

Technology program

**Technology Asset Management -
Applications (TAM – Apps)**

PUBLIC

Program Brief

Table of Contents

1	Document Background	3
1.1	Purpose of this document	3
1.2	References	3
1.3	Document History	3
1.4	Approvals	3
2	Executive summary	4
2.1	Program summary	4
3	Context	6
3.1	Background	6
3.2	Current limitations	7
3.3	Objective(s)	7
3.4	Technology Risk Drivers	7
3.5	Business drivers	8
4	Options	10
4.1	Overview	10
4.2	Option #1 Maintain current versions	10
4.3	Option #2 Perform lifecycle refreshes (RECOMMENDED)	13
4.4	Option #3 Best in class tools	17
5	Assessment and recommended option	20
5.1	Assessment of the options	20
5.2	Recommended option	20
6	Attachment 1 – Risk level matrix	22

Program Brief

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 EDPR submission.

1.2 References

Document	Version	Author
AusNet Services FY19-FY23 Technology Plan	V1.00	AusNet Services

1.3 Document History

Date	Version	Comment	Person
09/08/18	V0.1	Initial document	Zhao, Yuanyuan
10/08/18	V1.0	Issued for Review	Gottlieb, Zak
14/09/2018	V2.0	2 nd Cycle Final Issue	Gottlieb, Zak
06/03/2019	V2.0a	Benefits updated	Graeme Young
12/03/2019	V2.1	Minor updates	Janine Perri
18/03/2019	V2.2	Consistency edits	John Hancock
20/03/2019	V2.3	Consistency workshop	John Hancock, Tom Lillis, Janine Perri
01/04/2019	V2.4	Minor updates post workshop	Tom Lillis, Dale Alexander, Janine Perri
05/07/2019	V3.0	Cost updates & customer benefits	Emily Pong, Jackson Shen
19/08/2019	V3.1	Post AN review	Emily Pong
15/09/2019	V6.0	Reviewed for FY change Change CLCOE to TAM	Yargi Kilinc
22/10/19	V7.0	Issued for draft to Regulatory team	Samantha Scanlon
18/11/19	V7.1	Incorporated review feedback	Samantha Scanlon

1.4 Approvals

Position	Date
Technology Leadership Team	

Program Brief

2 Executive summary

2.1 Program summary

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

Table 2-1 Summary table

Key objective(s) of the program	AusNet Services has over 200 Technology systems which affect its business. During the next regulatory period, lifecycle management is required for many of these systems.							
Key benefits to customers	This program of work includes performing periodic patching and enhancements to the systems, as aligned to the standard technology lifecycle and to maintain vendor/supplier support.							
Cost allocation	Electricity Distribution	49%			Electricity Transmission	30%		
	Gas Distribution	21%						
Program type	Recurrent				<input checked="" type="checkbox"/>			
	Non-Recurrent				<input type="checkbox"/>			
	Client Devices				<input type="checkbox"/>			
Program timings	Program duration:				5 years			
Expenditure forecast	(\$m)	FY22	FY23	FY24	FY25	FY26	Total	
	Capex	[C-I-C]						
	Opex							
	Electricity distribution cost							
	Total program cost							
Estimated life of system	Lifecycle management typically occurs on a 2 to 5 year timeline							
Customer Engagement	As the first DNSP in Australia to trial the New Reg process, we 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. We acknowledge this feedback							

Program Brief

	and have taken it into consideration when proposing the most appropriate option for this business case.
--	---

A number of systems widely used across AusNet Services (specific systems detailed in the cost estimator) are nearing end of life and require lifecycle refreshes in order to ensure they continue to run as expected and required by the business. This program involves a lifecycle refresh of these systems, where it is prudent and efficient to do so.

The program will ensure that:

- all these critical systems continue to be supported by their vendors, as vendors tend to reduce (and eventually remove) support for legacy systems. Engaging a third-party to provide support can involve significant costs
- the critical systems receive all the latest patches and bug fixes, as cyber security attacks often target known vulnerabilities in current systems so with regular patching and bug fixing, AusNet Services can limit downtime caused by cyber security incidents
- ultimately, AusNet Services can maintain operating efficiency and ensure the continuity and reliability of supply for customers.

The primary objectives for this program of work are outlined below:

- Perform periodic patching and enhancements to the systems, as aligned to the standard technology lifecycle. This is a key component of protecting against cyber security threats.
- Maintain vendor/supplier support
- (With this support) Gain access to the expertise required to resolve incidents
- Access patches for security vulnerabilities and bug fixes
- Limited dependence on customisation, in the absence of vendor support

Alignment to AER ICT expenditure assessment framework

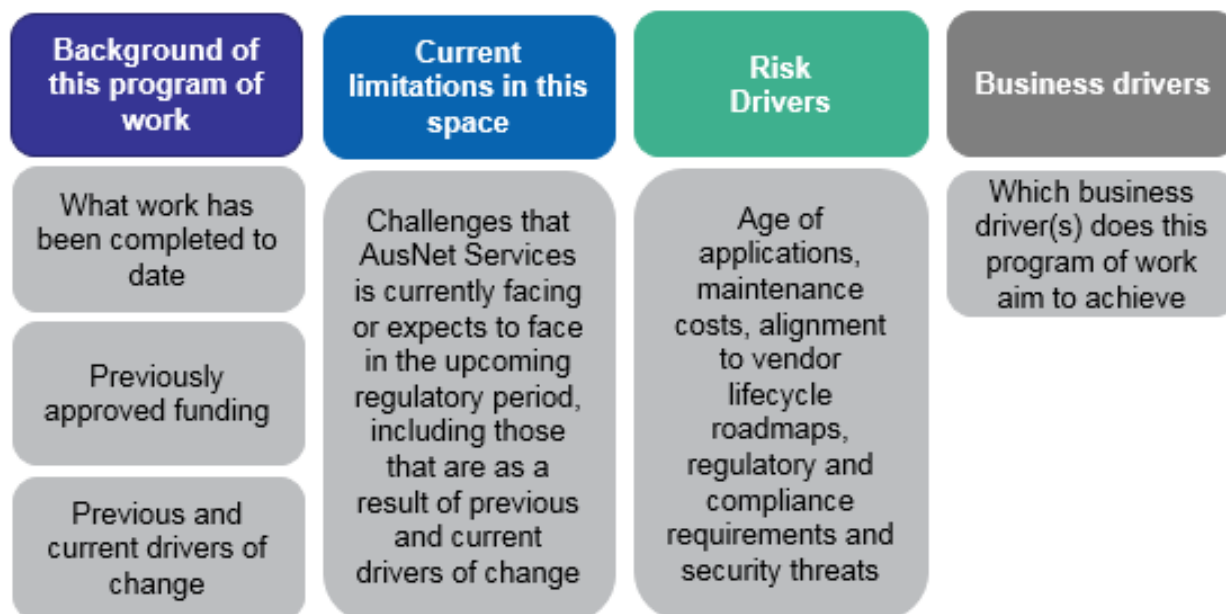
In accordance with the draft framework outlined in the AER's Consultation paper – ICT Expenditure Assessment of May 2019, we have categorised this program as recurrent expenditure, on the basis that it relates to prudent lifecycle management of AusNet Services' Enterprise Systems and Regulated Energy Services (RES) systems. 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.

Program Brief

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

AusNet Services operates over ~200 applications or Technology Systems which affect its distribution business, ranging from critical systems which manage and augment the network, through to standard office tools for everyday tasks such as email. AusNet Services categorises these systems into two major groups:

No	Grouping	Description
1	Enterprise Systems	<p>These systems are designed to integrate multiple areas, systems and internal business portals through the interchange of information from various sources and related databases.</p> <p>These solutions enable AusNet Services to retrieve and disseminate critical data, providing staff with relevant operating information, specific to their given roles.</p> <p>This also includes several tools utilised widely across the business to support operations. These make up the bulk of the ~200 systems including ERP, Corporate Applications, Analytics through to specific systems required to manage and operate the network, call centers, reporting and running all day to day operations at AusNet Services.</p> <p>This group also captures the ERP licensing true-ups each year.</p>
2	Regulated Energy Services (RES) systems	<p>This group includes geospatial systems, drawings management systems, scheduling tools, amongst many other network management solutions.</p>

Program Brief

3.2 Current limitations

A number of critical systems within the groupings outlined which are required for day to day operations at AusNet Services are nearing end of life or require system lifecycle maintenance to ensure operations. Once these applications are out of service, AusNet Services will have no supplier support resolving issues and will need to customise applications to ensure continued operations. In some cases, there are limited options beyond buying very costly extended support.

Failing to patch and refresh these systems will create additional maintenance costs, also putting strain on day to day operations. If these systems are not managed in line with their lifecycle, this will also introduce a significant cyber security risk and minimise the business' ability to leverage modern analytics required to meet customer expectations.

Although there are ~200 applications in use across the business, the focus of this lifecycle investment program (based on size and nature of spend) for the next regulatory period is on the following key systems:

- License true ups across enterprise systems (primarily EAM/ERP)
- Mobility device system refreshes
- Enterprise asset information system
- Commercial and treasury systems
- Drawings management and spatial systems.

3.3 Objective(s)

The focus of this program of work in the forecast regulatory period is to ensure these systems are appropriately maintained. This program of work will perform periodic patching and enhancements to the systems, as aligned to the standard technology lifecycle. By upgrading these systems to more current versions, they will continue to be supported by suppliers, receive maintenance releases, support packs, security corrections and statutory updates. With this support, AusNet Service gains access to the expertise required to resolve incidents, as well as patches for security vulnerabilities and bug fixes as they are available, with limited customisation and ensuring the business meets annual statutory and legal obligations. The proposed expenditure on lifecycle refreshes secure the platforms' support over the forecast period and continue the business' successful efforts to reduce overall 'business as usual' Technology spending.

3.4 Technology Risk Drivers

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

1. **Technology applications risk increases over time.** Application 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 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.
2. **As technology applications age the cost of maintenance increases.** Vendors will provide cost effective support until a point is reached where their costs increase, or services are no

^[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/

Program Brief

longer offered. Vendors need to provide internal capability to support both old and new applications, where the old applications 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 applications.

3. **Regulatory and market compliance.** Vendors will provide statutory and regulatory releases periodically which require structured programs to deliver to ensure compliance.
4. **The price-performance of technology applications continues to improve over time, lowering the total cost of delivering like-for-like services.** Failing to refresh applications locks in higher costs, not only from the applications' vendors but also from service providers, and lower service capabilities to the business.
5. **Security.** Applications are subject to cyber security attacks. Periodic refreshes are required to remove vulnerabilities which allow for unauthorised access leading to major business disruption or loss of critical information. 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. The work covered by the brief includes mission critical systems that support network operations.

3.5 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 three key business drivers which set the direction for the business.

These business drivers are:

- Lead energy transformation, embracing change
- Drive efficiency and effectiveness throughout the portfolio
- Generate trust and respect with customers and partners

We consider that this program of work will be most relevant to '**drive efficiency and effectiveness throughout the portfolio.**' This business driver is achieved by ensuring the continuity of operations at AusNet Services. This research has been further validated through the ICT deep drive presented to the customer forum.

The probable consequences of not maintaining the lifecycle of systems used on a day-to-day basis across the organisation include:

- Increased support costs of customisations to the out-of-support systems;
- Increased frequency of system failure impacting the availability and reliability of the systems, compromising the ability to meet service levels and deliver required outcomes;
- Increased resolution time for critical system defects and incidents; and
- Inability to effectively support asset maintenance and replacement programs of work.

These outcomes would result in significant costs and disruption to the business. This would be both inefficient and drive ineffective working practices, ultimately hampering the business' ability to meet customer's expectations through the forecast regulatory period.

Program Brief

Maintaining patching and enhancement updates in line with the standard technology lifecycle plan will enable the business to continue to operate efficiently and maintain operations in line with regulatory requirements and customer expectations for the continuity and surety of supply:

- Apply resolutions and corrections to known or identified defects and issues;
- Creating the option to commission enhanced system functionality and new capabilities in the future if driven by business need;
- Reduce impact on internal staff to support system maintenance and issue resolution;
- Ensure compatibility of the systems platform
- Rationalise instances of custom code; and
- Ensure resilience against cyber intrusions on more robust and better protected versions of systems.

Program Brief

4 Options

4.1 Overview

This section provides an overview of a select number of options, which may feasibly alleviate the current limitations. Each option represents a combination of initiatives which fit within the program of work.

Table 4-1 Brief overview of the options

Brief overview of each of the options	
Option 1	Maintain current versions – allow systems to become out of date and out of vendor support but perform necessary management to maintain operations.
Option 2 (Recommended)	Perform lifecycle refreshes – Where prudent and efficient, move systems onto more current and reliable versions, maintaining vendor support and relevant patching and enhancements.
Option 3	Best in class tools - Migrate systems to cloud solutions and best in class tools and as-a-service solutions.

4.2 Option #1 Maintain current versions

Under this option, AusNet Services would maintain the current systems, performing no refreshes across each of the major system groupings (Enterprise systems and RES systems).

By not taking any steps to maintain the lifecycle of these systems, the systems would then exit standard support and AusNet Services would be forced to either purchase extended support (which is expensive) or perform support services in-house, and rely on customisations to the solution to resolve defects and develop enhancements.

This option is not recommended due to lack of technical vendor support and increased likelihood of experiencing system performance, stability, data and quality issues. This leads to increased risk of failing to meet business, operational and regulatory requirements. The probable consequences of this option include, growing costs of customisation, increasing frequency of system outages and downtime, limited ability to meet end user service requirements from the system, and growing resolution times when system faults ultimately occur.

Alignment to objectives

The focus of this program of work in the forecast regulatory period is to ensure these systems are maintained, meeting business and operations requirements.

Program Brief

Table 4-2 Objectives analysis of option 1

Objective	Outcome	Detail
Perform periodic patching and enhancements to the systems, as aligned to the standard technology lifecycle	✗	This option does not perform periodic patching and as such does not deliver on this objective
Maintain vendor/supplier support	✗	By not maintaining the lifecycle currency of this system, vendor support will be extremely limited, and costly
(With this support) Gain access to the expertise required to resolve incidents	✗	As software becomes out of date, technicians and personnel with operating experience will become increasingly limited, making incident resolution more challenging
Access patches for security vulnerabilities and bug fixes	✗	Without updates, there will be no access to new patches
Limited dependence on customisation, in the absence of vendor support	✗	Without patches there will be an ever-increasing dependence on customisation to keep systems running

Costs

Table 4-3 Costs of option 1

(\$m)	FY22	FY23	FY24	FY25	FY26	Total
Capex	[C-I-C]					
Opex						
Electricity distribution cost						
Total program cost						

Benefits

This option will provide significant cost savings by limiting spend on system patches and lifecycle refreshes. Although this option would result in a lower cost of maintenance, the significant risks associated with reduced maintenance articulated above outweigh cost saving benefits.

Risks

There are a number of 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 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.

Program Brief

Figure 6-1

		Consequence				
		1	2	3	4	5
L i k e l i h o o d	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

for additional information on this rating system.

Table 4-4 Risks of option 1

	Risks	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 3. Outages limit end users from conducting their business as usual and slows down the business' ability to respond to incidents both internally and externally	Possible	C
R1.2	Security intrusion into the system due to absence of patches and bug fixes on later versions of software	Level 3. Increased risk of intrusion, which will require additional effort from security team to prevent	Possible	C
R1.3	Critical regulatory reporting is delayed due to system malfunctions or outages	Level 3. Reporting will not be delayed but will require a significantly greater amount of effort	Likely	B

We consider that overall, this option has high risk.

Alignment to mitigation of key risk drivers

This option does not address drivers relating to technology risk of aging assets, increasing maintenance costs, regulatory and market compliance and security. Where we consider that a customer outcome is not directly achievable by the option or irrelevant, 'N/A' is applied.

Risk Driver		Achieved by
Application risk increases over time	X	N/A

Program Brief

Cost of maintenance increases as applications age	X	N/A
Regulatory and market compliance	X	N/A
Availability of new applications	X	N/A
Security	X	N/A

Alignment to business related drivers of expenditure

As discussed in Section 3.45, there are three 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 4-5 Business related drivers of option 1

Business drivers	How this program achieves this
Lead energy transformation, embracing change	N/A
Drive efficiency and effectiveness throughout the portfolio	N/A
Generate trust and respect with customers and partners	N/A

4.3 Option #2 Perform lifecycle refreshes (RECOMMENDED)

This option involves implementing a lifecycle refresh across each of the major system groups detailed above. A lifecycle refresh is consistent with AusNet Services' historic approach to maintaining its systems and is also consistent with good industry practice. It will ensure that systems continue to be supported and patching and enhancement updates are maintained in line with the standard technology lifecycle plan. This will enable the business to correct and resolve known defects and issues, through patches and refreshes, as well as gaining access to enhanced system functionality and new capabilities on more current versions of the system. There will also be a reduced requirement for internal staff support to resolve issues and more efficient working practices, through less outages and faster issue resolution. There will be less instances and greater rationalisation of custom code, as well as increased compatibility.

Through implementing this option, AusNet Services preserves these systems which are critical to day to day operations. It also helps the business uphold a high quality and continuity of supply for customers and ensure ongoing operating efficiency.

Alignment to objectives

The focus of this program of work in the forecast regulatory period is to ensure these systems are maintained, meeting business and operations requirements.

Program Brief

Objectives	Outcome	Rational
Perform periodic patching and enhancements to the systems, as aligned to the standard technology lifecycle	✓	This will be delivered by maintaining software prudently in line with lifecycle expectations, ensuring relevant patches are implemented, and enhancements and refreshes as appropriate
Maintain vendor/supplier support	✓	By managing systems in line with their lifecycle, vendor/supplier support will be maintained.
(With this support) Gain access to the expertise required to resolve incidents	✓	As support typically focus on most recent versions, by managing software in line with lifecycle, this objective will be met.
Access patches for security vulnerabilities and bug fixes	✓	This will be delivered by maintaining software prudently in line with lifecycle expectations, ensuring the business gets relevant patches, enhancements and refreshes, as appropriate.
Limited dependence on customisation, in the absence of vendor support	✓	Limited customisation will be required, as systems will be on more current and up to date versions, as appropriate and prudent to do so.

Costs

Table 4-6 Costs of option 2

(\$m)	FY22	FY23	FY24	FY25	FY26	Total
Capex	[C-I-C]					
Opex						
Electricity distribution cost						
Total program cost						

Benefits

We have attempted to estimate the some of the direct financial benefits to AusNet Services (and therefore its customers) of the lifecycle refresh, compared to a business as usual scenario (option 1) using a range of plausible estimates:

Benefit	Dependencies	Estimated savings
Patches and bug fixes resulting in ongoing vendor support and fewer planned outages	Downtime which would have occurred due to unplanned outages is eliminated with bug fixes and this time is used to be more productive	\$2.1m over FY22-26 (reduced downtime of 60 mins a week, impacting 572 employees, 10 unplanned system outages a year, \$72 average hourly rate)
Better and more efficient ways of working on more current versions of software	Newer ways of working will result in better operating practices and increase output for the same work time	\$4.8m over FY22-26 (efficient working saves 30 mins a week, impacting 572 employees, \$72 average hourly rate, 46 work weeks)

Program Brief

Benefit	Dependencies	Estimated savings
Reduction in the need for customisation and greater support costs for out of support systems	Less dependence on customisation, results in a significant reduction in hours required by internal teams to customise systems or work with relevant 3 rd parties to provide this support	\$1.8m over FY22-26 (50 systems requiring customisation, 100 hours per system, \$72 average hourly rate)

Risk mitigation benefits:

If maintenance of these systems is not undertaken then it exposes the AusNet Services business and customers to significant risks that may negatively impact network performance, service delivery, regulatory compliance, customer satisfaction, operational efficiency and cost control.

Examples include:

- System failures that directly affect the continuity of supply of electricity to customers.
- Delays to asset maintenance and asset replacement programs of work.
- Degraded service level performance and/ or customer satisfaction (e.g. increased incident response times and/or an inability to keep customers informed).
- Inability to satisfy regulatory reporting requirements in a timely manner.
- Penalties associated with compliance breaches (e.g. new customer connections).
- Increased vulnerability to security threats and intrusions.
- Increased reliance on customised systems to support business operations and the resultant increase in support costs.
- Loss of vendor support and system specific expertise.
- Inability to access enhanced system functionality that provides more efficient ways of working.
- Exposure to future step function cost increases for system refreshes and replacements.

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 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.

Program Brief

Figure 6-1

		Consequence				
		1	2	3	4	5
L i k e l i h o o d	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

for additional information on this rating system.

Table 4-7 Risks of option 2

	Risks	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. Outages limit end users from conducting their business as usual activities and slows down the business' ability to respond to incidents both internally and externally	Unlikely	D
R2.2	Security intrusion into the system due to absence of patches and bug fixes on later versions of software	Level 3. Increased risk of intrusion, which will require additional effort from security team to prevent	Unlikely	D
R2.3	Critical regulatory reporting is delayed due to system malfunctions or outages	Level 3. Reporting will not be delayed but will require a significantly greater amount of effort	Unlikely	D

As we have identified low risks, we consider that overall this option is rated low.

Alignment to mitigation of key risk drivers

As discussed in Section 3.4, this option is fully aligned in respect to reducing technology risk and providing a stable environment.

Program Brief

Risk Driver		Achieved by
Application risk increases over time	✓	By maintaining critical applications in line with their supplier lifecycle maintenance requirements.
Cost of maintenance increases as applications age	✓	Staying in Vendor application support window is more efficient and cost effective than getting customised vendor support.
Regulatory and market compliance	✓	Maintaining application assets in line with its lifecycle ensures compliance.
Availability of new applications	✓	Obtain efficiency by replacing obsolete technology applications.
Security	✓	Critical lifecycle refresh remedy vulnerabilities and ensure the security and reliability of the network.

Alignment to business related drivers of expenditure

As discussed in Section 3.45, there are three 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 4-8 Business related drivers of option 2

Business drivers		How this program achieves this
Lead energy transformation, embracing change	✓	Refreshing applications can provide a foundation for additional solutions and features to then be available to AusNet Services.
Drive efficiency and effectiveness throughout the portfolio	✓	Refreshing applications will provide stability and operational effectiveness for critical systems.
Generate trust and respect with customers and partners	✓	Operation risks are mitigated. Therefore, continuity and reliability of supply is maintained, which contributes to brand and reputation.

Program Brief

4.4 Option #3 Best in class tools

Option 3 involves the implementation of a new best in class system wherever a lifecycle replacement is required. This option will take a cloud first approach, and wherever possible move to a managed cloud-based solution.

When making lifecycle refreshes, systems will be replaced with software as a service solution (as soon as possible and prudent within the EDPR period), essentially outsourcing the management and maintenance of the system entirely. This would involve replacing the existing system, functionality, data and associated business processes to the new platforms and systems. Significant costs associated with business change management and new ways of working will also be incurred, to avoid disruption to business as usual operations during the transition.

Whilst this would enable AusNet Services to continue to operate at a current version of technology, as well as best in class solutions, this option requires significant investment by AusNet Services to implement. Whilst this may enable the use of new modern features, the disruption and cost would be inconsistent with AusNet Services' strategic objective to 'drive efficiency and effectiveness throughout the portfolio.'

Alignment to objectives

The focus of this program of work in the forecast regulatory period is to ensure these systems are maintained, meeting business and operations requirements.

Objective	Outcome	Rational
Perform periodic patching and enhancements to the systems, as aligned to the standard technology lifecycle	✓	This will be delivered by moving to newest versions of best in class systems.
Maintain vendor/supplier supported	✓	New solutions will all be supported by vendors.
(With this support) Gain access to the expertise required to resolve incidents	✓	Refreshed systems are more likely to have skilled technicians available, however, there is a risk that there may be limited qualified personnel to support the most modern tools, as they may be newer to market.
Access patches for security vulnerabilities and bug fixes	✓	This will be delivered using refreshed versions of all systems as they are moved to their relevant best in class replacement.
Limited dependence on customisation, in the absence of vendor support	✓	Limited customisation will be required, as systems will be on more current and up to date versions across all systems.

Program Brief

Costs

Table 4-9 Costs of option 3

(\$m)	FY22	FY23	FY24	FY25	FY26	Total
Capex	[C-I-C]					
Opex						
Electricity distribution cost						
Total program cost						

Benefits

Benefits for option 3 are the same as those for option 2 with the opportunity for more efficient ways of working as the tools outlined are more modern than those in option 2.

Risks

There are a number of risks associated with this particular 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 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

		Consequence				
		1	2	3	4	5
L i k e l i h o o d	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

for additional information on this rating system.

Table 4-10 Risks of option 3

	Risks	Consequence	Likelihood	Risk rating
R3.1	Increases system failures, outages and downtime causing delays,	Level 3. Outages limit end users from	Unlikely	D

Program Brief

	inefficiencies and inability to operate and meet customers' expectations from the business	conduction their business as usual and slows down the business' ability to respond to incidents both internally and externally		
R3.2	Security intrusion in to the system due to absence of patches and bug fixes on later versions of software	Level 3. Increased risk of intrusion, which will require additional effort from security team to prevent	Unlikely	D
R3.3	Critical regulatory reporting is delayed due to system malfunctions or outages	Level 3. Reporting will not be delayed but will require a significantly greater amount of effort	Unlikely	D

As we have identified low risks, we consider that overall this option is rated low. Unlike option 2, option 3 comes with a major migration from the current environment and introduces additional costs.

Alignment to mitigation of key risk drivers

As discussed in Section 3.4, this option is fully aligned in respect to reducing technology risk and providing a stable environment.

Risk Driver		Achieved by
Application risk increases over time	✓	By maintaining critical applications in line with their supplier lifecycle maintenance requirements. Additionally, there would be a level of application migration to cloud applications.
Cost of maintenance increases as applications age	✓	Staying in Vendor application support window is more efficient and cost effective than getting customised vendor support.
Regulatory and market compliance	✓	Maintaining application assets in line with its lifecycle ensures compliance.
Availability of new applications	✓	Obtain efficiency by replacing obsolete technology applications.
Security	✓	Critical lifecycle refresh remedy vulnerabilities and ensure the security and reliability of the network.

Alignment to business related drivers of expenditure

As discussed in Section 3.5, there are three business drivers that AusNet Services has identified and is focussing on over the next regulatory period FY2022-26. The table below highlights how this option

Program Brief

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 3

Business drivers	How this program achieves this
Lead energy transformation, embracing change	These new modern solutions include the most contemporary tools and solutions on the market, both as a service and cloud-based solutions, and will enable AusNet Services staff to access the most up to date ways of working.
Drive efficiency and effectiveness throughout the portfolio	N/A - More modern tools and solutions will offer new efficient ways of working. However, in this case they will come at a prohibitively high cost, when applied across the board, limiting their ability to deliver on this business driver effectively.
Generate trust and respect with customers and partners	N/A

Program Brief

5 Assessment and recommended option

5.1 Assessment of the options

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

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

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

	Option 1	Option 2	Option 3
Alignment to objectives	[C-I-C]		
Costs			
Overall risk rating			
Alignment to technology risk drivers			
Alignment to business related drivers of expenditure			

5.2 Recommended option

Based on this assessment, Option 2 is the recommended option as it achieves the majority of the intended outcomes for the program at substantially lower cost and without the transition risks associated with Option 3. This option not only reflects the most prudent level of expenditure to deliver the outcomes sought it also limits the business' risk exposure to unplanned critical system downtime. It improves overall security through current patches and updates, whilst maintaining vendor support, limiting the need for the business to depend on costly customisation.

Program Brief

Table 5-2 Confirmation of scope of recommended option

In scope	Out of scope	Dependencies
All systems listed in the cost estimator	Any system or tool not detailed in the cost estimator and supporting documentation	IT Infrastructure, particularly the Infrastructure TAM program, which will serve to host and provide the associated storage requirements for any system covered in this brief
		The cyber security capability developed as a part of the Security Program will underpin the ongoing safety and protection of the systems covered in this brief. Once these systems are in place, any additional security required for the systems will be covered as a part of this brief

Table 5-3 Risk mitigations

	Risks	Rating	Mitigation
R2.1	Increases system failures, outages and downtime causing delays, inefficiencies and inability to operate and meet customers' expectations from the business	D	By implementing option 2, downtime will be limited as outages and down time are less likely on modern more up to date with patched for bug fixes applied to the systems
R2.2	Security intrusion in to the system due to absence of patches and bug fixes on later versions of software	D	Once systems are maintained in line with their lifecycle on option 2, they will receive patches and bug fixes limiting the likelihood of intrusions
R2.3	Critical regulatory reporting is delayed due to system malfunctions or outages	D	On more current versions and patched systems, delays to regulatory reporting caused by system outages will be limited

Program Brief

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

		Consequence				
		1	2	3	4	5
L i k e l i h o o d	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