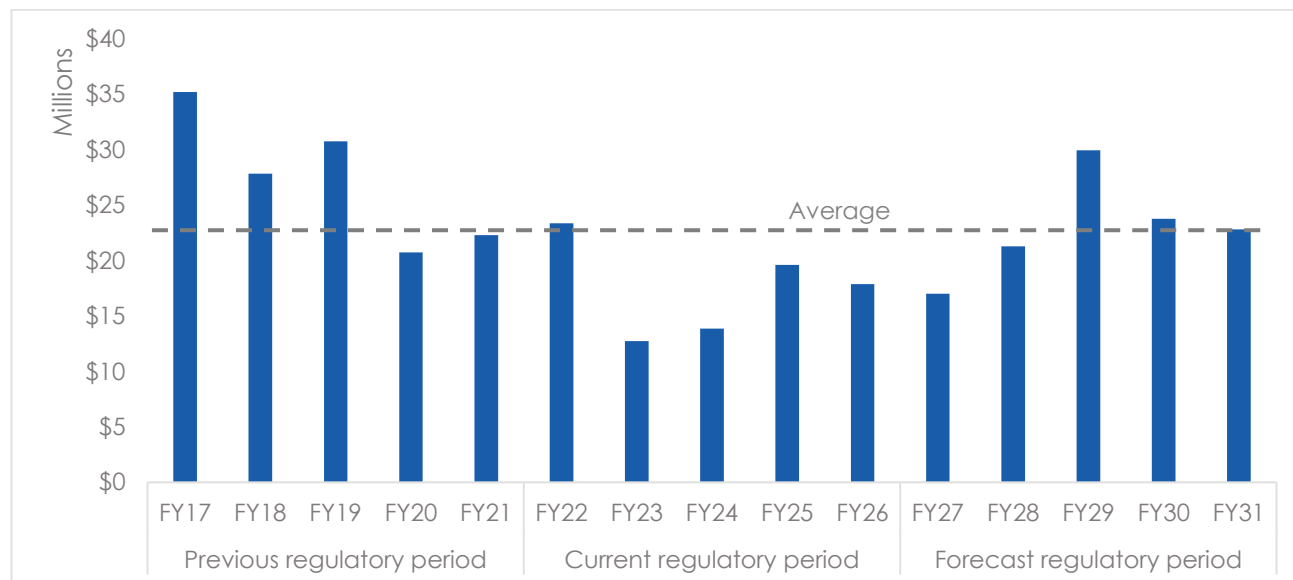
In the 2022-26 proposal we examined options to move infrastructure services to the cloud, in line with broader technology maturity opportunities. Our assessment was that keeping operating technology infrastructure in-house was appropriate for applications and systems that required significant data and processing needs, and minimised risks. However, we found opportunities to move legacy applications to the cloud where demand for these services would reduce over time. In some cases we found that moving data heavy services to the cloud caused latency issues with performance, and we sought to move these back in premises.

As noted in the next section, we consider that our current mix of cloud and on-premises for ICT infrastructure is optimal, and our forecast capital expenditure is focused on refreshing our servers, network equipment and end user devices based on prudent replacement cycles.

2.4 Historical recurrent expenditure

Figure 3 identifies our annual recurrent capital expenditure including applications, infrastructure, metering and cyber security. It shows that annual capital expenditure on updating systems is expected to increase compared to the current period, but is significantly lower than previous periods. We note that the data includes recurrent capex on cyber security, metering and infrastructure that are part of separate business cases.

Figure 3 – Recurrent expenditure on ICT - excluding client devices (\$m, real 2024)



We note that expenditure has declined from the previous regulatory period. In the FY2022 to 2026 regulatory period we completed a program to proactively move to cloud-based products, rather than renewing on premises, where this was assessed as prudent after taking into consideration system criticality and security, and the costs of migration and ongoing opex. Our proposal reflects this revised footprint, with associated lower recurring capex.

However, in the current period we have also implemented a number of significant new services such as Advanced Distribution Management System (ADMS) and Distributed Energy Resources Management System (DERMS). This increased demand in services, with associated infrastructure, will see increase in recurrent capex as currency of these systems is maintained.

With overall recurrent capex remaining relatively consistent over this period, this demonstrates the effectiveness of AusNet's balancing and optimisation between on-premises and cloud implementations, and that AusNet's procurement strategies are enabling us to obtain good value for money from our vendors when acquiring replacement infrastructure and that we continue to keep pace with efficiencies in technologies.

3. Needs identification

The purpose of this section is to identify the forecast methods and components of the proposed recurrent infrastructure capex program, and to demonstrate why it is efficient and prudent.

3.1 Strategy in the 2027-31 period

Our starting point for developing our forecast for the 2027-31 period was to assess whether there were any improvements we could make to the way we manage our ICT infrastructure services.

As noted in Section 2.2, AusNet has optimised its mix of cloud and on-premise infrastructure in the current regulatory period. We have found opportunities to migrate legacy applications and systems to the cloud, where we expect diminishing demand for processing and storage over time. However, our experience is that on-premises infrastructure is necessary to support performance of high demand applications and systems, as migrating these to the cloud creates latency and other performance issues.

In the 2027-31 regulatory period, we will examine ways to fine-tune performance of our data centres by moving towards 'private cloud' architecture arrangements. Currently, AusNet's data centre hosts isolated servers and storage dedicated to specific applications and systems. In turn, this limits opportunities to substitute infrastructure where the need arises. A private cloud enables perfect substitution for servers and storage, and could result in more efficiencies if adequately provisioned and managed. Our budgets for the FY2027-21 period reflect such optimisations of the existing infrastructure.

3.2 Approach to identifying needs

Our Digital and Risk Management policy is to replace components of infrastructure when the support period expires. This is consistent with the general practice of other distribution networks, given the criticality of ongoing support for our applications and systems. We use data analytics however to test whether there are opportunities to keep the asset in service, such as limited use of storage servers, indicating a lower risk of failure. Importantly, we have externally tendered for infrastructure equipment where we consider the lowest lifecycle costs to meet our needs.

Our capital expenditure forecasts for the 2027-31 period are based on operating experience-based assessment of replacement cycles and costs for our existing infrastructure. Granular assessment of infrastructure replacement needs out to 2031 is challenging so far in advance.

Our identification of needs also sought to identify whether there remained a continued business need for infrastructure, with consideration to whether non-recurrent needs may meet the recurrent need. **Table 1** sets out the proposed capital expenditure in the 2027-31 period for ICT infrastructure.

Table 1 – Underlying need for infrastructure (\$m, real 2024)²

System or Application	Description of need	Cost
Shared Data Centre Infrastructure	The 2 data centres require continual refreshes to ensure that storage, servers and other computing equipment provide the necessary support for the current suite of applications and systems.	\$10.0m
Hardware for ADMS, DERMS, SCADA data historian, data and analytics, and system integration platforms.	As per the business case for TAM- Applications, we have identified an ongoing business need for these applications. The hardware is necessary to operate these applications and systems.	\$12.2m
User devices	Cyclical refreshes of laptops, mobiles and other end user devices ensure that our support can securely and efficiently access applications and systems.	\$2.0m
Telecommunications hardware	This includes refreshing and supporting the equipment in the data centres required to communicate between servers and user devices.	\$1.2m
Hi-security network	This involves refreshing the telecommunications network that supports communication.	\$2.2m
Data centre facilities and security	The data centres facilities require necessary capital refreshes including air conditioning and security infrastructure.	\$2.0m

² Refer AusNet EDPR 2027-31 Digital Program NPV Model

4. Options consideration

The purpose of this section is to identify the options we have considered in developing our proposed program of recurrent capex for the 2027-31 period for ICT infrastructure.

4.1. Assessment approach

In developing this business case we have focused on the AER's expectations on the method and approach that should be applied to proposed recurrent ICT expenditure as set out in the AER's guidance note – "Non-network ICT capex assessment approach" of November 2019.

The AER identifies three approaches to assess recurrent expenditure. In terms of bottom-up analysis, the AER recognises that recurrent expenditure relates to maintaining an existing service and that it will not always be the case that the investment will have a positive NPV. It expects that a business case will consider possible multiple timing and scope options of the investments (to demonstrate prudence) and options for alternative systems and service providers (to demonstrate efficiency). The AER also assesses the program as a whole including whether the proposed expenditure varies from historical trends, and benchmarking analysis compared to peer networks.

To give effect to this methodology we undertook the following approach to develop a prudent and efficient program for our existing infrastructure for applications and systems.

- We undertook risk and cost analysis of approaches to updating our infrastructure for current systems and applications. This involved understanding the full extent of the risk of 'doing nothing' relative to the approach of performing lifecycle refreshes (section 4.2)
- We further tested the viability of these two options at granular level relative to the specific infrastructure for each application or system (Appendix A)
- To validate the recommendation of this assessment, we benchmarked the preferred program with the levels of expenditure in the current and prior regulatory periods (as shown in section 2.4)

Note that unlike the Technology Asset Management Applications (TAM Applications) business case, assessment of further alternate options such as full systems re-platforming or refreshing critical operational systems only has not been incorporated. These options are not considered credible for this infrastructure business case, as the cost to completely re-platform all infrastructure would be materially higher and derive no incremental value with infrastructure a homogenous commodity, and current infrastructure primarily supports critical operational systems hence limited opportunity for risk-based prioritisation.

4.2. Risk and cost analysis of alternative strategies

We used risk-cost analysis to determine the optimal strategy for recurrent expenditure on infrastructure as set out in **Table 2**. Option 1 was to actively manage infrastructure without refreshes. Option 2 was to refresh infrastructure in line with vendor recommendations. As detailed in section 4.1, potential third options of full infrastructure re-platform or critical operational infrastructure only refreshes were considered non-credible and hence not included in assessment.

The three risk areas evaluated relative to our risk framework are:

- Increases in system failures, outages and downtime causing delays, inefficiencies and inability to operate and meet customers' expectations from the business.
- Cyber security intrusion into the AusNet environment due to hardware vulnerabilities in the absence of upgrades, patches and bug fixes.
- Critical regulatory requirements are not met, or reporting is delayed, due to system malfunctions or outages.

Table 2 - Options

OPTION	SUMMARY
Option 1: Actively manage existing infrastructure	Operate infrastructure without updates or refreshes and actively manage the risks.
Option 2: Refresh infrastructure in line with vendor recommendations (Recommended option)	Where prudent and efficient, perform updates to infrastructure in line with vendor recommendations.

4.2.1. Option 1 – Actively manage without vendor support

Under this option, we would undertake minimal refreshes and actively manage the risks of operating infrastructure beyond the expected or recommended cycle. This would effectively operate the infrastructure longer than the recommended refresh period. We would actively manage the risks of infrastructure that has failed in service.

There are a number of risks associated with this option, as highlighted in the table below. **Table 3** shows the risk matrix relative 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.

Table 3 - Risk assessment of Option 1

		Consequence				
		1	2	3	4	5
Likelihood	Almost certain	Yellow	Yellow	Orange	Red	Red
	Likely	Green	Yellow	Orange	R1.1, R1.3	Red
	Possible	Dark Blue	Green	Yellow	R1.2	Red
	Unlikely	Dark Blue	Green	Green	Yellow	Orange
	Rare	Dark Blue	Dark Blue	Green	Yellow	Yellow

Legend
A (Red)
B (Orange)
C (Yellow)
D (Green)
E (Dark Blue)

RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
R1.1 Increases system failures, outages and downtime causing delays, inefficiencies and inability to operate and meet customers' expectations from the business	Level 4. Infrastructure supports critical operational systems, with outages impacting network control and ability to respond to operational incidents. Significant scale of impact due to unpredictable and potential cascading dependency outages	Likely	B
R1.2 Security intrusion into the system due to absence of patches and bug fixes on later versions of software	Level 4. Intrusion to critical operational system has potential to broadly impact network control and outage response. Significant scale of impact due to potential breadth of intrusion	Possible	B
R1.3 Critical regulatory requirements are not met, or reporting is delayed, due to system malfunctions or outages	Level 4. Infrastructure supports critical metering and outage management applications, resulting in inability (or significant manual workload) to deliver regulatory requirements	Likely	B

The costs for this option represent an active management approach, with increased opex required to enable greater support resourcing to provide reactive response to anticipated infrastructure issues and failures. Capex investment will still be required to replace failed infrastructure, with costs reflecting a “fun to failure” forecast for the installed infrastructure.³

While relatively lower cost (as per **Table 4**), we consider that overall this option has elevated risk, does not meet the needs of the business and of our customers as a prudent operator, and is therefore not a recommended option.

³ Refer AusNet EDPR 2023-31 NPV Model

Table 4 - Forecast expenditure for Option 1 (\$'million, real FY24)

Cost item	FY27	FY28	FY29	FY30	FY31	Total
Capex	\$2.63M	\$2.36M	\$2.12M	\$2.32M	\$2.41M	\$11.84M
Opex	\$2.17	\$1.95	\$1.75	\$1.91	\$1.99	\$9.77
Total	\$4.80	\$4.31	\$3.87	\$4.23	\$4.40	\$21.61

4.2.2. Option 2 – Perform lifecycle refreshes (recommended option)

This option involves refreshing infrastructure in line with vendor recommendations. Investment will be made consistent with lifecycle recommendations, and support model and arrangements will remain consistent with current operations. This option is recommended due to reducing the likelihood of risk to as low as reasonably practical, and minimising likelihood and consequences relative to Option 1. This can be seen in Table 5 where all risks are rated as D.

Table 5 - Risk assessment of Option 2

		Consequence					Legend
		1	2	3	4	5	
Likelihood	Almost certain	Yellow	Yellow	Orange	Red	Red	A
	Likely	Green	Yellow	Orange	Orange	Red	B
	Possible	Dark Blue	Green	Yellow	Orange	Red	C
	Unlikely	Dark Blue	Green	R2.1, R2.2, R2.3	Yellow	Orange	D
	Rare	Dark Blue	Dark Blue	Green	Yellow	Yellow	E

RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
R2.1 Increases system failures, outages and downtime causing delays, inefficiencies and inability to operate and meet customers' expectations from the business	Level 3. Reduced impact of outages that impact operational systems, with more limited potential for cascading dependency outages, and greater ability for timely response with vendor support	Unlikely	D
R2.2 Security intrusion into the system due to absence of patches and bug fixes on later versions of software	Level 3. Greater ability with vendor support to detect and contain any intrusion to operational systems, thereby reducing impact	Unlikely	D
R2.3 Critical regulatory requirements are not met, or reporting is delayed, due to system malfunctions or outages	Level 3. Reduced impact with required capabilities expected to be maintained, enabling regulatory requirements (potentially with manual workarounds)	Unlikely	D

Cost for this option are shown in Table 5 below, and represent forecast capex for upgrades and replacements of infrastructure at time-intervals consistent with vendor recommendations. No incremental opex is anticipated with this option, as support models remain consistent with current operations.⁴

Based on the risk and cost assessment, we consider that Option 2 is a prudent approach, and is consistent with our ICT policy and customer expectations.

⁴ Refer AusNet EDPR 2027-31 Digital Program NPV Model

Table 5 - Forecast expenditure for Option 2 (\$'million, real FY24)

Cost item	FY27	FY28	FY29	FY30	FY31	Total
Capex	\$6.58M	\$5.90M	\$5.30M	\$5.80M	\$6.02M	\$29.60M
Opex	-	-	-	-	-	-
Total	\$6.58M	\$5.90M	\$5.30M	\$5.80M	\$6.02M	\$29.60M

Appendix A – Line by line assessment




Table 2 – Options analysis for identified systems and applications

Application/System	Option 1	Option 2	Preferred	Why
ADMS – Hardware	Replace on Failure	Maintain within vendor primary and extended support.	Option 2	The high availability and disaster recovery capability that AusNet has negotiated with its key infrastructure service partners reduces the risk of extended support.
DERMS – Hardware	Replace on Failure	Maintain within vendor primary and extended support.	Option 2	The high availability and disaster recovery capability that AusNet has negotiated with its key infrastructure service partners reduces the risk of extended support.
Data Centre Facilities including Security	Replace on Failure	Maintain within vendor primary and extended support.	Option 2	Can result in a complete datacentre failure. Critical systems (ADMS, DERMs, etc) are operating in these datacentres therefore the datacentre facilities should also be classed critical. The high availability and disaster recovery capability reduces the risk of extended support.
Shared Data Centre Infrastructure	Replace on Failure	Maintain within vendor primary and extended support.	Option 2	Some of these systems are consider less critical, however systems with this classification often forgo the other protections such as high availability and rapid disaster recovery. Maintaining vendor extended support reduces the potential and improves the potential restoration time as a result of a hardware failure.
SCADA Data Historian – Hardware	Replace on Failure	Maintain within vendor primary and extended support.	Option 2	The high availability and disaster recovery capability reduces the risk of extended support.
Data and Analytics Distribution Systems (on premise) – Hardware	Replace on Failure	Maintain within vendor primary and extended support.	Option 2	The on-premise data and analytics platform is becoming more critical as it support functions such as Loss of Neutral. A high availability and disaster recovery capability has been applied to this environment which reduces the risk of HW in extended support.
User Devices (laptops, mobile, peripherals)	Replace on Failure	Support mixed model AusNet supplied devices, BYOD and Citrix.	Option 2	The mixed model provide the most flexibility and lowest cost by enabling BYOD where possible. BYOD is extensively used by Digital support partners.
System Integration Platforms – Hardware	Replace on Failure	Maintain within vendor primary and extended support.	Option 2	The high availability and disaster recovery capability reduces the risk of extended support.
High Security Network	Replace on Failure	Maintain within vendor primary and extended support.	Option 2	The redundant paths provide high availability and disaster recovery capability reduces the risk of extended support.
Telecommunications Systems	Replace on Failure	Maintain within vendor primary and extended support.	Option 2	Systems deliver customer communications such as SMS, market regulator interactions and field network control communications. Vendor support maintains reliability of critical capabilities

AusNet Services

Level 31
2 Southbank Boulevard
Southbank VIC 3006
T +613 9695 6000
F +613 9695 6666
Locked Bag 14051 Melbourne City Mail Centre Melbourne VIC 8001
www.AusNetServices.com.au

Follow us on

-  @AusNetServices
-  @AusNetServices
-  @AusNet.Services.Energy

AusNet

