AusNet

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

Business case: Technology Asset Management - Applications

Date: January 2025

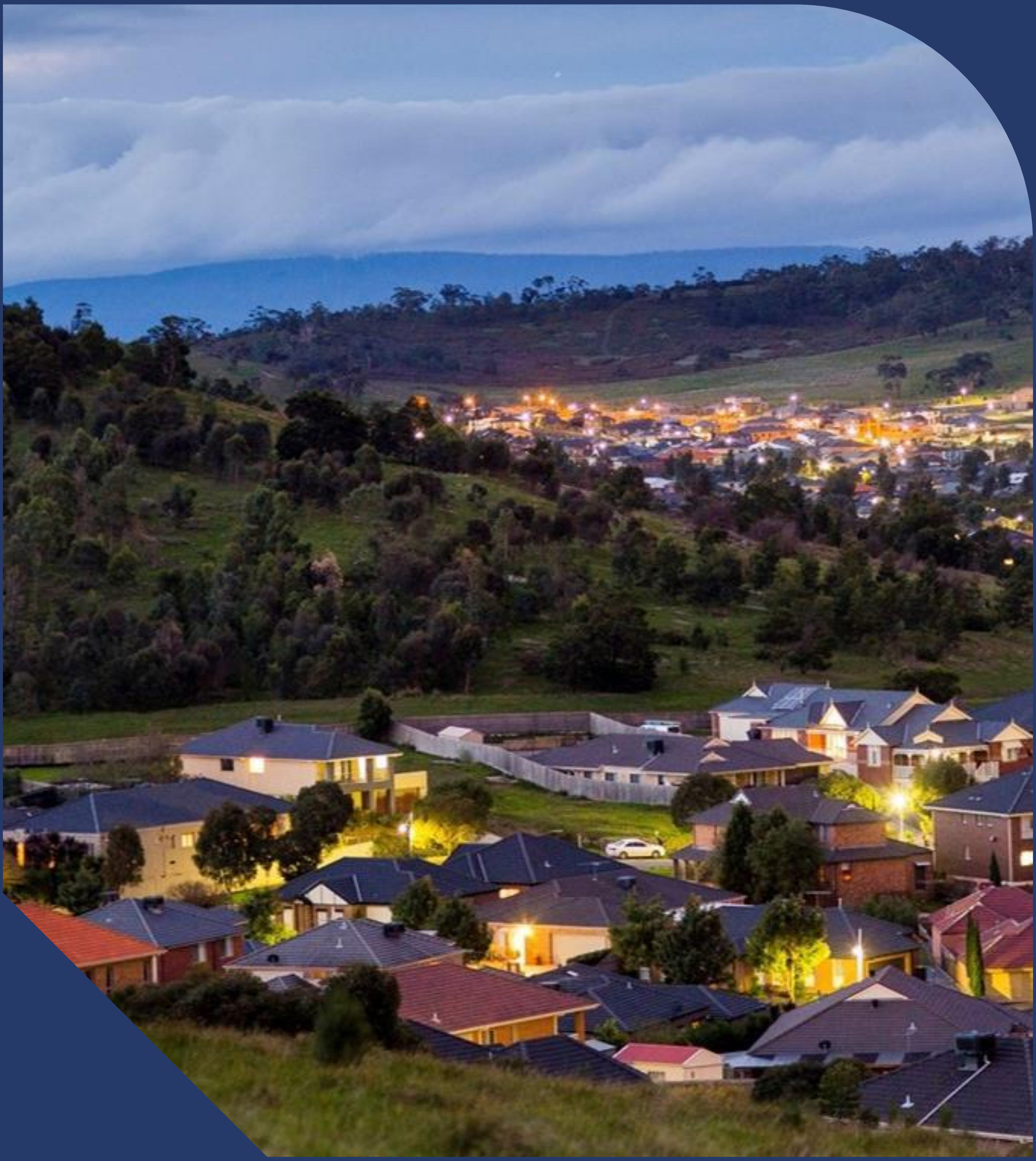


Table of contents

Document history

DATE	VERSION	COMMENT
12/09/2024	V1.0	Initial draft business case for review
22/11/2024	V2.0	Revised business case incorporating input
28/11/2024	V3.0	Updated for final review
30/12/2024	V4.0	Final business case document

Related documents

DOCUMENT	VERSION	AUTHOR
Technology Asset Management (TAM) Infrastructure Business Case	V4.0	AusNet Services
Technology Strategy and Investment Plan	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

AusNet has over 200 technology systems and applications that help us deliver an affordable and reliable distribution network service to our customers. They support key functions such as operating our network safely and reliably, providing customers with information on outages and enabling communications, ensuring network bills are accurate, assisting efficient asset planning, and ensuring our business is run efficiently.

This business case is focused on "Technology Asset Management" (TAM): maintaining the resiliency and existing capability from those technology applications we rely on to deliver Standard Control Services. New capability needs and options are detailed in companion business cases in AusNet's regulatory proposal.

The proposed expenditure is to ensure systems and applications are current and supported, consistent with our ICT and risk management policies. This reflects that technology assets are dependent on support from the product supplier (ie: vendor). Vendors often update their product to reflect changes in the market and will typically not support outdated versions. In the absence of vendor support, the systems and applications are more vulnerable to failing in service and to cyber-security risks.

We have identified needs in the 2027-31 period by undertaking a bottom-up assessment of each of our applications and systems to determine the known or likely timing of vendor updates, patches and bug fixes. Our needs identification tested if the current functionality provided by the application or system was still required to support a business function in the 2027-31 regulatory period.

In terms of options analysis, we applied the following methods to determine the optimal program:

- We undertook risk and cost analysis of options to updating current systems and applications. We identified that 'doing nothing' was inconsistent with our obligations as a reasonable and prudent operator and not credible. We also found that although deferring updates on non-critical systems still exposed us to heightened cyber-security risks, the reduction in costs was minimal. Again, this is not consistent with our reasonable and prudent operator obligations. On that basis we consider that continuing with our current ICT policy to maintain supported applications and systems is a prudent and efficient approach for the 2027-31 period.
- For each application or system, we considered whether there were viable alternative approaches to updating the application or system such as third-party support from alternative providers, moving to a new vendor product, or providing the capability through a new platform in our non-recurrent program. This showed that maintaining current vendor support is most appropriate, given the underlying investment in each application or system.
- As a final step, we sought to benchmark the preferred program with past levels of expenditure in the last two regulatory periods, which showed that investment has remained consistent despite the addition of significant new applications and systems.

The proposed program for the 2027-31 regulatory period is $60.8 million ($ real 2024). **Figure 1** identifies forecast recurrent capex on each application and system. [

CIC

]

[

CIC

]

2. Context

Digitalisation has provided an opportunity for AusNet to improve the efficiency of our services, and to provide enhanced customer experience, where customers are willing to pay for the additional cost. Over the course of the last decade, we have evolved our technology products to meet core functions and have continually scanned the market to provide the best value for money. The purpose of this section is to explain the criticality of ICT assets, the different categorisations we apply, the evolution and journey of our technology ecosystem, and the current approach to supporting our systems.

2.1 Criticality of current ICT assets

Our ICT applications comprise an integrated platform of technology systems and applications that support our network management and corporate functions. We currently operate over 200 ICT applications and systems.

The applications provide a critical support function to deliver distribution services to our customers reliably and efficiently. This includes systems and application that:

- **Operate our network securely and efficiently** – Our real time systems help us manage and control our network to ensure that we can reduce outages and respond to extreme events.
- **Support customer information and accessibility** - Provide important information to our customers through our website including outage tracking, and enable digital communications through customer portals.
- **Efficient management of network assets** – Our applications and systems improve the planning and decisions of our distribution network infrastructure, ensuring that we provide reliable services at least cost to customers.
- **Integrate our customers' solar and batteries securely** – We have invested in applications and systems that enable to us maximise our customer's solar on the network while ensuring the system remains secure.
- **Accurate and timely network bills** – Our billing systems ensure that our customers (mainly retailers and the end-consumers we contract directly with) receive accurate, verified and timely bills.
- **Run an efficient and well-coordinated business** – Our approach to integrate systems ensures that we meet our corporate reporting obligations, and improve our analysis and decisions analytics.
- **Improve safety and environmental outcomes** – We have well developed systems to manage community and worker safety risks and environmental risks.

2.2 Categories of applications and systems

We have categorised our existing ecosystem of systems and applications into two categories based on whether they provide support across our electricity and gas networks (Enterprise Systems), or whether they specifically relate to the electricity distribution network business (Regulated Energy Systems, RES).

Enterprise Systems

These systems operate across our electricity and gas businesses, providing economies of scale. AusNet has invested in systems that enable integration across different functions including asset management, finance, procurement and human resources. The systems enable retrieval and analysis of critical data in a consistent format. The costs of updating these systems are shared across our business, with the allocation to standard control services based on the AER approved Cost Allocation Methodology.

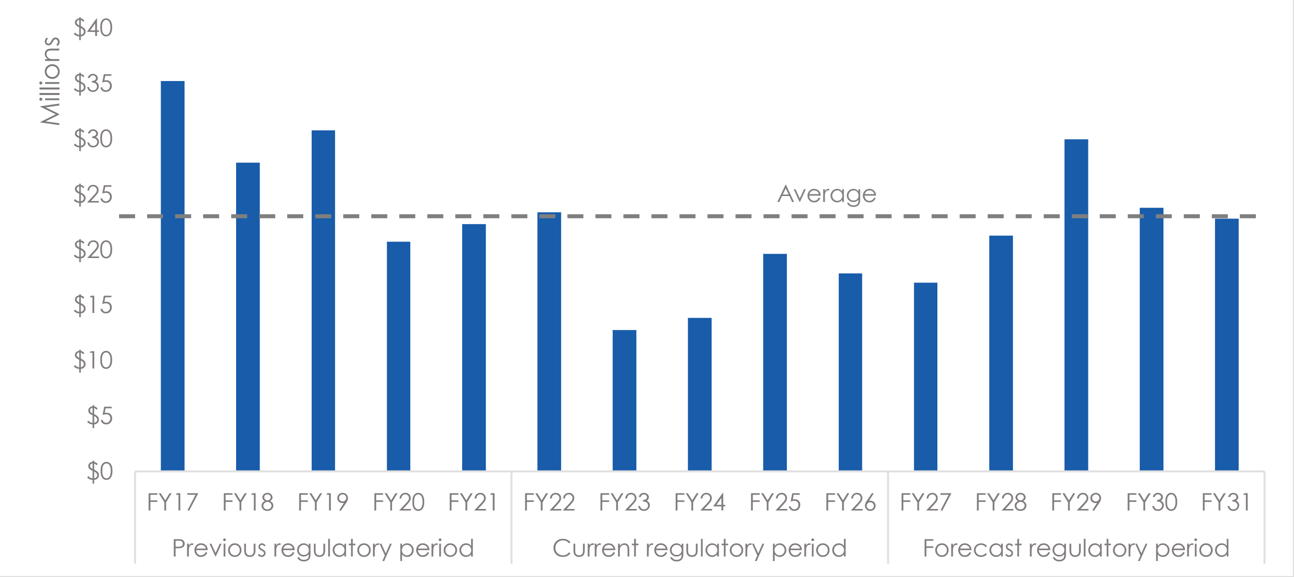
Regulated Energy Services (RES) systems

These systems specifically relate to our electricity distribution network functions. This includes real time network operations and outage management, geospatial systems, drawings management systems, scheduling tools, managing our customer's distribution energy resources and asset planning. The costs of updating these systems are allocated solely to Standard Control Services.

2.3 Historical performance

Figure 2 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 also includes recurrent capex on infrastructure, metering and cyber security that are part of separate business cases.

Figure 1 – Recurrent expenditure on ICT - excluding client devices ($m, real 2024)



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.

In the current period we have continued our simplification strategy by identifying areas where technology can be simplified to reduce complexity and cost by removing waste. This included further reducing data centre footprint and cloud optimisation. While no further focused cloud migration programs are planned in the coming period, we have noted a trend of some vendors to migrate their products to the cloud, requiring transition in order to maintain currency (even if not justified from a cost-benefit basis).

While this work has enabled our recurrent costs to decrease, in the current period we have also implemented a number of significant new applications and systems, including Advanced Distribution Management System (ADMS), Distributed Energy Resources Management System (DERMS), and enhanced customer engagement platforms. Investment to maintain currency of these platforms is included in the proposal. We have also made important updates to our suite of existing applications including [CIC] which is also reflected. Refresh of these material new systems is forecast for the FY2027-31 period.

2.4 Current ICT and Risk Management policies

Our approach to maintaining our application portfolio is governed by our Digital Architecture Policies Standards and Guidelines. Our technology investments are targeted at managing risk and improving value.

AusNet's current approach is to keep applications current by implementing version updates, patches and bug fixes in line with vendor advice on timing. Through the process, we test:

- Whether the underlying business or network need for the application or system remains relevant and suitable for future drivers.
- Whether there are alternative options to updating the current system or application, including third party support from alternative providers, moving to a new product or providing the capability through a new platform in our non-recurrent program.

3. Identified needs

The purpose of this section is to identify the overarching driver of recurrent capex in technology systems and applications, and to pinpoint our approach to identifying investment needs across our suite of technology assets.

3.1 Drivers of investment

The overarching driver for investment is to ensure our current systems and applications retain resilience and currency to reduce the risk that they fail in service or give rise to cyber-security threats. Unlike network assets, technology assets have a short technical life and are much more dependent on the support from the initial supplier (ie: vendor) to provide support and ongoing product updates to address defects or security vulnerabilities. To this end, vendors often update their product to reflect changes in the market and will typically not support outdated versions. In addition, applications and systems require patching and bug-fixes to maintain performance and security.

As such the investment is to maintain existing capability by updating our applications and systems to ensure continued vendor support:

- **Technology applications require vendor support** – Extending the life of technology applications after the vendor end of life date increases business risk as the likelihood of failure to business applications increases. The stability of applications is maintained through application refreshes.
- **Vendors continually update their products** – Vendors periodically release updated versions of their products to ensure they remain current to the market and improve effectiveness over time.
- **Vendors may not provide support for out-dated versions** – It becomes uneconomic for vendors to provide support for outdated applications, due to decreasing customer base. This cost is passed on to the customer and often exceeds the cost of deploying and maintaining new applications.
- **Unsupported systems are more vulnerable to failure and cyber security risks** – Unsupported systems give rise to higher risk of failure and cyber-security vulnerabilities. When applications are no longer supported by a vendor, 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.

3.2 Approach to identifying needs

Our approach to identify needs was to determine the known or likely timing of vendor updates to each of our existing applications and systems. In some cases, we did not have exhaustive bottom-up information on upcoming vendor upgrades given that we are forecasting to 2031. In these cases, we sought to apply an estimate of the likely vendor update cycle which is generally about 5 years.

Our identification of needs also sought to identify whether there remained a continued business need for the application or system. This considered whether the function may be provided through a planned non-recurrent ICT investment.

Table 1 sets out the list of enterprise systems and applications requiring update investments in the 2027-31 regulatory period. We identify the current function, and the vendor product requiring recurrent capex to maintain support.

Table 1 – Enterprise systems and applications requiring recurrent capex in the 2027-31 period

System or Application	Description of current function	Vendor product
Enterprise Resource Planning (ERP)	AusNet uses an ERP to run advanced analytics alongside high-speed transactions across business functions in a single integrated system. This includes finance, human resources, procurement, asset management, and works management.	[CIC]
Customer Systems	Through our website, AusNet provides information to our customers and community including outage tracking. Our customer portals enable customers to connect to our network, make claims and report faults.	[CIC]
Data and Analytics	AusNet uses an on-cloud enterprise data warehouse which aggregates data from many	[CIC]

	different sources into a central and consistent data repository to support data analysis and reporting.	
Network Billing	AusNet uses a network billing system to meet its obligations to bill a customer's retailer based on approved network tariffs and energy usage and those services we contract for directly.	[CIC]
System Integration Platforms	AusNet uses a cohesive set of integration software (middleware) products that enable data exchange and processes between applications. This includes an Application Programming Interface (API) that provides protocols for software applications to communicate with each other. We also use data integration to combine and harmonise data from into a unified, format for analysis.	[CIC]
Health Safety Environment and Quality	Ausnet uses systems to track, monitor and report on Health, Safety, Environment and Quality functions including risk management.	[CIC]
Identity Management	For security purposes, AusNet has a system that enables core identity and access to systems. The system provided functions such as single sign on and two factor authentication for employees and contracts which require access to AusNet systems.	[CIC]
Other business systems	For simplicity AusNet has grouped an array of approximately 50 applications that require minimal expenditure to update. The applications provide capabilities including small engineering and design application, Human Resources, contract assessment, and information management	50 smaller applications and systems

Table 2 sets out the current regulatory energy service systems and applications including their current function, and the vendor product and timing of update.

Table 2 – Regulated Energy Services systems

System or application	Description of current function	Vendor product
ADMS	The Advanced Distribution Management System (ADMS) is AusNet's core operational tool for actively managing the electricity distribution network. The current functionality of the system includes outage management, incident management, and control functions such as switching and restoration. Also supports the call centre function.	[CIC]
Energy Data Management (IS-U)	This is a module in SAP (Industry Solution for Utilities) that is currently used to track connection (NMI) standing data including address and contact details for customers connected to our electricity network.	[CIC]
Low Voltage Analytics Program	AusNet collects data on the performance of the low voltage network from smart meter information including power quality. The information assists with voltage compliance, dynamic voltage management, identifying issues with solar compliance, and identifies loss of neutral.	[CIC]
Distributed Energy Resources Management (DERMS)	AusNet utilises a software platform to manage our customers' rooftop solar to manage supply and demand issues that may have an adverse impact on the security of services. Currently the system is utilised to provide a Solar Emergency Backstop	[CIC]

	when rooftop export levels impact the security of the network. The system will also be utilised for flexible exports and forecasting DER penetration and associated constraints on our network.	
Geospatial Systems	AusNet uses Geographic Information Systems to manage an accurate, comprehensive and integrated geospatial view of the entire network including its characteristics to assist with asset management planning and design	[CIC]
SCADA Data Historian	AusNet utilises SCADA to monitor and control assets on the high and medium voltage sections of its network. The historian is a vital element of the SCADA system that logs and stores data over time and enables us to carry out time-series analysis on network performance.	[CIC]
Engineering applications	Our engineers use a series of engineering tools to plan, design and manage the network. This includes design specifications, drawing tools and computer aided designs, systems setting and calculation tools such as ratings and line impedance, etc.	Various
Telecommunications Systems	AusNet utilises telecommunication systems to communicate performance of assets and to respond to emergencies.	[CIC]
Weather and Solar Services	Ausnet uses applications that provides solar irradiance and weather data from data providers which are integrated into various systems to ensure the reliability and security of the distribution network and for forecasting purposes	[CIC]
Network Access Management	AusNet uses systems that request and authorise access to the network to perform maintenance tasks.	[CIC]
Protection and Control Settings	AusNet uses power system modelling software for secondary protection settings and DFA schemes	[CIC]

4. Options assessed

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 applications and systems.

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 prudency) and options for alternative systems and service providers (to demonstrate efficiency). The AER also assess 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 applications and systems.

- We undertook risk and cost analysis of options to updating our current systems and applications. This involved understanding the full extent of the risk of 'doing nothing' and testing whether an alternative approach of only updating critical systems would be justified on a risk-cost basis (section 4.2)
- For each application or system, we considered whether there were viable alternative approaches to updating the application or system such as third-party support from alternative providers, moving to a new product or providing the capability through a new platform in our non-recurrent program (section 4.3)
- To validate the recommendations of these assessments, we benchmarked the preferred program with the levels of expenditure in the current and prior regulatory periods (as shown in section 2.3)

4.2. Risk and cost analysis of alternative strategies

We used risk-cost analysis to determine the optimal strategy for recurrent expenditure on applications as set out in **Table 3**. Option 1 was to actively manage without vendor support. Option 2 was to undertake our current ICT and risk policy of performing updates and patches to maintain vendor support on all applications and systems. Option 3 was to allow non-critical operating systems to become out of date and without vendor support, but ensure critical systems maintain vendor support, relevant patching and enhancements.

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 system due to absence of patches and bug fixes on later versions of software.
- Critical regulatory reporting is delayed due to system malfunctions or outages.

Table 3 - Options

OPTION	SUMMARY
Option 1: Actively manage without vendor support	Run our existing stock of applications and systems without performing any updates or patching and actively manage consequences in-house
Option 2: Performing updates, patches and bug fixes **(Recommended option)**	Where prudent and efficient, refreshing systems to more current and reliable versions, maintaining vendor support and relevant patching and enhancements
Option 3: Perform lifecycle refreshes of only critical operating systems	Actively manage non-critical systems but allow them to become out of date and without vendor support, while ensuring that critical operational systems maintain vendor support, relevant patching and enhancements.

4.2.1. Option 1 – Actively manage without vendor support

Under this option, we would continue to run our existing stock of applications and systems without vendor support. Management of the system would be undertaken in-house, without any vendor updates or patching, and with reduced knowledge of potential security exposures. We note that cloud applications would continue to be supported by vendors.

There are a number of risks associated with this option, as highlighted in the table below. **Table 4** 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 4 - Risk assessment of Option 1

		Consequence				
		1	2	3	4	5
Likelihood	Almost certain	🟨	🟨	🟧	🟥	🟥
	Likely	🟩	🟨	🟧	🟧 **R1.1, R1.2**	🟥
	Possible	🟦	🟩	🟨	🟧 **R1.3**	🟥
	Unlikely	🟦	🟩	🟩	🟨	🟧
	Rare	🟦	🟦	🟩	🟨	🟨

Legend
🟥 **A**
🟧 **B**
🟨 **C**
🟩 **D**
🟦 **E**

	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. Outages limit end users from conducting their business as usual and slows down the business' ability to respond to operational incidents both internally and externally Significant scale of impact due to unpredictable and potential cascading dependency outages, and extended response without vendor support	Likely	B
R1.2	Security intrusion into the system due to absence of patches and bug fixes on later versions of software	Level 4. Increased risk of intrusion, which will require additional effort from security team to prevent and detect without vendor support	Likely	B
R1.3	Critical regulatory reporting is delayed due to system malfunctions or outages	Level 4. Reporting may be delayed and will require a significantly greater amount of effort	Possible	B

Costs for this option are shown in **Table 5** below. Management of applications in-house, without vendor support, is anticipated to require progressively higher opex, due to growth in the support organisation required to provide response to issues and outages, and to retain knowledge of legacy applications. In this option a level of ongoing capex investment is forecast to be required, to account for application upgrades forced by failures or version dependencies between applications.[1]

While limiting cost, 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.

[1] Refer AusNet EDPR 2027-31 Digital Program NPV Model

Table 5 - Forecast expenditure for Option 1 ($'million, real FY24)

Cost item	FY27	FY28	FY29	FY30	FY31	Total
Capex	$3.04M	$3.82M	$6.45M	$5.42M	$5.58M	**$24.32M**
Opex	$3.03M	$3.96M	$6.13M	$5.28M	$5.41M	**$23.80M**
Total	**$6.08M**	**$7.78M**	**$12.58M**	**$10.70M**	**$10.99M**	**$48.12M**

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

This option involves implementing a lifecycle refresh across each of the system groups detailed earlier. A lifecycle refresh is consistent with AusNet Services' historic approach to maintaining its systems and is also consistent with good industry practice.

This option is recommended due to reducing risk to as low as reasonably practical; 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				
		1	2	3	4	5
Likelihood	Almost certain	🟨	🟨	🟧	🟥	🟥
	Likely	🟩	🟨	🟧	🟧	🟥
	Possible	🟦	🟩	🟨	🟧	🟥
	Unlikely	🟦	🟩	🟩 **R2.1, R2.2, R2.3**	🟨	🟧
	Rare	🟦	🟦	🟩	🟨	🟨

Legend
🟥 **A**
🟧 **B**
🟨 **C**
🟩 **D**
🟦 **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 limit end users from conducting their business as usual and slows down the business' ability to respond to operational incidents both internally and externally. Impact reduced as more limited potential for cascading dependency outages, and more 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. Reduced impact of security intrusion, with reduced vulnerability and greater data security across breadth of applications, plus vendor support to manage detection and response	Unlikely	D
R2.3	Critical regulatory reporting is delayed due to system malfunctions or outages	Level 3. Reduced impact with reporting unlikely to be delayed but will require a greater amount of effort	Unlikely	D

The costs of this option reflect upgrades, patching and refresh of systems in accordance with vendor recommendations, so as to maintain currency and support. Capex costs and timing are assessed on a system-by-system basis, based on known vendor upgrade time-horizons and costs or historic benchmarks where appropriate. Recognising the trend of some vendors to move newer application versions solely to the cloud, the cost of this option includes opex uplift to account for these forced cloud migrations. The total capex and opex costs for this option are shown in **Table 6** below.[2]

We consider that Option 2 is the prudent operating approach, consistent with regulatory and customer expectations, and our risk and ICT policies.

Table 6 Forecast expenditure for Option 2 ($'million, real FY24)

Cost item	FY27	FY28	FY29	FY30	FY31	Total
Capex	$7.61M	$9.55M	$16.13M	$13.55M	$13.96M	**$60.80M**
Opex	$0.52M	$0.81M	$0.81M	$0.81M	$0.81M	**$3.74M**
Total	**$8.13M**	**$10.36M**	**$16.94M**	**$14.36M**	**$14.76M**	**$64.54M**

4.2.3. Option 3 – Perform lifecycle refreshes on critical operational systems only

This option is effectively a hybrid of Option 1 and Option 2. The approach seeks to perform lifecycle refreshes on all critical operating systems such as ADMS and DERMS where there is a direct link to the reliability of electricity services if a failure of the system was to arise. Non-critical systems including enterprise systems or those with secondary impacts to operating systems would be actively managed as per Option 1.

As can be seen from **Table 7**, the risks are less than Option 1, but do not reduce the risk to as low as reasonably practical as per Option 2. Relevantly, the risk of security intrusion is the same as Option 1 reflecting the nature of cyber security risks where attacks can occur from any system that is not up to date (the "weakest link" system). Regulatory reporting risk also remains elevated as this often relies on non-operational enterprise systems.

Table 7 - Risk assessment of Option 3

		Consequence				
		1	2	3	4	5
Likelihood	Almost certain	🟨	🟨	🟧	🟥	🟥
	Likely	🟩	🟨	🟧	🟧 **R3.2**	🟥
	Possible	🟦	🟩	🟨 **R3.3**	🟧	🟥
	Unlikely	🟦	🟩	🟩 **R3.1**	🟨	🟧
	Rare	🟦	🟦	🟩	🟨	🟨

Legend
🟥 **A**
🟧 **B**
🟨 **C**
🟩 **D**
🟦 **E**

	RISK	CONSEQUENCE	LIKELIHOOD	RISK RATING
R3.1	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 limit end users from conducting their business as usual and slows down the business' ability to respond to operational incidents both internally and externally. Impact reduced as more limited potential for cascading dependency outages, and more timely response with vendor support	Unlikely	🟩 D
R3.2	Security intrusion into the system due to absence of patches and bug fixes on later versions of software	Level 4. Increased risk of intrusion from unsupported systems (weakest links), which will require additional effort from security team to prevent and detect without vendor support	Likely	🟧 B

[2] Refer AusNet EDPR 2027-31 Digital Program NPV Model

R3.3	Critical regulatory reporting is delayed due to system malfunctions or outages	Level 3. Reporting that requires non-operational system data may be delayed and will require a significantly greater amount of effort	Possible	C

Table 8 below shows the costs of this option. With non-critical systems not receiving lifecycle refreshes, forecast capex is lower than Option 2. As detailed in Option 1, greater in-house support will be required for these systems, with corresponding opex increase.[3]

While lower cost than Option 2, this option is not preferred due to intolerable level of risks particularly in relation to cyber security.

Table 8 Forecast expenditure for Option 3 ($'million, real FY24)

Cost item	FY27	FY28	FY29	FY30	FY31	Total
Capex	$3.04M	$8.62M	$10.94M	$12.62M	$9.99M	**$45.22M**
Opex	$2.51M	$0.80M	$3.14M	$0.80M	$2.46M	**$9.71M**
Total	**$5.56M**	**$9.42M**	**$14.08M**	**$13.42M**	**$12.46M**	**$54.93M**

4.3. Detailed assessment by application

In addition to testing the strategy to maintain currency of applications, we also examined alternative options to ensure the currency of existing applications and systems but would deliver the required function. Table 7 sets out our options analysis which considers whether third party support providers could provide support, or whether there are other products available.

For each application, the options evaluated are:

- **Approach 1** – Implement an alternate (e.g. third party) non-vendor support arrangement
- **Approach 2** – Continue current arrangements to maintain currency and vendor support
- **Approach 3** – Migrate to an alternate product, typically requiring non-recurrent capex investment, but which may enable product consolidation and alternate support arrangements

This application-by-application evaluation did not identify prudent alternate support arrangements for our vendor-delivered applications (internally developed applications are supported internally). These assessment results, of leveraging vendor support for the existing application portfolio, are incorporated into the recommended Option 2 recurring investment option (Section 4.2.2).

[3] Refer AusNet EDPR 2027-31 Digital Program NPV Model

Table 6 – Analysis of varying support and maintenance approaches for identified systems and applications

Application/System	Approach 1	Approach 2	Approach 3	Preferred	Why
Enterprise Resource Planning (ERP)	External managed service ([CIC])	Maintain [CIC] vendor support	Replace [CIC] with other vendor solution [CIC]	Approach 2	Recently investing in new [CIC] capability [CIC]. Maximise that investment.
Energy Data Management ([CIC])	External managed service ([CIC])	Maintain [CIC] vendor support	Replace [CIC] with other vendor solution [CIC]	Approach 2	Recently investing in new [CIC] capability [CIC]. Maximise that investment.
ADMS	Support internally by extending existing resources.	Maintain [CIC] vendor support	Replace [CIC] with other vendor solutio[CIC]	Approach 2	Recently investing in new ADMS capability. Previous market scan in 2021 resulted in the selection of [CIC]. Maximise that investment. Previous applications issues have required [CIC] SMEs to resolve; building internally the required depth and breadth of knowledge would be challenging.
DERMS	Support internally by extending existing resources.	Maintain [CIC] vendor support	Replace with other DERMS solution.	Approach 2	Recently investing in new DERMS capability for Solar Emergency Backstop. Vendor was selected in 2023, implemented 2024. Maximise that investment. Leverage efficiencies based on vendor roadmap that see future [CIC] DERMS capability more integrated to provide a holistic solution.
Customer Systems	NA - Service based licensing (cloud)	Maintain vendor support	Replace with other solution.	Approach 2	Significant investment has been made in both [CIC]. Recent investment in 2024 following Outage Tracker issues.
Geospatial Systems	Support internally by extending existing resources.	Maintain [CIC] vendor support	Replace with other solution	Approach 2	The core GIS [CIC] is tightly integrated into the [CIC] ADMS [CIC]. Replacement will require significant investment.
Other Business Systems	Support internally by extending existing resources.	Maintain vendor support	Replace with other solutions	Approach 2	Replacement would require significant investment, particularly in replicating current systems integration and data interconnectivity
Data and Analytics (DNA) Distribution Systems (on premise)	Support internally by extending existing resources.	Maintain [CIC] vendor support	Replace with other solutions	Approach 2	Invested in [CIC] in 2024 to perform key functions Dynamic Voltage Management, Solar Compliance, Loss of Neutral. Plan is to further consolidate legacy inhouse analytics platforms into [CIC].

Data and Analytics (DNA) Distribution Systems (cloud)	Support internally	NA	NA	Approach 1	Managed in [CIC] as PaaS and IaaS. DNA leverages [CIC] standard capabilities [CIC]. Migrating to a new cloud service would be very costly. [CIC] will be deprecated over time.
SCADA Data Historian	Support internally by extending existing resources.	Maintain vendor support	Replace other solutions [CIC]	Approach 2	[CIC] contains significant amount of historical data, migration would be costly. Currently deployed on-premise, with cloud solution typically costly due to large data volumes.
HSEQ	Support internally by extending existing resources.	Maintain vendor support	Replace other solutions [CIC]	Approach 2	Safety systems are critical to AusNet's Mission Zero and have recently been refreshed with no lower cost options available in the market currently.
Identity Management	Support internally by extending existing resources.	Maintain vendor support	Replace other solutions [CIC]	Approach 2	Identity management key to meet security objectives. AusNet use commonly supported identity management solution [CIC].
Network Billing	NA (cloud)	Maintain [CIC]	Leverage [CIC]	Approach 2	[CIC]highly functional. Migration to other product would be complex and require significant investment with minimal to no financial benefits.
System Integration Platforms	Support internally by extending existing resources.	Maintain vendor support	Replace other solutions [CIC]	Approach 2	Significant invest has been made in integration platforms, [CIC]. Migration will be costly.
Telecommunications Systems ([CIC])	Support internally by extending existing resources.	Maintain vendor support	Replace other solutions [CIC]	Approach 2	Existing systems highly integrated with network operations systems. Migration would be costly.
Network Access Management	Support internally	NA	NA	Approach 1	Internal custom solutions. Supported and managed internally. No viable vendor products have been identified.
Weather and Solar Services	Support internally	NA	NA	Approach 1	Cloud sourced data integrated into AusNet system via the integration platform and data replication technologies.

Appendix A - Costings

Table 8 sets out the cost estimates for each application or system. This has been based on either the known or estimated costs of maintaining support, consistent with the preferred option in Table 3.

Table 7 – Costings by system or application ($ real 2024)

Initiatives TAM - Applications	CAPEX, total FY27-31
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
[CIC]	[CIC]
TOTAL	**$60,800,000**

AusNet Services

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

Follow us on

@AusNetServices
@AusNetServices
@AusNet.Services.Energy

AusNet