# Technology program GAAR FY2024-28

**Technology Asset Management – Applications ("TAM Applications")**

missionzero

## Table of Contents

# 1   Document Background

## 1.1   Purpose of this document

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

## 1.2   References

| Document | Version | Author |
|---|---|---|
| **AusNet Services FY19-FY23 Technology Plan** | V1.0 | AusNet Digital |
| **2021 Gas Business Plan** | V1.0 | Joanne Soysa |
| **GAAR Technology Strategy 2024-2028** | V1.0 | Ausnet Digital |
| | | |

## 1.3   Document History

| Date | Version | Comment | Person |
|---|---|---|---|
| **10/01/2022** | v0.1 | Document Created | Sara Taylor |
| **14/04/2022** | V0.2 | Amendments | Mathew Abraham |
| **01/06/2022** | V0.3 | Amended for review | Mathew Abraham |
| **17/06/2022** | V0.4 | Post review amendments | Mathew Abraham |
| | | | |

## 1.4   Approvals

| Position |
|---|
| **Technology Leadership Team** |

## 2  Executive summary

### 2.1  Program summary

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

**Table 2.1 Summary table**

| Key objective(s) of the program | | AusNet has over 200 Technology systems which affect its business. During the next regulatory period, lifecycle management is required for many of these systems.<br><br>This program of work includes performing periodic patching and the necessary enhancements to the systems, as aligned to the standard technology lifecycle and to maintain vendor/supplier support. | | | |
|---|---|---|---|---|---|
| Key benefits to customers | | The top 3 benefits associated with these lifecycle refreshes include:<br>• Ability to apply resolutions and corrections to known or identified defects and issues, through patches and updates.<br>• More current versions of systems will help bring back into balance the internal staff support for system maintenance and issue resolution.<br>• More up to date versions will allow the continued operation of current systems, avoid increasing maintenance costs while also providing the scope for to deploy enhanced system functionality and new capabilities should that be required. | | | |
| **Cost allocation** | Electricity Distribution* | 49% | Electricity Transmission | | 30% |
| | Gas Distribution | 21% | | | |
| **Program type** | **Recurrent** | | | ⊠ | |
| | **Non-Recurrent** | | | ☐ | |
| | **Client Devices** | | | ☐ | |
| **Program timings** | Program duration: | 5 years | | | |

| | ($m) | FY24 | FY25 | FY26 | FY27 | FY28 | Total |
|---|---|---|---|---|---|---|---|
| **Expenditure forecast** | Capex | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $2.71 |
| | Opex (Incl step-change) | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $0.35 |
| | **Gas Distribution cost** | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | **$3.06** |
| | Total program cost | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $22.91 |

## Program Brief

| Estimated life of system | Lifecycle management typically occurs on a 3-5 year timeline. |
|---|---|
| **Customer Engagement** | This program was proposed (and approved) as part of AusNet's Electricity Distribution Price Reset (EDPR) and Transmission Revenue Review (TRR) submissions. This brief pertains to the Gas Access Arrangement (GAAR) allocation of these costs. |
| | We have undertaken significant stakeholder engagement. |
| | As part of the EDPR process, we held deep dive workshops with stakeholders 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. |
| | We acknowledge the feedback received from both sessions and have taken it into consideration when proposing the most appropriate option for this business case. |
| | This brief has also taken into consideration: |
| | • The challenge we received from stakeholders as part of the GAAR engagement process to minimise discretionary IT spend where possible – a challenge consistent with the broader feedback we received on our capital investments. |
| | • Recent customer engagement studies conducted by AusNet, including the Energy Sentiments Survey (2021) and the AusNet Listening Report "Engaging Victorians on the Future of the Gas Networks" (2021). |

A number of systems widely used across AusNet are nearing end of life and require lifecycle refreshes to ensure they continue to run as expected. 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. Vendors tend to move away from providing full support for legacy systems and 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 can limit downtime caused by cyber security incidents.
- Ultimately, AusNet can maintain operating efficiency and ultimately maintain 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.
- Gain access to the expertise required to resolve incidents.
- Access patches for security vulnerabilities and bug fixes.
- Limited dependence on customisation to resolve defects and develop enhancements (where necessary) in the absence of vendor support.

## Program Brief

### Alignment to AER ICT expenditure assessment framework

In accordance with the AER - Guidance Note - Non-network ICT capex assessment approach for electricity distributors - 28 November 2019, we have categorised this program as recurrent expenditure, on the basis that it relates to prudent lifecycle management of AusNet's systems. As such, we have not undertaken NPV analysis in support of the project. However, consistent with AusNet's internal practices, we have developed a detailed business case in support of the chosen option.
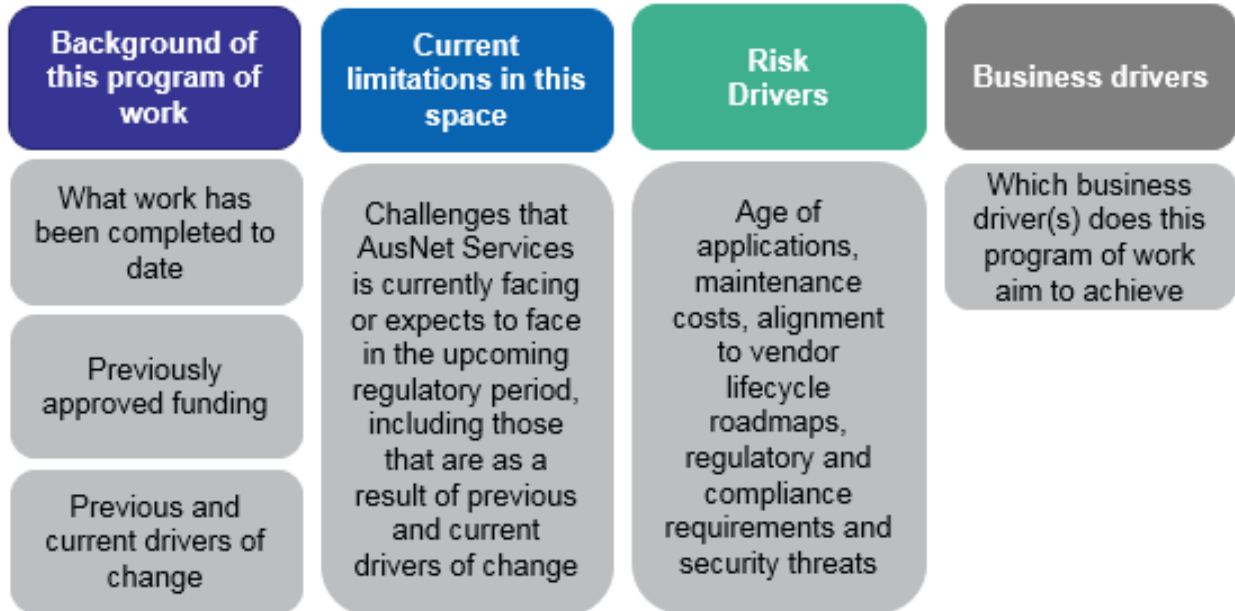
### Accounting Standard changes

The International Accounting Standards Board (IASB) released guidance clarifying how Software-as-a-Service (SaaS) solutions should be treated. Since early 2021, AusNet is no longer able to capitalise implementation costs, including license feeds during development, initial design, configuration, testing, and modification costs associated with SaaS solutions. There are some exceptions to this rule however, generally where AusNet does not have possession of the underlying software, but use it on an as-needs basis, costs will now be attributed to opex only. This is the first regulatory submission under these rules. Where systems are required to be SaaS to maintain vendor support or to mitigate cyber or other vulnerability risks, we have proposed SaaS upgrades moving forward. Therefore, despite shared costs in previous submissions falling under capex, these are now reflected in an opex step-change, while keeping consistent with AusNet's standard allocation. Overall, we have kept the underlying total cost of the program stable.

# 3 Context

This section 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**

| Background of this program of work | Current limitations in this space | Risk Drivers | Business drivers |
|---|---|---|---|
| What work has been completed to date | Challenges that AusNet Services is currently facing or expects to face in the upcoming regulatory period, including those that are as a result of previous and current drivers of change | Age of applications, maintenance costs, alignment to vendor lifecycle roadmaps, regulatory and compliance requirements and security threats | Which business driver(s) does this program of work aim to achieve |
| Previously approved funding | | | |
| Previous and current drivers of change | | | |

## 3.1 Background

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

| No | Grouping | Description |
|---|---|---|
| 1 | Enterprise Systems | These systems are designed to integrate multiple areas, systems, and internal business portals through the interchange of information from various sources and related databases. |
| | | These solutions enable AusNet to retrieve and disseminate critical data, providing staff with relevant operating information, specific to their given roles. |
| | | This also includes 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. |
| | | This group also captures the ERP licensing true-ups each year. |
| 2 | Regulated Energy Services (RES) systems | This group includes geospatial systems, drawings management systems, scheduling tools, amongst many other network management solutions (e.g., SDMg and SCADA). |

## 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 are nearing end of life or require system lifecycle maintenance to ensure continued operations. Once these applications are out of service, AusNet 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:

- Gas specific system upgrades and refreshes.
- 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.

Where migrating to a SaaS solution is required to maintain vendor support, AusNet has done so. With this support, AusNet Services:

- Gains access to the expertise required to resolve incidents.
- Obtains patches for security vulnerabilities and bug fixes as they are available.
- Avoids limited customization.
- Ensures the business meets annual statutory and legal obligations.

The proposed expenditure on lifecycle refreshes secures the platforms' support over the forecast period and continues AusNet's efforts to reduce overall 'business as usual' Technology spending.

## 3.4    Technology Risk Drivers

All Technology Asset Management (TAM) expenditure initiatives identified and proposed by AusNet 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

## Program Brief

'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 longer offered. Vendors, therefore, provide internal capability to support both old and new applications, where the old applications are used by a decreasing customer base.  The cost of providing this level of support is passed on to the customer and often exceeds the cost of deploying and maintaining new applications.

3.  **Industry moves to Cloud and 'As a Service' products that replace previously on premise versions. "**By 2025, Gartner estimates that over 95% of new digital workloads will be deployed on cloud-native platforms, up from 30% in 2021". This move is being driven by the impact of the pandemic and further economic efficiency and sustainability drivers that will continue to serve as a catalyst for digital innovation and the adoption of cloud services.

4.  **Regulatory and market compliance.**  Vendors will provide statutory and regulatory releases periodically which require structured programs to deliver to ensure compliance.

5.  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.

6.  **Security.**  Applications are under ongoing cyber-attack from hackers.  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, therefore, 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 has selected four key business drivers which set the direction for the business.

These business drivers are:

- Maintaining current service performance.
- Updating and implementing recent technologies to enable AusNet to respond to changes due to decarbonisation and alternate fuels introduction.
- Complying with new obligations.
- Delivering improvements requested by our customers regarding sustainability and cost.

We consider this program of work will be most relevant to **'Maintaining current service performance'.** This business driver will be achieved by enhancing capabilities that ensure the

---

[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

continued reliability of the gas distribution business while also laying the foundations to allow for a smoother change to the gas market from the potential introduction of alternate fuels.

The probable consequences of not maintaining the currency 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.
- 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.

Ausnet ensures that it maintains patching and enhancement updates in line with our asset management policies which defines key criteria including business criticality of our application solutions and alignment within our risk appetite with regards to potential asset failure. This enables the business to continue to operate efficiently and maintain operations in line with regulations and customer expectations by:

- Applying 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.
- Reducing the impact on internal staff to support system maintenance and issue resolution.
- Ensuring compatibility of the systems platform.
- Rationalising the instances of custom code; and
- Ensuring resilience against cyber intrusions due to the presence of more robust and better protected versions of systems.

## 3.6    Approach to developing expenditure forecast

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

A full overview of the approach can be found in section 3.2 of the GAAR IT Strategy document.

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

- Needs analysis to identify areas of the network and business processes that require investment over the upcoming regulatory period.

- Bottom-up discussion with business and technology architects and delivery leads to develop options to address the investment need, including scope, key objectives, and drivers influencing the requirement for the programs.

- Consideration of different options to achieve the objectives of the program and analysis of their relative costs, benefits, and risks.

- Top-down view to ensure that the Digital Strategy investment portfolio represents prudent and efficient expenditure for the upcoming period, relative to AusNet's previous expenditure and also benchmarked against other comparable gas distribution businesses.

**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 Overview of the options**

| Option 1 | Business as usual (no new applications or systems, only refreshing as needed). |
|---|---|
| Option 2 (Recommended) | Perform lifecycle refreshes – Where prudent and efficient, move systems onto more current and reliable versions (including SaaS where required), 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 solution. |

## 4.2  Option #1 Business as usual

Under this option, AusNet would maintain the current systems, performing refreshes at a minimum for key systems and dependant on risk or vendor support needs. No new applications across the major system groupings (Enterprise systems and RES systems) would be implemented.

This option would see some systems exit standard support and AusNet would be forced to either purchase extended support (which is expensive) or perform support services in-house and rely on customisations to resolve defects and develop enhancements.

This option is not recommended due to:

- Potential lack of technical vendor support.

- Increased likelihood of experiencing system performance, stability, data, and quality issues.

Both these issues lead 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 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.

**Table 4-2 Objective's analysis of Option 1**

| Objective | Outcome | Detail |
|---|---|---|
| Perform periodic patching and enhancements to the systems, as aligned to the standard technology lifecycle. | ✔ | This option would perform a minimum of periodic patching, which heightens the risk of system degradation. |
| Maintain vendor/supplier support. | ✘ | By not maintaining the lifecycle currency of these systems, vendor support will be extremely limited, and costly. |

## Program Brief

| Objective | Outcome | Detail |
|---|---|---|
| (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 regular updates, there will be limited 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) | FY24 | FY25 | FY26 | FY27 | FY28 | Total |
|---|---|---|---|---|---|---|
| Capex | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $0.62 |
| Opex | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $0.06 |
| **Gas distribution cost** | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | **$0.62** |
| Total program cost | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $2.96 |

### 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.

### Figure 6-1



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 conduction 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 is rated 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 |
|---|---|---|
| | | 14/26 |
| Regulatory and market compliance | X | N/A |
| Availability of new applications | X | N/A |
| Security | X | N/A |

**Program Brief**

**Program Brief**

### Alignment to business related drivers of expenditure

As discussed in Section 3.5, there are four gas distribution business drivers that AusNet 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 |
|---|---|
| Maintaining current service performance. | Business as usual (no new applications or systems, only refreshing current applications). |
| Updating and implementing recent technologies to enable AusNet to respond to changes due to decarbonization and alternate fuel's introduction. | N/A – No uplift from existing capabilities. |
| Complying with new obligations. | N/A – No uplift from existing capabilities. |
| Delivering improvements requested by our customers regarding sustainability and cost. | N/A – No uplift from existing capabilities. |

## 4.3    Option #2 Perform lifecycle refreshes (RECOMMENDED)

This option involves implementing a lifecycle refresh across each of the major system groups detailed above, with a move to SaaS solutions only where required to maintain support. A lifecycle refresh is consistent with AusNet's 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 asset lifecycle policies in alignment of risk appetite policies. This will enable the business to correct and resolve known defects and issues, through patches and refreshes. In addition, due to the nature of the refresh, we will gain 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 be diverted to resolve increasing issues, so less outages and faster issue resolution should occur. There will be less instances and greater rationalisation of custom code, as well as increased compatibility.

Through implementing this option, AusNet 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.

| 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, |

### Program Brief

| Objectives | Outcome | Rational |
|---|---|---|
| | | 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) | FY24 | FY25 | FY26 | FY27 | FY28 | Total |
|---|---|---|---|---|---|---|
| Capex | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $2.71 |
| Opex | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $0.35 |
| **Gas distribution cost** | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | **$3.06** |
| Total program cost | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $22.91 |

### Benefits

We have attempted to estimate direct financial benefits to AusNet (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 FY24-28 For example: 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 FY24-28 For example: efficient working saves 30 mins a week, impacting 572 |

### Program Brief

| Benefit | Dependencies | Estimated savings |
|---|---|---|
| | | employees, $72 average hourly rate, 46 work weeks |
| Reduction in the need for customization 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<sup>rd</sup> parties to provide this support | $1.8M over FY24-28<br>For example: 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 AusNet 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 gas 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 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.

**Program Brief**

**Figure 6-1**



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.

| Risk Driver | | Achieved by |
|---|---|---|
| Application risk increases over time. | ✓ | By maintaining critical applications in line with their supplier lifecycle maintenance requirements. |

**Program Brief**

| | | |
|---|---|---|
| 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 four gas distribution business drivers that AusNet 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 |
|---|---|
| Maintaining current service performance. | Refreshing current applications and upgrading where prudent. |
| Updating and implementing recent technologies to enable AusNet to respond to changes due to decarbonization and alternate fuel's introduction. | Refreshing applications will provide stability and operational effectiveness for critical systems. |
| Complying with new obligations. | N/A |
| Delivering improvements requested by our customers regarding sustainability and cost. | Refreshing applications can provide a foundation for additional solutions and features to then be available to AusNet.<br><br>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 SaaS solutions.

When making lifecycle refreshes, systems will be replaced with 'as a service' solutions (as soon as possible and prudent within the GAAR 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.

While this would enable AusNet to continue to operate at a current version of technology, as well as best in class solutions, this option requires significant investment by AusNet to implement. In addition, while this may enable the use of new modern features, the disruption and cost would contradict AusNet's 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) | FY24 | FY25 | FY26 | FY27 | FY28 | Total |
|------|------|------|------|------|------|-------|
| Capex | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $9.33 |
| Opex | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $0.09 |
| **Gas Distribution cost** | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | **$9.39** |
| Total program cost | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | [C-I-C] | $44.43 |

### 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**



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 | Level 3. Outages limit end users from conduction their | Unlikely | D |

## Program Brief

| | | | | | |
|---|---|---|---|---|---|
| | delays, inefficiencies, and inability to operate and meet customers' expectations from the business. | business as usual and slows down the business' ability to respond to incidents both internally and externally. | | | |
| R3.2 | 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 | |
| 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 four gas distribution business drivers that AusNet 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.

<div align="center">**Table 4-11 Business related drivers of Option 3**</div>

| Business drivers | How this program achieves this |
|---|---|
| Maintaining current service performance | Refreshing current applications and upgrading where prudent. |
| Updating and implementing recent technologies to enable AusNet to respond to changes due to decarbonization and alternate fuel's introduction. | 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 staff to access the most up to date ways of working. |
| Complying with new obligations | N/A |
| Delivering improvements requested by our customers regarding sustainability and cost. | N/A - More modern tools and solutions will offer new efficient ways of working. However, in this case they will come at a prohibitive cost, when applied across the board, limiting their ability to deliver on this business driver effectively |

**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 a number of criteria to assess each of the options. These criteria ensure a comprehensive view of each option's ability to achieve AusNet's business and customer objectives as well as the AER's requirements that expenditure is 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** | Does not achieve objectives | Aligned with program objectives | Aligned with program objectives |
| **Costs ($m)** | $0.61 | $3.06 | $9.39 |
| **Overall risk rating** | High | Low | Low |
| **Alignment to technology risk drivers** | No alignment (1/5) | High alignment (5/5) | High alignment (5/5) |
| **Alignment to business related drivers of expenditure** | No alignment (1/4) | High alignment (3/4) | Medium alignment (2/4) |

## 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 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.

**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 |

| In scope | Out of scope | Dependencies |
|---|---|---|
|  |  | 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 into 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. |

# 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 |