Multinet Gas Networks

Attachment 9.19

IT Business Cases

Final Plan 2023/24 – 2027/28

July 2022

Contents

1 Capex V.22.IT – Apps renewals 4
1.1 Project approvals 4
1.1 Project overview 4
1.2 Background 6
1.3 Risk assessment 10
1.4 Options considered 12
1.2 Summary of costs and benefits 16
1.3 Recommended option 16
Appendix A – Comparison of risk assessments for each option 21
Appendix B – Application lifecycle management 22
Appendix C – Minor system enhancements 23
2 Capex V.23.IT - Infrastructure renewals 24
2.1 Project approvals 24
2.2 Project overview 24
2.3 Background 26
2.4 Risk assessment 28
2.5 Options considered 30
2.6 Summary of costs and benefits 35
2.7 Recommended option 35
Appendix A – Infrastructure categories 38
Appendix B – Comparison of risk assessments for each option 41
Appendix C – Lifecycle management framework 42
3 Capex V.24.IT – AGIG One IT 43
3.1 Project approvals 43
3.2 Project overview 43
3.3 Background 45
3.4 Risk assessment 56
3.5 Options considered 58
3.6 Summary of costs and benefits 65
3.7 Recommended option 65
Appendix A AGIG One IT program 69
Appendix B Uplift Cyber Security Technology and Capability 70
B.1 Initiative overview 70

B.2 Summary of options considered 71
B.3 Proposed solution 74
B.4 Australian Energy Sector Cyber Security Framework 79
Appendix C OneERP 85
C.1 Initiative overview 85
C.2 Summary of options considered 86
C.3 Proposed solution 87
C.4 Summary 89
Appendix D Data architecture, reporting and governance 91
D.1 Initiative overview 91
D.2 Summary of options considered 93
D.3 Proposed solution 93
Appendix E Comparison of risk assessments for each option 98
Appendix F Cost estimates 99
4 Capex V.21.CS – Digital Customer Experience 100
4.1 Project approvals 100
4.2 Project overview 100
4.3 Background 102
4.4 Risk assessment 107
4.5 Options considered 109
4.6 Summary of costs and benefits 116
4.7 Recommended option 116
Appendix A Comparison of risk assessments for each option 121
Appendix B Detailed digital program requirements 122

1 Capex V.22.IT – Apps renewals

1.1 Project approvals

Table 1.1: Project approvals

Prepared by	Cameron Honey, Head of Technology Services
Reviewed by	Kalpna Shukla, Head of Architecture
Approved by	Paul May, Chief Financial Officer

1.1 Project overview

Table 1.2: Project overview

Description of the problem / opportunity	Multinet Gas Networks Limited (MGN) maintains and operates a suite of Information Technology (IT) and Operational Technology (OT) applications that are integral to the efficient and effective management of the gas network and are required to meet a range of legal and regulatory obligations. The applications renewal and upgrades program of work is necessary to safeguard these business-critical applications by ensuring they are updated and maintained appropriately. This project involves systematically upgrading applications over the next (2023 to 2028) access arrangement (AA) period. The key objectives of this project are to: • continue to maintain reliable, secure, compliant and efficient business processes and systems; • continue to obtain vendor support for software and applications that enable MGN business operations; • preserve the ongoing integrity of MGN's data and services; and • enable MGN to continue to comply with a range of regulatory and other obligations. The key benefits of this project are to substantially reduce the risk of system failures or integration between systems not working as required, and maintaining the required levels of data security and integrity.
Untreated risk	As per MGN risk matrix = **High**
Options considered	• **Option 1** – Replace on failure/technical obsolescence ($0 million upfront) • **Option 2** – Upgrade and maintain applications on a regular basis, consistent with good industry practice, manufacturers' recommendations, and our application lifecycle management plan ($17 million)
Proposed solution	Option 2 is the proposed solution and is recommended as the most cost-effective way of mitigating the risks posed by outdated and unsupported applications. It involves implementing a lifecycle management plan for all applications to maintain a modern, fit-for-purpose suite of applications that enable and support MGN business operations. This is consistent with good industry practice and manufacturer's recommendations. The project will mitigate the risks associated with retaining outdated and unsupported applications as follows.

<table>
<tr><td></td><td>

People – high risk of outdated or inaccurate data held in legacy systems relating to the location or operation of gas assets that may lead to injuries to contractors or members of the public;
Supply – high risk of increased frequency of system outages that may disrupt MGN business operations or system problems that cannot be resolved;
Reputation – high risk of reputational damage to MGN by not maintaining up to date and fit for purpose technology solutions for employees, customers, retailers, regulators and other MGN stakeholders;
Financial – high risk of increased costs to maintain legacy systems using outdated and unsupported technology, or in the event of failure, expensive system recovery activities; and
Compliance – high risk of not being able to efficiently meet current and future compliance obligations if technology solutions are not maintained or updated.

Option 1 is not recommended as MGN would incur significant additional operational expenditure to keep legacy, unsupported applications, or in the event of failure, to recover systems and data. It does not mitigate the risks associated with retaining legacy and unsupported versions of critical applications in a timely manner to allow the MGN business to operate effectively.
</td></tr>
<tr><td>Estimated cost</td><td>
The forecast direct capital cost during the AA period (July 2023 to June 2028) is $17 million.
<table>
<tr><th>$'000 real 2021</th><th>2023/24</th><th>2024/25</th><th>2025/26</th><th>2026/27</th><th>2027/28</th><th>Total</th></tr>
<tr><td>Capex</td><td>2,287</td><td>4,427</td><td>2,986</td><td>3,850</td><td>3,658</td><td>17,208</td></tr>
</table>
Tables may not sum due to rounding
</td></tr>
<tr><td>Basis of costs</td><td>All costs in this business case are expressed in real unescalated dollars at June 2021 unless otherwise stated.</td></tr>
<tr><td>Alignment to our vision</td><td>
This project aligns with the Delivering for Customers aspect of our vision by ensuring MGN technology systems supporting customer services are adequately maintained and available to meet their needs.

This project aligns with our vision objective of being A Good Employer, as it aims to provide employees and third-party users of MGN systems with current, reliable, accurate and fit-for-purpose technology solutions that allow the business and its contractors to operate effectively.

This project aligns to our vision to be Sustainably Cost Efficient as the project will execute a lifecycle management plan that follows good industry practice and manufacturer's recommendations, mitigates risks, optimises capital and operational expenditure and minimises application support costs.
</td></tr>
<tr><td>Consistency with the National Gas Objective and Rules (NGO and NGR)</td><td>
This project complies with the following National Gas Rules (NGR):

NGR 79(1) – the proposed solution is consistent with good industry practice, several practicable options have been considered, and market rates have been tested to achieve the lowest sustainable cost of providing this service.

NGR 79(2) – proposed capex is justifiable under NGR 79(2)(c), as it is necessary to maintain and improve the safety of services, maintain the integrity of services, and comply with regulatory obligations as follows:

maintain and improve the safety of services (rule 79(2)(c)(i)) - the safety of services will be adversely affected if there is a security breach and/or any of the critical IT systems fails;

</td></tr>
</table>

	• maintain the integrity of services (rule 79(2)(c)(ii)) - the integrity of the services will be adversely affected if critical systems are unavailable; and • comply with a regulatory obligation or requirement (rule 79(2)(c)(iii)) – the project mitigates the risk of a breach of regulatory obligations (e.g. Retail Market Procedures requirements for processing timeframes) if key systems are not available or customer data is compromised. **NGR 74** – the forecast costs are based on the latest market rate testing and reflect the lifecycle management and estimation approach described in the IT Plan. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.
Treated risk	As per risk matrix = **Low**
Stakeholder engagement	We are committed to operating our networks in a manner that is consistent with the long-term interests of our customers. To facilitate this, we conduct regular stakeholder engagement to understand and respond to the priorities of our customers and stakeholders. Feedback from stakeholders is built into our asset management considerations and is an important input when developing and reviewing our expenditure programs. Our customers have told us their top three priorities are price/affordability, reliability of supply, and maintaining public safety. They also told us they expect us to deliver a high level of public safety and are satisfied that this is the current practice. This program is designed to ensure the network operates in line with good industry practice and standards, and enables compliance, thereby helping to maintain a safe and reliable service to our customers. The proposed solution to maintain our assets in good working order will also help to maintain the reliability of gas supply at the lowest sustainable cost.
Other relevant documents	• Attachment 9.9 IT Investment Plan

1.2 Background

The MGN network delivers gas to over 700,000 consumers. To enable the efficient and effective management of the network, and provision of services to our customers, we maintain and operate a suite of Information Technology (IT) and Operational Technology (OT) applications. These applications also enable us to meet a range of legal and regulatory obligations, including those prescribed in the:

- the National Gas Law (NGL) and National Gas Rules (NGR);
- the Victorian Gas Distribution System Code[1];
- the Victorian Gas Industry Act 2001[2];
- the Victorian Retail Market Procedures[3] (RMP) (see Box 1.1); and
- Energy Safe Victoria's (ESV's) gas and pipeline safety requirements[4].

Box 1.1: MGN's obligations under the Retail Market Procedures

In accordance with Section 1.2 of the Retail Market Procedures, the Australian Energy Market Operator (AEMO) established a Gas Interface Protocol (GIP), which governs the manner and form in which information is to be

1 Essential Services Commission, "*Gas Distribution System Code*", Version 11.0.
2 http://www.austlii.edu.au/au/legis/vic/consol_act/gia2001167/
3 AEMO, http://www.aemo.com.au/Gas/Policies-and-Procedures/Retail-Gas-Market-Procedures/Victoria
4 http://www.esv.vic.gov.au/About-ESV

provided, notice given, notices or documents delivered and requests made as contemplated by the RMP. Further, Section 1.2.4 of the RMP states that MGN is:

- "bound by, the Gas Interface Protocol in respect of the provision of information, giving of notice, delivery of notices or documents and making of requests, and the receipt of information, notice, notices, documents or requests, as contemplated by these Procedures."; and
- "any failure to use the FRC HUB in accordance with the FRC HUB Operational Terms and Conditions may result in MGN being issued a breach notice."

If the breach is found by AEMO to be material, it must be referred to the AER under section 91B of the NGL. This provision in the NGL is a civil penalty provision, which means that the AER can issue an infringement notice[5] and/or **institute civil proceedings** in the Federal Court and seek an injunction or an order that MGN remedy the breach; and/or an order that a penalty be paid.[6]

In addition, Participant Build Pack 3 - FRC B2B System Architecture Section 6, specifically addresses security noting "An Internet based message service, by its very nature, presents certain security risks… Beyond the requirements herein, participants should make themselves familiar with these risks and institute countermeasures balanced against an assessment of the inherent risks and the value of the asset(s) that might be placed at risk."

To maintain the integrity and availability of the technology services upon which our services depend, MGN must continue to maintain and upgrade its suite of applications with current and supported versions. This is particularly important considering the ever-increasing complexity, integration and customer facing nature of technology systems that drive operational efficiencies and business effectiveness.

As a prudent operator, MGN has ongoing maintenance plans for its applications to ensure:

- maintenance of the current levels of technology services by continuing to maintain reliable, secure, compliant and efficient business processes and systems;
- preserving the ongoing integrity of MGN data and services;
- mitigating risks associated with MGN's core business systems; and
- continued compliance with MGN's legislative and regulatory obligations under the various instruments set out above, including the RMP[7].

Software patches and version upgrades are provided by manufacturers, who recommend that their technology be upgraded to ensure continued provision of ongoing support and maintenance and that any known issues including security vulnerabilities are addressed. These upgrades are required to manage the transition of one version of the technology to a subsequent improved version of the technology, correct defects in the technology (which includes how a technology type interacts with other technology types) and attend to security concerns.

Generally, an application upgrade will involve not only the application upgrade itself, but also upgrades to the underlying associated technology platform components, assessment, design and implementation of any changes to configuration, customisations and integrations associated with the upgrades and complete testing of all impacted end-to-end processes.

---

5 The maximum infringement notice is $4,000 for individuals ($20,000 for body corporates).

6 The maximum civil penalty is $20,000 for individuals ($100,000 for body corporates), plus $2,000 ($10,000) for every day it continues.

7 AEMO, "*Retail Market Procedures (Victoria)",* Document No: PROJECT-57-30 Version No: 10.0, 14 Sep 2015, http://www.aemo.com.au/Gas/Policies-and-Procedures/Retail-Gas-Market-Procedures/Victoria

Software application assets are usually upgraded on a two to three-year cycle[8] depending on the assets and the policies of the vendors for the frequency of upgrades. The application of version upgrades to critical business systems every two to three years is good industry practice as vendors typically provide at least one major and several minor upgrades or patches over that period. There exists interdependencies between the various software applications, which are integrated to support business requirements. This interdependency creates a working construct of software applications, and associated technology platform components, that are at risk if they are not maintained at compatible software release levels as prescribed by technology vendors. The interoperability of disparate applications must be constantly monitored in order to have visibility of potential incompatibilities. The application of version upgrades through a quality-based testing regime mitigates any risks associated with this issue.

To ensure that the application systems are kept stable, secure and at optimum performance, MGN utilises an application lifecycle management methodology to determine upgrade timelines and priorities. This enables appropriate levels of operation, data integrity and inter-operability between various vendor provided technologies. The Application Upgrade Plan is in place as a stay in business program of work that ensures compliance with an underlying principle of staying at a minimum of N-1[9] for application upgrades. The alignment with industry practice of N-1 ensures ongoing vendor support and mitigates the risk of security breaches, system outages and potential regulatory non-compliance. MGN's application lifecycle management methodology is provided in Appendix B.

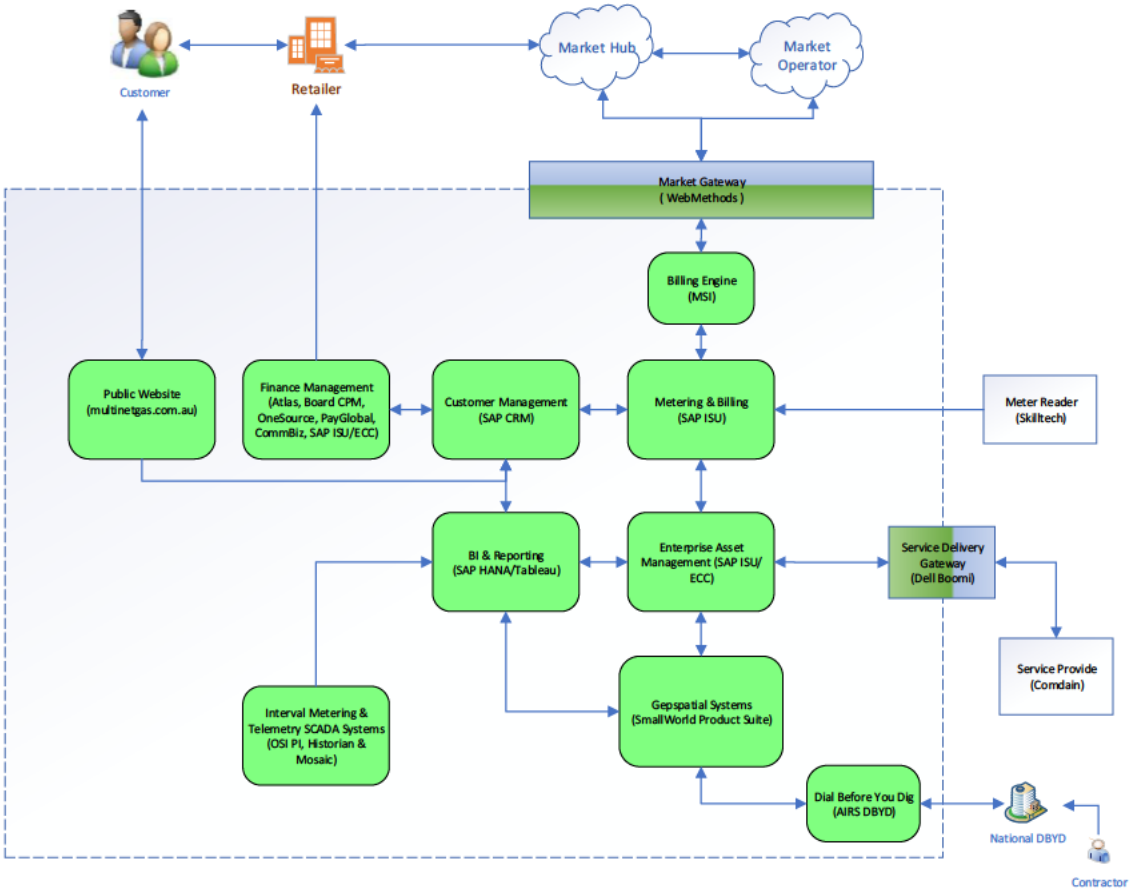
1.2.1 MGN's application environment

Figure 1.1 outlines the MGN application environment and the high level of integration between core systems.

[8] ServiceNow and OSI Pi technology upgrades have been identified as an exception to the applied 2-year cycle of application upgrades. The rapid change in technology cycle and the ongoing speed of change for these applications indicates that a yearly upgrade cycle is a prudent approach in this area.

[9] N-1 Refers to the specific software version number, which is associated with a specific vendor software. Where "N" representing the current version of the released and supported software, whereas -1 would refer to an older version of the same vendor software which would still be supported. Upgrade versions are provided by vendors who recommend that their technology be upgraded to ensure ongoing support and maintenance contracts.

Figure 1.1: MGN's application environment



In the current AA period, a number of major projects to upgrade key applications were completed. These projects delivered improved applications, providing increased scalability, flexibility and reliability, while also ensuring that MGN continues to meet relevant regulatory and customer obligations. The program has so far successfully delivered a variety of key system enhancements, including major upgrades to GIS and EDMS, new mobility capability, AEMO mandated schema changes in support of new market transactions for Life Support customers, along with establishing foundation platforms to leverage efficiencies in business operations through data centre consolidation, enablement of standard processes and task automation. The ultimate beneficiaries of these improvements are our customers.

Applications renewal is an ongoing process, which means upgrades to these, and other systems must continue over the next AA period. During the next AA period (July 2023 to June 2028), several critical IT systems are due to be upgraded. These are:

- Geospatial Information System
- EDMS (Meridian)
- Service Now Consolidation
- Network Viewer
- Public Websites
- S/4 HANA (MGN allocation)
- Smart Metering
- WebMethods

- MSI Replacement
- OSI Pi; and
- Small applications, minor works and system enhancements

This business case considers the costs and benefits of continuing with our current proactive applications upgrade strategy, or reverting to a reactive replace on obsolescence/failure approach.

1.3 Risk assessment

Risk management is a constant cycle of identification, analysis, treatment, monitoring, reporting and then back to identification (as illustrated in Figure 1.2). When considering risk and determining the appropriate mitigation activities, we seek to balance the risk outcome with our delivery capabilities and cost implications. Consistent with stakeholder expectations, safety and reliability of supply are our highest priorities.

Figure 1.2: Risk management principles

Our risk assessment approach focuses on understanding the potential severity of failure events associated with each asset and the likelihood that the event will occur. Based on these two key inputs, the risk assessment and derived risk rating then guides the actions required to reduce or manage the risk to an acceptable level.

Our risk management framework is based on:

- AS/NZS ISO 31000 Risk Management – Principles and Guidelines,
- AS 2885 Pipelines-Gas and Liquid Petroleum; and
- AS/NZS 4645 Gas Distribution Network Management.

The Gas Act 1997 and Gas Regulations 2012, through their incorporation of AS/NZS 4645 and the Work Health and Safety Act 2012, place a regulatory obligation and requirement on MGN to reduce risks rated high or extreme to low or negligible as soon as possible (immediately if extreme). If it is not possible to reduce the risk to low or negligible, then we must reduce the risk to as low as reasonably practicable (ALARP).

When assessing risk for the purpose of investment decisions, rather than analysing all conceivable risks associated with an asset, we look at a credible, primary risk event to test the level of investment required. Where that credible risk event has an overall risk rating of intermediate or higher, we will undertake investment to reduce the risk.

Six consequence categories are considered for each type of risk:

1 **People** – injuries or illness to employees and contractors or members of the public

2 **Supply** – disruption in the provision of services/supply, impacting customers

3 **Environment** (including heritage) – impact on the surroundings in which the asset operates, including natural, built and Aboriginal cultural heritage, soil, water, vegetation, fauna, air and their interrelationships

4 **Reputation** – impact on stakeholders' opinion of MGN/AGIG, including personnel, customers, investors, security holders, regulators and the community

5 **Financial** – financial impact on MGN/AGIG

6 **Compliance** – the impact from non-compliance with operating licences, legal, regulatory, contractual obligations, debt financing covenants or reporting / disclosure requirements

Note that risk is not the sole determinant of what investment is required. Many other factors such as growth, cost, efficiency, sustainability, and the future of the network are also considered when we develop engineering solutions. The risk management framework provides a valuable tool to manage our assets, and prioritise our works program, however it is not designed to provide a binary (yes/no) trigger for investment. As prudent asset managers, we apply our experience and discretion to manage and invest in our distribution networks in the best interests of existing and potential customers.

A summary of our risk management framework, including definitions, has been provided in Attachment 9.5.

The primary risk event being assessed is that as IT applications age, it becomes increasingly difficult to address security weaknesses and implement the remedial actions required to resolve a system failure. In a worst-case scenario, the application or technology platform may have a catastrophic failure and cannot be recovered, resulting in an urgent need to implement either an upgrade or replacement of that system to restore network operations. The likelihood of this risk event occurring will increase with time if a suitable ongoing upgrade program is not completed.

Security breaches, and unavailability of operational and corporate systems give rise to people, supply, customer/reputational, compliance and financial consequences, as described below.

- People - Failure of critical applications will have adverse effects across the business as the true state of the network will not be reliably known, creating public safety risks; for example, if the Geospatial Information System (GIS) system fails, it could result in the Dial Before You Dig (DBYD) service not providing the latest gas location information to the public. This could result in a significant public safety issue if underground excavation is carried out in an area that MGN had indicated was clear of gas assets, but in fact was not. Furthermore, security breaches may cause outages in operational systems resulting in insufficient safety information being available in real time to field crews and lack of a pictorial representation of the asset, increasing the likelihood of a safety incident.
- Supply - Unaddressed deficiencies and poor integration between systems may result in inefficient work order processing, an inability to make spatial and logical queries, an inability to carry out timely repairs and maintenance, longer outages and operational risks of errors in manual data processes compared to electronic communications and confidential information being compromised.
- Reputation - MGN's reputation could be damaged significantly in the event of health and safety incidents, supply disruptions, delayed repairs and maintenance, compromised corporate, staff and customer information and resultant litigation.
- Compliance - The Health and Safety and Operational risks will result in slower and inefficient responses to call outs, and longer outages, which may result in breaches of the service standards, set out in the Victorian Gas Distribution System Code. In addition, security breaches may result in confidential customer data being compromised. Unsupported and poorly integrated systems and compromised customer information may result in MGN not complying with a range of legal and regulatory obligations (e.g. the RMP).
- Financial - The Health and Safety, Operational, Customer and Compliance consequences outlined above will result in sizeable additional costs (including potentially Guaranteed

Service Level (GSL) payments) and compromised staff and customer data could lead to significant litigation costs. In addition, without the continuation of IT vendor support which requires movement to a recent version of the software, MGN will be forced to find and hire expensive IT specialists with detailed knowledge of the outdated systems' inner workings and the programming language used. Financial penalties may also be imposed for not complying with RMP or other regulatory obligations.

A summary of the untreated risk[10] assessment is provided in Table 1.3. As this table shows, the untreated risk has been rated as 'High' because the people, reputational and financial related risks are high.

Table 1.3: Risk rating – untreated risk

Untreated risk	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Major	Minimal	Severe	Severe	Severe	
Risk Level	Low	High	Negligible	Intermediate	Intermediate	Intermediate	

1.4 Options considered

The following options have been identified to address the risks outlined above and support MGN's business objectives:

- Option 1 – Repair/replace on failure
- Option 2 – Upgrade and maintain applications

These options are discussed in the following sections.

1.4.1 Option 1 – Repair/replace on failure

This option would entail critical IT systems being repaired or replaced on failure or technical obsolescence. Vendor software patches would not be applied. The only maintenance performed would be critical system bug fixes required to keep the systems running.

1.4.1.1 Cost assessment

The benefit of this option is that no upfront capital investment is required.

However, while there are no upfront capital costs, the high operational risks associated with this option are likely to result in significantly higher operational costs over the next AA period if MGN's applications become unstable, fail or are subject to security breaches. Other additional costs could include:

- Guaranteed Service Level (GSL) payments;
- litigation costs due to compromised staff and/or customer data;
- additional costs due to a requirement to hire expensive IT specialists on short notice; and
- financial penalties imposed for not complying with RMP or other regulatory obligations.

1.4.1.2 Risk assessment

Option 1 results in MGN being unable to adequately treat any of the risks to which it is exposed. Whilst our existing suite of applications will continue to operate and support

[10] Untreated risk is the risk level assuming there are no risk controls currently in place. Also known as the 'absolute risk'.

business operations, doing nothing to maintain them will result in gaps in risk treatment as well as the inability to mitigate new risks. It would also result in existing capabilities degrading over time resulting in failure of previously addressed risk mitigations.

As shown in Table 1.4, the treated risk for Option 1 remains high and therefore does not meet the requirements of our risk management framework. Additionally, the likelihood of failure will continue to increase over time, likely resulting in a higher risk rating in subsequent AA periods.

Table 1.4: Risk assessment – Option 1

Option 1	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Major	Minimal	Severe	Severe	Severe	
Risk Level	Low	High	Negligible	Intermediate	Intermediate	Intermediate	

Specifically, under Option 1, the following issues will arise:

- core applications will no longer be supported by software manufacturers;
- failure in older applications may occur, resulting in lengthy and unplanned network outages;
- applications will become unstable and more vulnerable to cyber attacks, increasing the likelihood of security breaches. Security breaches compromise the confidentiality and integrity of corporate and customer data, putting the safety of network services at risk and compromising staff and customer data;
- if there is a failure of key systems, MGN will not be compliant with a range of legal and regulatory obligations, e.g. the RMP;
- applications will be unable to support MGN's strategic objectives;
- technology upgrades for core software will be required, so not continuing with the planned upgrades will mean the opportunity for the 'change out' of inefficient/obsolete technologies will be missed;
- staying with existing systems as software licence renewals become due will lock MGN into old technology and another full license payment for the duration of the licence agreement period. Furthermore, the costs of maintenance and support agreements will increase as the systems are not upgraded and therefore placed out of the prescribed vendor maintenance cycle; and
- MGN's core applications are reliant on each other to allow high volumes of transactions to flow from one application to another and any system failure can have a significant impact across all network operations for an extended period of time while the remediation work is completed.

These risk consequences would be realised and magnified unnecessarily because reactive remedial actions take significant time and cost to implement. Furthermore, MGN's management and staff would be under pressure to recover functionality quickly, thereby increasing the risk of error.

1.4.1.3 Alignment with vision objectives

Table 1.5 shows how Option 1 aligns with our vision objectives.

Table 1.5: Alignment with vision – Option 1

Vision objective	Alignment
Delivering for Customers – Public Safety	N
Delivering for Customers – Reliability	N
Delivering for Customers – Customer Service	N
A Good Employer – Health and Safety	-
A Good Employer – Employee Engagement	N
A Good Employer – Skills Development	-
Sustainably Cost Efficient – Working within Industry Benchmarks	N
Sustainably Cost Efficient – Delivering Profitable Growth	N
Sustainably Cost Efficient – Environmentally and Socially Responsible	-

Option 1 would not align with our objectives of *Delivering for Customers*, as it would not allow MGN to address application operation and support risks which may result in issues with service reliability, potentially impacting public safety. Application reliability and performance, upon which MGN is dependent, would also impact delivery of customer services.

It would not fully meet MGN objectives of managing risks related to consistent and reliable performance of core applications that facilitate employee tasks and business processes, hence putting MGN employee efficiency and effectiveness at risk. This would impact employee engagement and therefore would not be consistent with being *A Good Employer*.

It would not allow MGN to comply with technology industry benchmarks of maintaining supported and reliable applications that underpin business operations. Further, unsupported and unreliable business applications increase operational costs through higher volumes of support activity, potential system outages disrupting business operations and higher vendor costs to fix system failures. Thus, MGN would not be able to meet its objectives of Working within Industry Benchmarks or Delivering Profitable Growth. This option therefore does not align with our objective to be *Sustainably Cost Efficient*.

1.4.2 Option 2 – Upgrade and maintain applications

As a prudent operator, MGN has undertaken appropriate risk assessments of the criticality of its IT systems. In accordance with these assessments, and good industry practice, we consider that continuing to maintain systems to current version minus one (n-1) is the most efficient and effective means of ensuring continued compliance with the wholesale market requirements.

Option 2 involves a plan to systematically upgrade MGN applications in accordance with this approach and our technology lifecycle management plan to ensure software currency, vendor support, security risk mitigation, and maintenance of features and functionality for business users.

1.4.2.1 Cost assessment

The estimated direct capital cost of this option for MGN is $17 million over the next AA period. This estimate is based on estimated costs of upgrading and maintaining the existing application suite as well as anticipated changes to the overall application landscape.

Table 1.6: Cost estimate – Option 2, real 2021 $'000

Option 2	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Capex	2,287	4,427	2,986	3,850	3,658	17,208

The key benefit of this option is that the security and integrity of the MGN applications will be maintained via a prudent cycle of application upgrades.

Other benefits of upgrading MGN applications include:

- ensuring upgraded applications continue to provide required integrated functionality to support business processes;
- managing alignment with other co-existing applications, including with other AGIG entities;
- ensuring validity of support requirements with technology vendors;
- maintaining systems security with critical security upgrades applied thereby protecting information assets from confidentiality, integrity and availability risks;
- providing for the continuation of vendor support (which generally requires movement to a recent version of the vendor's software);
- improving the security and integrity of business information as vendors place greater emphasis on these solutions; and
- ensuring compliance to market requirements for the latest application systems.

1.4.2.2 Risk assessment

This option reduces the likelihood of system(s) failure, the integration between systems not operating as required and the risk of staff and customer data being compromised from 'Unlikely' to 'Remote'. This is consistent with our risk management framework, as it reduces the residual risk outcome from 'High' to 'Intermediate', as shown in Table 1.7.

Table 1.7: Risk Assessment – Option 2

Option 2	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Intermediate (ALARP)
Consequence	Minor	Major	Minimal	Severe	Minor	Severe	
Risk Level	Negligible	Intermediate	Negligible	Low	Negligible	Low	

1.4.2.3 Alignment with vision objectives

Table 1.8 shows how Option 2 aligns with our vision objectives.

Table 1.8: Alignment with vision – Option 2

Vision objective	Alignment
Delivering for Customers – Public Safety	Y
Delivering for Customers – Reliability	Y
Delivering for Customers – Customer Service	Y

Vision objective	Alignment
A Good Employer – Health and Safety	Y
A Good Employer – Employee Engagement	Y
A Good Employer – Skills Development	-
Sustainably Cost Efficient – Working within Industry Benchmarks	Y
Sustainably Cost Efficient – Delivering Profitable Growth	Y
Sustainably Cost Efficient – Environmentally and Socially Responsible	-

Option 2 aligns with our objectives of *Delivering for Customers*, as it would deliver the appropriate risk mitigation to ensure availability and reliability of core MGN applications used in the delivery and management of the gas network for customers.

Option 2 will continue the approach under the current AA period of maintaining applications in accordance with a lifecycle management plan to ensure supportability, fit-for-purpose functionality and confidentiality of data. This complies with our objective to provide employees with a good technology experience using modern tools designed to optimise efficiency and deliver employee engagement, consistent with being *A Good Employer*.

This option also aligns with best industry practice to maintain current and supported business applications under a lifecycle management plan. This approach delivers lower support costs than would otherwise be the case. Therefore, this option does align with our objective to be *Sustainably Cost Efficient*.

1.2 Summary of costs and benefits

Table 1.9 presents a summary of how each option compares in terms of the estimated cost, the residual risk rating, and alignment with our vision objectives.

Table 1.9: Comparison of options

Option	Estimated cost (real $ million)	Treated residual risk rating	Alignment with vision objectives
Option 1	0	High	Does not align *with Delivering for Customers*, *A Good Employer* or *Sustainably Cost Efficient*
Option 2	17.2	Intermediate (ALARP)	Aligns with *Delivering for Customers, A Good Employer* and *Sustainably Cost Efficient*

1.3 Recommended option

Option 2 is the proposed solution. This solution involves execution of a defined application lifecycle management plan to systematically upgrade software and applications, maintaining business applications to a supported level to deliver greater reliability, functionality, security and inter-operability and preserve the ongoing integrity of our services.

1.4.3 Why is the recommended option prudent?

Option 2 is the most prudent option because it is most the cost-effective way of dealing with the risks posed by outdated and unsupported applications. It is also consistent with good industry practice.

The proposed solution mitigates the high risks associated with the 'Do Nothing' option by ensuring the security and integrity of the technology environment via a prudent cycle of application upgrades. The increased risk of system failure and the related impacts associated with these options are unacceptable.

Option 2 ensures than MGN not only meets minimum expected legislative obligations, but also minimises business disruption caused by unplanned system outages, under-performing applications or lack of appropriate vendor support. It also allows MGN to optimise business processes by ensuring appropriate and fit-for-purpose application functionality exists.

This option is consistent with our vision of being a good employer and will support lower overall costs of delivering services which is sustainably cost efficient and in the long term in the interests of customers.

1.4.4 Estimating efficient costs

The estimated direct capital cost of this option for MGN is $17 million over the next AA period. This estimate is based on estimated costs of upgrading and maintaining the existing application suite as well as anticipated changes to the overall application landscape.

The application roadmap (Appendix B) has been used to identify and prioritise upgrades. As well as existing systems, the estimate incorporates upgrades for the new One ERP system (S/4 HANA) being delivered in 2023/24. In accordance with the application lifecycle management plan, this would be due for a system maintenance upgrade in 2026/27.

The forecast cost breakdown is shown in the table below.

Table 1.9: Breakdown of cost estimate, real 2021 $'000

Project	2023/24	2024/25	2025/26	2026/27	2027/28	Total
GIS upgrade	-	462	-	651	2,733	**3,845**
EDMS upgrade	438	-	-	-	-	**438**
Service Now consolidation	107	-	-	-	-	**107**
Network Viewer upgrade	-	281	-	-	281	**562**
S/4 HANA (MGN Allocation)	-	-	-	1,521	-	**1,521**
WebMethods upgrade	1,097	-	-	-	-	**1,097**
MSI replacement	-	2,074	1,300	-	-	**3,375**
OSI Pi Upgrade	45	360	45	45	45	**539**
Public website upgrade	-	-	-	308	-	**308**
Minor system enhancements[11]	600	600	1,200	1,200	600	**4,200**
HCM refresh	-	649	441	125	-	**1,215**
Total	**2,287**	**4,427**	**2,986**	**3,850**	**3,658**	**17,208**

Tables may not sum due to rounding

Forecast expenditure on IT applications renewal and upgrade in the next access arrangement period is approximately $3 million higher than the expected spend in the current period. The key reason for this is the upgrade of some application upgrades (e.g. WebMethods) in the last period were allocated to the United Energy separation project. This was because various programs were on the critical path of the transition and therefore had to be updated to ensure the version was up to date and therefore supported through the move.

We also deferred some of the less critical applications upgrades due to funding restrictions. We had not forecast the Unite Energy separation, and therefore were unable to include these costs in the last AA proposal. This meant we had to prioritise our limited funding to those critical IT projects. As mentioned, while this may be possible over a few years, it is a false economy, and eventually we would have to incur upgrade costs. However, delivering upgrades as they are required is more prudent for risk management purposes.

[11] These are small or less complex applications used throughout the MGN business or activities required for any MGN application that is minor in nature or an enhancement to application operation or features. These activities are planned and executed to meet business requirements and prioritised by the business to optimise available funds. A full list of these is provided in Appendix C.

Table 1.10 Recurrent spend by application, real 2021 $'000

Project	Current AA period forecast	Next AA period forecast
GIS upgrade	4,404	3,845
EDMS upgrade	259	438
Service Now consolidation	250	107
Network Viewer upgrade	-	562
S/4 HANA (MGN allocation)	4,288	1,521
WebMethods upgrade	-	1,097
MSI replacement	-	3,375
OSI Pi upgrade	-	539
Public website upgrade	-	308
System enhancements	4,051	4,200
HCM refresh	-	1,215
Small application refresh	370	-
Misc. other	537	-
Total	**14,160**	**17,208**

Costs for this project have been estimated utilising standard Australian market rates for labour and consulting, previous costs for similar projects and competitive tender pricing for services and licensing. Project streams will be delivered throughout the access arrangement to optimise the use of Project specific resources and ensure full utilization of these resources.

The unit rates used for all projects managed within this program of work include the internal labour, external labour and materials/other costs forecast.

We have considered the impact of all other IT project on the project timing and delivery of this program.

1.4.5 Consistency with the National Gas Rules

In developing these forecasts, we have had regard to Rule 79 and Rule 74 of the NGR. Regarding all projects, and as a prudent asset manager, we consider whether capex conforms from several perspectives before committing to capital investment.

NGR 79(1)

The proposed solution is prudent, efficient, consistent with accepted and good industry practice and will achieve the lowest sustainable cost of delivering pipeline services:

- Prudent – Consistent upgrading of software applications is necessary to mitigate the high risks associated with operating outdated software, including non-compliance with the RMP

and other relevant regulations and legislation, potential customer and business interruptions, health and safety and corresponding adverse financial and reputation impacts.

- Efficient – Upgrades will be delivered using a combination of internal and external resources and using the Project Management Office to provide guidance and governance to the project. This is consistent with good industry practice and proven to be efficient. The expenditure is therefore consistent with the expenditure that a prudent service provider acting efficiently would incur.
- Consistent with accepted and good industry practice – Version upgrades will be applied to business systems every three years, consistent with standard industry practice. This will result in all critical systems being up to date, secure and supported by vendors, consistent with good industry practice.
- To achieve the lowest sustainable cost of delivering pipeline services – Upgrading our MGN IT systems is the lowest sustainable cost for suitable long-term mitigation of the risks discussed. The only other viable option for risk mitigation would be full replacement of existing IT systems with new systems which would be completely cost prohibitive and would also result in significant burden on staff. The chosen option is therefore consistent with the objective of achieving the highest quality and lowest sustainable cost of service delivery.

NGR 79(2)

The proposed capex is justifiable under NGR 79(2)(c)(i), 79(2)(c)(ii) and 79(2)(c)(iii), as it is necessary to maintain the safety and integrity of services and to comply with regulatory obligations. Failure or non-availability of critical IT systems, for example due to a security breach, may affect safety or integrity of services, or result in non-compliance with regulatory obligations (e.g., RMP requirements for processing timeframes).

NGR 74

The forecast costs are based on the latest market rate testing (late 2021) and reflect the lifecycle management and estimation approach described in the IT Plan. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.

Appendix A – Comparison of risk assessments for each option

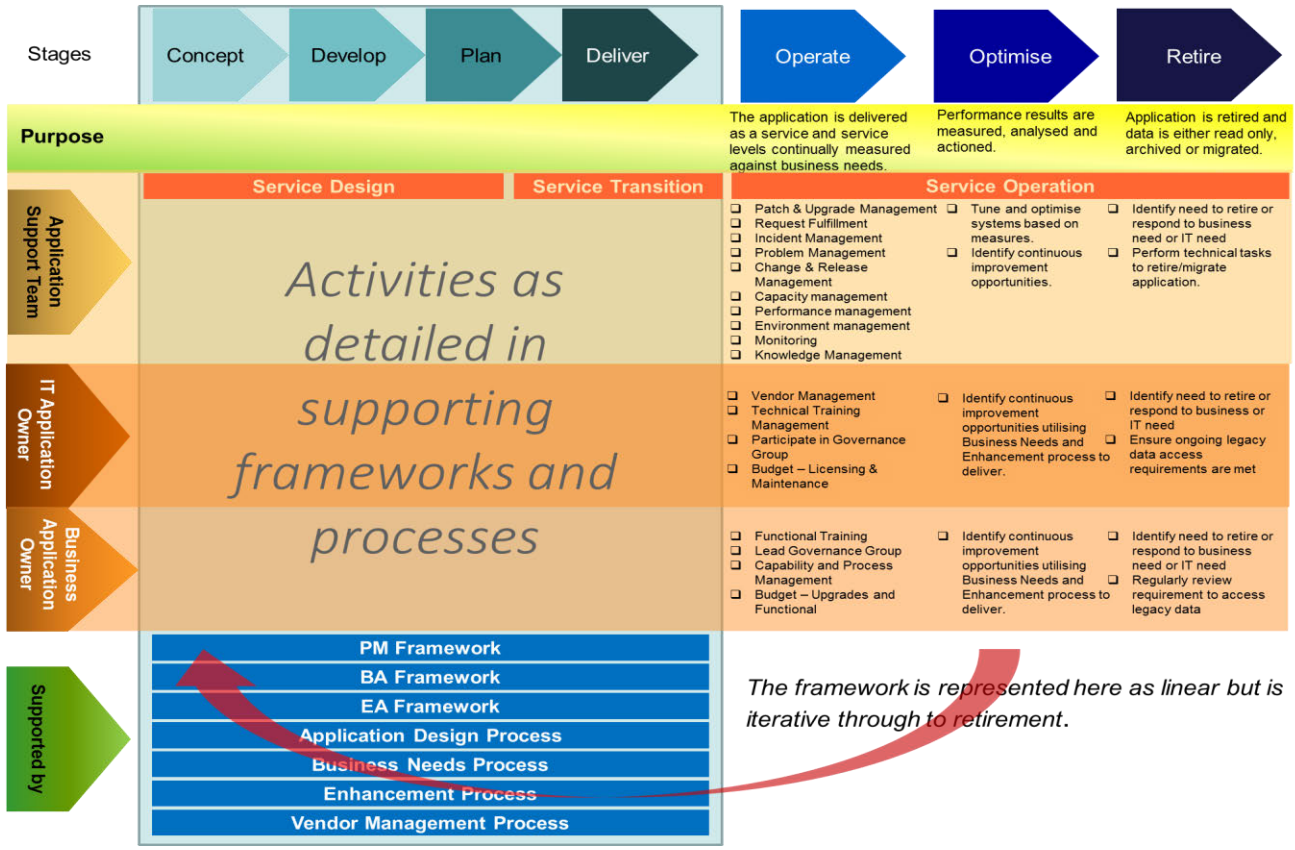
Untreated risk	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Major	Minimal	Severe	Severe	Severe	
Risk Level	Low	High	Negligible	Intermediate	Intermediate	Intermediate	

Option 1	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Major	Minimal	Severe	Severe	Severe	
Risk Level	Low	High	Negligible	Intermediate	Intermediate	Intermediate	

Option 2	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Intermediate (ALARP)
Consequence	Minor	Major	Minimal	Severe	Minor	Severe	
Risk Level	Negligible	Intermediate	Negligible	Low	Negligible	Low	

Appendix B – Application lifecycle management

Application Lifecycle Management Framework



Appendix C – Minor system enhancements

#	Application Name	Function
1.	Investor Portal	Public website for AGIG investors
2.	Robotic Process Automation	Utility for automation of business processes
3.	Project Management Tool	Project planning, tracking and governance tool
4.	SAP CRM (until replaced by Digital Customer Experience)	Customer Relationship Management tool used for customer interactions
5.	SAP IS-U	Finance, Procurement, Billing, Asset Management system core to all gas operations
6.	Tableau (until replaced by OneERP Phase 2)	Reporting platform
7.	Satori CCM	SAP segregation of duties checker
8.	Board CPM	Board paper preparation tool
9.	MG SAP Outage Contingency	Work Order recording tool for when SAP is unavailable
10.	DBYD (AIRS)	Data extraction tool to provide gas asset location details
11.	HP Quality Centre (HPALM)	Application Lifecycle Management and Testing tool
12.	Visual Risk	Treasury tool
13.	CommBiz (CBA) - integ from OneERP 2	Banking B2B tool
14.	ServiceNow Annual Upgrade (FSM / ITSM)	Field Service and Service Management tool
15.	MSI - CATS/B2B (until replaced by OneERP Phase 2)	Market System Interface for Retailer and AEMO B2B transactions
16.	SAP S/4 HANA	ERP system replacing existing SAP systems

2 Capex V.23.IT - Infrastructure renewals

2.1 Project approvals

Table 2.1: Project approvals

Prepared by	Cameron Honey, Head of Technology Services
Reviewed by	Kalpna Shukla, Head of Architecture
Approved by	Paul May, Chief Financial Officer

2.2 Project overview

Table 2.2: Project overview

Description of the problem / opportunity	Multinet Gas Networks' (MGN's) existing IT data centre and office equipment will reach the end of its useful life during the next Access Arrangement (AA) period (2023/24 - 2027/28). The Infrastructure Renewals project considers the upgrade or replacement of this equipment required over the period. Its key objectives are to ensure that MGN can: • continue to maintain reliable, secure, compliant and efficient business processes and systems, substantially reducing the risk of system failures or poor application performance; • continue to obtain vendor support for hardware, operating systems, infrastructure related software, networking components and appliances that enable MGN business operations; • provide a reliable and high-performing user experience in the use of key technology and systems to deliver services; • preserve the ongoing integrity of data and services; and • continue to comply with a range of regulatory and other obligations. If the project is not carried out, MGN's critical business systems may be exposed to higher security risks, sub-optimal performance and a greater risk of failure or prolonged outage. This would adversely affect the safety and integrity of services and could result in MGN failing to fulfil its customer and regulatory obligations under the Victorian Retail Market Procedures and other legislative and regulatory instruments.
Untreated risk	As per MGN risk matrix = **High**
Options considered	• **Option 1** – Do Nothing - replace IT equipment on failure (no additional upfront capex) • **Option 2** – Proactively replace obsolete IT equipment in line with a lifecycle management framework ($9 million)
Proposed solution	Option 2 is the proposed solution as it is the most cost-effective way of mitigating the risks posed by outdated, under-performing and unsupported infrastructure. It is also consistent with good industry practice and manufacturer recommendations. Option 1 is not recommended as this option does not mitigate the risks associated with retaining legacy and unsupported infrastructure components and would result in a rushed and unstructured approach to infrastructure replacement or recovery activity following a failure scenario, which would likely result in a poor outcome at higher cost.

Estimated cost

The forecast direct cost during the next five-year period (July 2023 to June 2028) is $9 million ($2021).

Real 2021 $'000	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Capex	3,222	1,014	816	582	3,851	9,485

Basis of costs

All costs in this business case are expressed in real unescalated dollars at June 2021 unless otherwise stated.

Alignment to our vision

This project aligns with the *Delivering for Customers* aspect of our vision by ensuring MGN technology platforms and office equipment are adequately maintained and available to meet their needs.

This project aligns with our vision objective of being *A Good Employer*, as it aims to provide employees with current, reliable, high performing and fit-for-purpose technology solutions that allow the business to operate effectively.

This project aligns with our vision to be *Sustainably Cost Efficient* as the project is driven by a lifecycle management framework that follows good industry practice, mitigates risks, optimises capital and operational expenditure, and minimises infrastructure support costs.

Consistency with the National Gas Rules (NGR)

This project complies with the following National Gas Rules (NGR):

NGR 79(1) – Proactive asset lifecycle management of IT infrastructure is prudent and efficient, the proposed solution is consistent with good industry practice, other practicable options have been considered, and market rates have been tested to achieve the lowest sustainable cost of providing services.

NGR 79(2) – Proposed capex is justifiable under NGR 79(2)(c) as it is necessary to:

- maintain and improve the safety of services (rule 79(2)(c)(i)) - making this investment reduces the risk of failure of the critical systems and the risk of security breaches, which could adversely affect the safety of services;
- maintain the integrity of services (rule 79(2)(c)(ii)) – proactive lifecycle management of IT infrastructure reduces the risk that the integrity of network services will be adversely affected by a failure of IT infrastructure; and
- comply with a regulatory obligation or requirement (rule 79(2)(c)(iii)) - the proactive lifecycle management of IT infrastructure mitigates the risk of a breach of regulatory obligations (e.g. Retail Market Procedure requirements for processing timeframes) if the systems dependent on these critical pieces of infrastructure were not available.

NGR 74 – the forecast costs are based on the current market rate and are in line with historical costs incurred. The infrastructure renewal options have been based on service provider recommendations, and assessed by MGN's IT architects. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.

Treated risk

As per MGN risk matrix = **Low**

Stakeholder engagement

We are committed to operating our networks in a manner that is consistent with the long-term interests of our customers. To facilitate this, we conduct regular stakeholder engagement to understand and respond to the priorities of our customers and stakeholders. Feedback from stakeholders is built into our asset management considerations and is an important input when developing and reviewing our expenditure programs.

Our customers have told us their top three priorities are price/affordability, reliability of supply, and maintaining public safety. Our IT infrastructure is integral in supporting our day to day operations and any deferral of upgrades from the typical asset lifecycle of devices increases the risk of security breaches, system unavailability or failure that could have adverse impacts on the safety and reliability of our services and our ability to provide the levels of customer service our customers expect and value.

Other relevant documents	• Attachment 9.9 IT Investment Plan

2.3 Background

The Multinet natural gas distribution networks deliver gas to over 700,000 consumers. To maintain integrity of services, and to allow us to securely store, search, and process the large volumes of data we need to service our customers, we operate and maintain a suite of Information Technology (IT) and Operational Technology (OT) infrastructure. These assets include data centre platform equipment, core networking equipment, appliances, office networking equipment, workstation devices, office printers, office telephony equipment, and handheld equipment such as mobile phones and tablets.

These infrastructure assets are essential to allow us to perform our daily activities, as well as meet a range of legal and regulatory obligations, including those prescribed in the National Gas Law (NGL) and National Gas Rules (NGR), the Victorian Gas Distribution System Code, the Victorian Gas Industry Act 2001, the Retail Market Procedures (RMP[12]) and Energy Safe Victoria's (ESV's) gas and pipeline safety requirements[13].

Box 1.1: MGN's obligations under the Retail Market Procedures

In accordance with Section 1.2 of the Retail Market Procedures, the Australian Energy Market Operator (AEMO) established a Gas Interface Protocol (GIP), which governs the manner and form in which information is to be provided, notice given, notices or documents delivered and requests made as contemplated by the RMP. Further, Section 1.2.4 of the RMP states that MGN is:

- *"bound by, the Gas Interface Protocol in respect of the provision of information, giving of notice, delivery of notices or documents and making of requests, and the receipt of information, notice, notices, documents or requests, as contemplated by these Procedures.";* and
- *"any failure to use the FRC HUB in accordance with the FRC HUB Operational Terms and Conditions may result in MGN being issued a breach notice."*

If the breach is found by AEMO to be material, it must be referred to the AER under section 91B of the NGL. This provision in the NGL is a civil penalty provision, which means that the AER can issue an infringement notice[14] and/or **institute civil proceedings** in the Federal Court and seek an injunction or an order that MGN remedy the breach; and/or an order that a penalty be paid.[15]

In addition, Participant Build Pack 3 - FRC B2B System Architecture Section 6, specifically addresses security noting *"An Internet based message service, by its very nature, presents certain security risks… Beyond the requirements herein, participants should make themselves familiar with these risks and institute countermeasures balanced against an assessment of the inherent risks and the value of the asset(s) that might be placed at risk."*

---

12 AEMO, "*Retail Market Procedures (Victoria)",* Document No: PROJECT-57-30 Version No: 10.0, 14 Sep 2015, http://www.aemo.com.au/Gas/Policies-and-Procedures/Retail-Gas-Market-Procedures/Victoria

13 http://www.esv.vic.gov.au/About-ESV

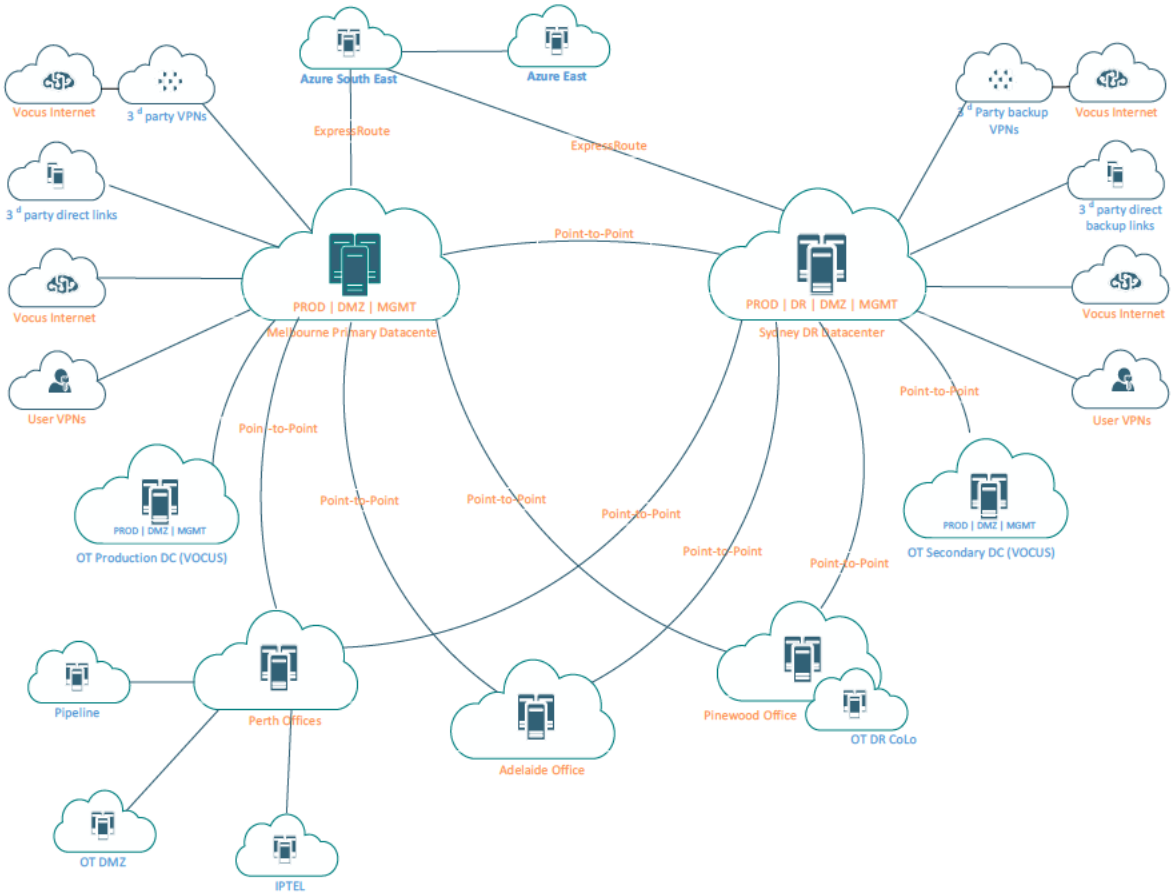
14 The maximum infringement notice is $4,000 for individuals ($20,000 for body corporates).

15 The maximum civil penalty is $20,000 for individuals ($100,000 for body corporates), plus $2,000 ($10,000) for every day it continues.

2.3.1 MGN's technology infrastructure environment

MGN is a part of Australian Gas Infrastructure Group (AGIG). Figure 2.1 below outlines the AGIG technology infrastructure environment and network layout that connects all AGIG offices, including the MGN locations.

Figure 2.1: Technology Infrastructure Environment



The MGN technology infrastructure at these locations is comprised of a variety equipment. As this infrastructure equipment ages, it becomes increasingly difficult to quickly implement the remedial actions required to resolve platform or system failures. In a worst-case (which becomes increasingly probable as the infrastructure ages), the platform or systems may experience a catastrophic failure and cannot be recovered, resulting in an urgent need of either an upgrade or replacement of that system to restore operations.

These IT infrastructure items must therefore be renewed or replaced before they reach the end of their useful life. The useful lives of IT assets can vary depending on how heavily they are used and moved around. Data centre, networking equipment and data centre appliances typically have a longer useful lifetime than end user equipment such as laptops, mobile phones and tablets, resulting in a different timing approach to replacement as the different types of equipment age and no longer perform at the standard required. These cycles are considered good industry practice.

Table 2.3 provides a summary of the existing MGN IT Infrastructure assets, a description of the asset types and the applicable asset lifecycle.

Table 2.3: MGN IT infrastructure assets

Infrastructure Asset Category	Description	Asset lifecycle
Data Centre Platform (IT)	Nutanix hyperconverged hardware incorporating compute, memory, storage and networking used to host corporate server workloads.	5 years
Data Centre Platform (OT)	Intel based computing hardware and storage area network (SAN) for OT server workloads.	5 years
Data Centre Core Network	Data centre based network routing and switching hardware.	5 years
Data Centre Appliances	Firewalls, Citrix Netscalers, Wireless LAN Controllers, etc.	5 years
Office Networking Equipment	Office based network routing and switching equipment.	5 years
Operating systems	Windows and Linux based operating systems	3-5 years
Databases	Relational databases – SQL, Oracle, Postgress	3-4 years
Infrastructure Mgmt. Tools	Monitoring, backup, orchestration, software distribution software, etc.	3-4 years
Authentication & Identity Management	Active Directory, group policy, security groups, distribution lists, etc.	3-4 years
End User Computing	End-point devices, client-based software and productivity/collaboration tools such Office365, Teams, etc.	3 years for physical equipment 3-4 years for user optimisation and collaboration tools

In the current AA period, a number of major projects to implement and upgrade key infrastructure components were completed. These projects delivered dedicated and improved IT and OT platforms for MGN, and onto which other data centre workloads for AGIG entities were also consolidated. This provided increased scalability, flexibility, reliability, and reduced platform costs across the AGIG businesses, while also ensuring that MGN continued to meet relevant regulatory and customer obligations. The ultimate beneficiaries of these improvements are MGN's customers.

2.4 Risk assessment

Risk management is a constant cycle of identification, analysis, treatment, monitoring, reporting and then back to identification (as illustrated in Figure 1.2). When considering risk and determining the appropriate mitigation activities, we seek to balance the risk outcome with our delivery capabilities and cost implications. Consistent with stakeholder expectations, safety and reliability of supply are our highest priorities.

Figure 2.2: Risk management principles

Our risk assessment approach focuses on understanding the potential severity of failure events associated with each asset and the likelihood that the event will occur. Based on these two key inputs, the risk assessment and derived risk rating then guides the actions required to reduce or manage the risk to an acceptable level.

Our risk management framework is based on:

AS/NZS ISO 31000 Risk Management – Principles and Guidelines,

AS 2885 Pipelines-Gas and Liquid Petroleum; and

AS/NZS 4645 Gas Distribution Network Management.

The Gas Act 1997 and Gas Regulations 2012, through their incorporation of AS/NZS 4645 and the Work Health and Safety Act 2012, place a regulatory obligation and requirement on MGN to reduce risks rated high or extreme to low or negligible as soon as possible (immediately if extreme). If it is not possible to reduce the risk to low or negligible, then we must reduce the risk to as low as reasonably practicable (ALARP).

When assessing risk for the purpose of investment decisions, rather than analysing all conceivable risks associated with an asset, we look at a credible, primary risk event to test the level of investment required. Where that credible risk event has an overall risk rating of intermediate or higher, we will undertake investment to reduce the risk.

Six consequence categories are considered for each type of risk:

1. **People** – injuries or illness to employees and contractors or members of the public
2. **Supply** – disruption in the provision of services/supply, impacting customers
3. **Environment** (including heritage) – impact on the surroundings in which the asset operates, including natural, built and Aboriginal cultural heritage, soil, water, vegetation, fauna, air and their interrelationships
4. **Reputation** – impact on stakeholders' opinion of AGN/AGIG, including personnel, customers, investors, security holders, regulators and the community
5. **Financial** – financial impact on AGN/AGIG
6. **Compliance** – the impact from non-compliance with operating licences, legal, regulatory, contractual obligations, debt financing covenants or reporting / disclosure requirements

Note that risk is not the sole determinant of what investment is required. Many other factors such as growth, cost, efficiency, sustainability, and the future of the network are also considered when we develop technology solutions. The risk management framework provides a valuable tool to manage our assets, and prioritise our works program, however it is not designed to provide a binary (yes/no) trigger for investment. As prudent asset managers, we apply our experience and discretion to manage and invest in our technology for our distribution networks in the best interests of existing and potential customers.

A summary of our risk management framework, including definitions, has been provided in Attachment 9.5.

The primary risk event associated with not renewing IT infrastructure is a failure of the infrastructure, resulting in security breaches, and unavailability of operational and corporate systems. The occurrence of this event would have adverse effects across the business and give rise to people, supply, customer/reputational, compliance and financial consequences, as described below.

- *People* - Any failure of critical infrastructure and the resulting outages to key applications would have adverse effects across the business as the true state of the network may not be reliably known, creating public safety risks; for example, if the infrastructure or server upon which the Geospatial Information System (GIS) system fails, it could result in the Dial Before You Dig (DBYD) service not providing the latest gas location information to the public. This could result in a significant public safety issue if underground excavation is carried out in an area that AGN had indicated was clear of gas assets, but in fact was not.
- Out of date equipment also results in a higher probability of IT and OT infrastructure being vulnerable to security incidents. Security breaches of the infrastructure may cause outages in

operational systems that would adversely affect the safety and integrity of services, potentially resulting in insufficient safety information being available in real time to field crews and lack of a pictorial representation of the asset, increasing the likelihood of a safety incident.

- *Supply* - As described above, there is an increased likelihood of failure in older infrastructure, which could result in unplanned production outages, and slower and inefficient responses to customer calls.
- Unreliable or poor performance of infrastructure can also result in inefficient work order processing, an inability to make spatial and logical queries, an inability to carry out timely repairs and maintenance, longer outages and operational risks of errors in manual data processes compared to electronic communications and confidential information being compromised.
- *Reputation* - AGN's reputation could be damaged significantly in the event of health and safety incidents; supply disruptions; delayed repairs and maintenance; compromised corporate, staff and customer information and resultant litigation.
- *Compliance* - Catastrophic failure in underlying infrastructure may result in outages of AGN's core IT or OT systems which, in turn, may lead to non-compliance with the RMP and AGN's other regulatory and customer obligations. For example, a failure in infrastructure supporting the ERP application could result in public leak reports or requests to turn meters on or off needing to be manually entered rather than being electronically transferred. This would delay the information getting to the operators in the field to do the work and significantly increase the risk of non-compliance with the RMP and the service standards set out in the Victorian Gas Distribution System Code (which could require a GSL payment);
- Health and Safety and Operational risks could also result in slower and inefficient responses to call outs, and longer outages, which may result in breaches of the service standards, set out in the Victorian Gas Distribution System Code. In addition, security breaches may result in confidential customer data being compromised.
- *Financial* - The consequences identified above may result in sizeable additional costs. In addition, without the continuation of vendor support that requires upgrades or replacements to maintain currency of the infrastructure, AGN will be forced to find and hire expensive consultants with detailed knowledge of outdated systems and infrastructure components.

A summary of the untreated risk[16] assessment is provided in Table 1.3. The table shows the overall untreated risk rating is high because the people, reputational and financial risks are high.

Table 2.4: Risk rating – untreated risk

Untreated	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Frequency	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Severity	Severe	Major	Minimal	Severe	Severe	Major	
Risk Level	Intermediate	High	Negligible	Intermediate	Intermediate	High	

2.5 Options considered

The following options have been identified to address the risks outlined above and support MGN's business objectives:

Option 1 – Do nothing (replace on failure)

Option 2 – Proactively replace obsolete IT equipment in line with a lifecycle management framework

[16] Untreated risk is the risk level assuming there are no risk controls currently in place. Also known as the 'absolute risk'.

These options are discussed in the following sections.

2.5.1 Option 1 – Do nothing

This option entails replacing data centre and office equipment on an ad-hoc basis in response to failure situations.

2.5.1.1 Cost assessment

The benefit of this option is that no upfront capital investment is required.

However while there are no upfront capital costs, the high operational risks associated with this option are likely to result in significantly higher operational costs over the next AA period due to an increased risk of failure in older infrastructure.

Other additional costs could include:

- reactive capital costs being incurred that are likely to be higher than they otherwise would be under a proactive and scheduled replacement approach, including additional costs due to a requirement to hire expensive IT specialists on short notice;
- the potential for Guaranteed Service Level (GSL) payments due to system unavailability;
- litigation costs due to compromised staff and/or customer data; and
- financial penalties imposed for not complying with RMP or other regulatory obligations.

2.5.1.2 Risk assessment

Option 1 represents a reactionary approach to treating the risks to which IT infrastructure is exposed. Whilst MGN's existing data centre infrastructure and office equipment would continue to operate and support business operations, reacting to failure scenarios or ad-hoc business requests to maintain them will result in gaps in risk treatment as well as MGN being unable to mitigate new risks. Existing infrastructure capabilities would also degrade over time, such that previously enabled mitigations may fail.

This option also maintains the existing level of People, Customer, Reputation and Financial risks, which would remain untreated. As shown in Table 2.5, the overall untreated risk under option 1 remains high, and will potentially rise to extreme in the subsequent AA periods as risks continue to increase. This option does not reduce risk to low or ALARP, and therefore does not meet the requirements of our risk management framework.

Table 2.5: Risk assessment – Option 1

Option 1	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Frequency	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Severity	Severe	Major	Minimal	Severe	Severe	Major	
Risk Level	Intermediate	High	Negligible	Intermediate	Intermediate	High	

Specifically, under option 1, the following issues will arise:

- core hardware will no longer be supported by vendors and hosted applications may become unstable;
- there is potential for a catastrophic failure that cannot be recovered, resulting in an urgent need to implement either an upgrade or replace a system to restore network operations. Under a reactive scenario, this would take significant time and cost to implement. Furthermore, MGN's management and staff would be under pressure to recover functionality quickly, thereby increasing the risk of error;
- infrastructure, specifically operating systems and infrastructure related software, will be more vulnerable to cyber-attacks and an increased likelihood of security breaches. Security breaches

compromise the confidentiality and integrity of corporate and customer data, and availability of operational and corporate systems, giving rise to risks across most categories;

- the opportunity for the 'change out' of inefficient/obsolete technologies will be missed and MGN may be locked into old technology and excessive (and increasing) full support and maintenance payments for the duration of any respective agreement;
- MGN's IT and OT applications are reliant on high performing infrastructure to allow the business to operate effectively, with high volumes of transactions flowing between applications as well as to other stakeholders. Any infrastructure failure can have a significant impact across all network operations for an extended period while remediation work is completed; and
- the technology infrastructure will be unable to support MGN's strategic objectives.

2.5.1.3 Alignment with vision objectives

Table 2.6 shows how Option 1 aligns with our vision objectives.

Table 2.6: Alignment with vision – Option 1

Vision objective	Alignment
Delivering for Customers – Public Safety	N
Delivering for Customers – Reliability	N
Delivering for Customers – Customer Service	N
A Good Employer – Health and Safety	N
A Good Employer – Employee Engagement	N
A Good Employer – Skills Development	-
Sustainably Cost Efficient – Working within Industry Benchmarks	N
Sustainably Cost Efficient – Delivering Profitable Growth	N
Sustainably Cost Efficient – Environmentally and Socially Responsible	-

Option 1 would not align with our objectives of *Delivering for Customers*, as it would only address infrastructure and office equipment risk on an as needed basis in response to failure or severe performance issues. Issues of service reliability, unplanned outages and lack of technology product support could potentially impact public safety, reliability of gas supply and MGN's reputation. Infrastructure reliability and performance, upon which MGN is dependent, would also impact delivery of customer services.

It would not fully manage risks related to consistent and reliable performance of data centre infrastructure and office equipment that facilitate employee tasks and business processes, hence putting MGN employee efficiency and effectiveness at risk. This would impact employee engagement and therefore would not be consistent with being *A Good Employer*.

It would not allow MGN to comply with technology industry benchmarks of maintaining supported and reliable infrastructure that hosts business applications that underpin business operations. Further, unsupported and unreliable infrastructure increases operational costs through higher volumes of support activity, potential system outages disrupting business operations and higher vendor costs to fix system failures. Thus, MGN would not be able to meet its objectives of Working within Industry Benchmarks or Delivering Profitable Growth. This option therefore does not align with our objective to be *Sustainably Cost Efficient*.

2.5.2 Option 2 – Proactively replace obsolete IT equipment

Option 2 involves a plan to systematically upgrade MGN data centre infrastructure and office equipment in accordance with good industry practice and a prudent technology lifecycle management framework. This includes replacing existing data centre infrastructure and related components as well as replacing the office equipment for the user population.

Our lifecycle management framework (summarised in Appendix C) supports a 'stay in business' program of work that ensures that data centre infrastructure and office computing equipment are kept stable, secure and at optimum performance. Consistent with industry practice, this maintains infrastructure at a level that can support the underlying principle of staying at a minimum of N-1[17] for related software and applications.

Alignment with N-1 ensures ongoing vendor support and mitigates the risk of security breaches, system outages and potential regulatory non-compliance, ensuring continued compliance with the wholesale market requirements. It enables appropriate levels of operation, data integrity and inter-operability between various vendor provided technologies[18].

2.5.2.1 Cost assessment

The estimated direct capital cost of this option for MGN is $9 million over the next AA period. The estimates are based on market rates for current services, new program activities and labour.

Table 2.7: Cost estimate – Option 2, real 2021 $'000

Option 3	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Capex	3,222	1,014	816	582	3,851	9,485

The benefits of managing MGN technology infrastructure and office equipment in accordance with a lifecycle management framework include:

- ensuring the IT and OT data centre infrastructure continues to provide the required level of performance, capacity, reliability, recoverability continuity and integration functionality to support business processes;
- a reduction in MGN's exposure to system and security related vulnerabilities, with critical security upgrades applied regularly, thereby protecting information assets from confidentiality, integrity and availability risks;
- ensuring currency of support requirements with technology vendors, ensuring continued provision of ongoing support and maintenance, and that any known issues including security vulnerabilities are addressed;
- ensuring than MGN continues to meet minimum expected legislative obligations and complies with market requirements; and
- minimising business disruption caused by unplanned system outages, under-performing infrastructure or a lack of appropriate vendor support.

[17] N-1 Refers to the specific software version number, which is associated with a specific vendor software. Where "N" representing the current version of the released and supported software, whereas -1 would refer to an older version of the same vendor software which would still be supported. Upgrade versions are provided by vendors who recommend that their technology be upgraded to ensure ongoing support and maintenance contracts.

[18] There are interdependencies between the various infrastructure components, which are integrated to support business requirements. This interdependency creates a working construct of hardware, software and appliances that are at risk if they are not maintained at appropriate versions or releases prescribed by technology vendors. The interoperability of disparate infrastructure must be constantly monitored in order to have visibility of potential incompatibilities

2.5.2.2 Risk assessment

This option will ensure appropriate risk mitigations are fully implemented and that this capability can be maintained throughout the access period. A managed and controlled plan to upgrade or replace legacy infrastructure will reduce the likelihood of equipment failure and the risk of staff and customer data being compromised. This reduces the overall risk level to intermediate (ALARP) which is consistent with the MGN risk management framework.

An intermediate rating is as low as reasonably practicable. This is because renewing the IT infrastructure does not reduce the risk consequence. A security breach or infrastructure failure can still carry major operational and reputation consequences, however, if we have up-to-date infrastructure a breach or failure is much less likely to happen.

The residual risk outcomes are shown in Table 2.8.

Table 2.8: Risk assessment – Option 2

Option 2	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Frequency	Remote	Remote	Remote	Remote	Remote	Remote	Intermediate (ALARP)
Severity	Severe	Major	Minimal	Severe	Severe	Major	
Risk Level	Low	Intermediate	Negligible	Low	Low	Intermediate	

2.5.2.3 Alignment with vision objectives

Table 1.8 shows how Option 2 aligns with our vision objectives.

Table 2.9: Alignment with vision – Option 2

Vision objective	Alignment
Delivering for Customers – Public Safety	Y
Delivering for Customers – Reliability	Y
Delivering for Customers – Customer Service	Y
A Good Employer – Health and Safety	Y
A Good Employer – Employee Engagement	Y
A Good Employer – Skills Development	-
Sustainably Cost Efficient – Working within Industry Benchmarks	Y
Sustainably Cost Efficient – Delivering Profitable Growth	Y
Sustainably Cost Efficient – Environmentally and Socially Responsible	-

Option 2 aligns with our objectives of *Delivering for Customers*, as it would deliver the appropriate risk reduction to ensure availability and reliability of the IT and OT data centre infrastructure hosting MGN's core applications that are used in the delivery and management of the gas network for customers.

Option 2 will continue the approach under the current AA period of maintaining data centre infrastructure and office equipment in accordance with a lifecycle management framework to ensure performance, supportability, fit-for-purpose functionality and security protection measures. This complies with our objective to provide employees with a good technology experience using modern tools designed to optimise efficiency and deliver employee engagement, consistent with being *A Good Employer*.

This option also aligns with best industry practice to maintain current and supported infrastructure and office equipment under a lifecycle management framework. This approach delivers lower

support costs than would otherwise be the case. Therefore, this option does align with our objective to be *Sustainably Cost Efficient*.

2.6 Summary of costs and benefits

Table 1. presents a summary of how each option compares in terms of the estimated cost, the residual risk rating, and alignment with our vision objectives.

Table 2.10: Comparison of options

Option	Estimated cost ($ million)	Treated residual risk rating	Alignment with vision objectives
Option 1	0	High	Does not align with *Delivering for Customers, A Good Employer* or *Sustainably Cost Efficient*
Option 2	9.5	Intermediate (ALARP)	Aligns with *Delivering for Customers, A Good Employer* and *Sustainably Cost Efficient*

2.7 Recommended option

Option 2 is the proposed solution. This solution involves replacing existing data centre infrastructure and related components, and office equipment, using a defined infrastructure and office equipment lifecycle management framework.

2.7.1 Why is the recommended option prudent?

Option 2 is the most prudent option because it is the most cost-effective way of dealing with the risks posed by outdated and unsupported infrastructure. It is also consistent with good industry practice.

The proposed solution mitigates the high and unacceptable risk of system failure and the related impacts associated with the 'Do Nothing' option, by ensuring the security and integrity of the technology environment. Specifically, option 2 will:

- reduce MGN's exposure to system and security related vulnerabilities and unplanned outages from the failure of critical infrastructure;
- ensure the stability of the IT and OT systems and enable core infrastructure, office equipment and other infrastructure related components;
- ensures than MGN not only meets minimum expected legislative obligations, but also minimises business disruption caused by unplanned system outages, under-performing equipment or lack of appropriate vendor support;
- allow MGN to optimise business processes by ensuring appropriate and fit-for-purpose infrastructure; and
- minimise financial risks.

This option is consistent with our vision of being a good employer and will support lower overall costs of delivering services which is sustainably cost efficient and in the long term in the interests of customers.

2.7.2 Estimating efficient costs

Costs for this project have been estimated using standard Australian market rates for labour and consulting, previous costs for similar projects and competitive tender pricing for services and licensing.

Replacement timelines and priorities are primarily driven by the device asset lifecycle, as defined in our lifecycle management framework. We have also had regard to our other IT programs of work in the next AA period (as described in our IT Investment Plan, provided at Attachment 9.9). In particular, the planned infrastructure renewal will ensure our devices are compatible with the objectives of the AGIG IT Strategy and Roadmap. Project streams will be delivered throughout the access arrangement to optimise and ensure the most efficient utilisation of resources, across both this, and other IT investments.

The estimated direct capital cost of this option for MGN is $9 million over the next AA period, as shown in the table below.

Table 2.11: Cost estimate – Option 3, real 2021 $'000

Option 2	Infrastructure Category (see Appendix A)	2023/24	2024/25	2025/26	2026/27	2027/28	Total
OS Currency	Operating Systems	429	-	215	157	157	958
Active Directory Consolidation and functional uplift	Authentication & Identity Mgt	153	-	-	-	132	285
Data Centre Strategy/ Upgrade/Replacement and Cloud Migration	Data Centre Platforms	429	-	215	157	157	958
Standard Operating Environment (SOE) image upgrade & deployment	End User Computing	330	-	-	-	330	660
SQL DB Currency	Databases	-	234	-	-	-	234
Oracle DB Decomm	Databases	-	249	-	-	-	249
Collaboration Upgrades (SharePoint, MS Teams)	End User Computing	-	124	-	-	-	124
Nutanix Platform Replacement	Data Centre Platforms (IT)	892	-	200	-	414	1,506
Core network strategy and carrier upgrade/replacement	Data Centre Core Network	289	-	-	-	-	289
Citrix Farm Upgrade	End User Computing	264	-	-	-	-	264
Infrastructure Tools Replacement	Infrastructure Management Tools	180	87	55	-	-	321
OT Infrastructure Replacement	Data Centre Platforms (OT)	-	-	-	-	2,356	2,356
Office Equipment Replacements	End User Computing	257	319	130	267	304	1,277
Total		**3,223**	**1,014**	**816**	**582**	**3,851**	**9,485**

Tables may not sum due to rounding

Forecast expenditure on IT infrastructure renewals in the next AA period is in line with that in the current period, as shown in Table 2.12.

Table 2.12 Infrastructure spend by category current vs next AA period, ($'000 real 2021)

Application	Current AA period forecast (Jan-18 to Dec-22)	Interim period (Jan-23 to Jun-23	Next AA period forecast (Jul-23 to Jun-28)
Data Centre consolidation	3,946	2,000	5,852
OT Infrastructure replacement	4,563	150	2,356

Office Equipment replacement	873	150	1,277
Total	**9,382**	**2,300**	**9,485**

We have considered the impact of all other IT projects on the project timing and delivery of this program.

2.7.3 Consistency with the National Gas Rules

In developing these forecasts, we have had regard to Rule 79 and Rule 74 of the NGR. With regard to all projects, and as a prudent asset manager, we give careful consideration to whether capex is conforming from a number of perspectives before committing to capital investment.

NGR 79(1)

The proposed solution is prudent, efficient, consistent with accepted and good industry practice and will achieve the lowest sustainable cost of delivering pipeline services:

- **Prudent** – The expenditure is necessary in order to maintain IT assets so that we can mitigate the risk of cyber security breaches, maintain the integrity of services, and enable our employees to carry out their day-to-day activities.
- **Efficient** – Proactive replacement of infrastructure assets that are at or nearing the end of their useful lives is a more efficient approach than replacing these assets upon failure. Deferring replacement can result in higher reactive costs if critical assets fail, or penalties for non-compliance with RMP obligations.
- **Consistent with accepted and good industry practice** – proactive asset lifecycle management is good industry practice regardless of the type of asset. Energy network business are becoming more dependent on IT systems and provision of timely and accurate information, therefore it is good practice to make sure IT infrastructure assets are up to date and are resilient to cyber security threats.
- To achieve **the lowest sustainable cost of delivering pipeline services** – The infrastructure renewals are necessary to mitigate cyber security risks, which can result in costly service interruptions. Proactive replacement is typically also less expensive than reactive replacement. Ensuring stable IT assets will also allow the proposed investments in applications to be appropriately exploited. The project is therefore consistent with the objective of achieving the lowest sustainable cost of delivering services.

NGR 79(2)

Proposed capex is justifiable under NGR 79(2)(c)(i), (ii) and (iii) as it is necessary to maintain integrity of services, and to comply with a regulatory obligation, in particular our data provision requirements under the RMP.

NGR 74

The forecast costs are based on the latest market rate testing and project options consider the managed service providers recommendations to meet the business needs and ongoing program of work identified in this business case. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.

Appendix A – Infrastructure categories

- ***Data Centre Platforms* (IT)** – This is comprised of high performance, hyper-converged hardware upon which server operating systems are hosted that run the business applications. The clusters include memory, compute and storage capacity to run virtualised operating systems (Windows or Linux) for the various business applications. Data Centre platform equipment is typically replaced every 5 years in line with asset depreciation cycles. The current IT data centre platform equipment was implemented in 2019 and is due for replacement in 2024.
- ***Data Centre Platforms* (OT)** – This is comprised of high-performance server hardware providing a virtualised layer upon which server operating systems are hosted that run the OT applications. The environment includes memory, compute and storage capacity to run virtualised operating systems (Windows or Linux) for the various OT applications. Data Centre platform equipment is typically replaced every 5 years in line with asset depreciation cycles. The current MGN OT data centre platform equipment was implemented in 2021 and would be due for replacement in 2026.
- ***Data Centre Core Network*** – This is comprised of high performance switching and routing equipment that enables network connectivity from MGN's office locations to the central Data Centre where the applications are hosted as well as between AGIG office locations to enable inter-company communication and collaboration. Data Centre Core Network equipment is typically replaced every 5 years in line with asset depreciation cycles. The current data centre core network equipment was implemented in 2019 and is due for replacement in 2024.
- ***Data Centre Appliances*** – This is comprised of specialised equipment such as firewalls that define the perimeter of the internal and external (internet) networks through which all traffic into and out of the data centre flows. They also provide segregation of the networks that make up the technology environment with rule-based filtering applied to all traffic to ensure protection from suspicious traffic or malicious attempts to infiltrate the AGIG data centre. Data Centre appliance equipment is typically replaced every 5 years in line with asset depreciation cycles. The current data centre appliances were implemented in 2019 and are due for replacement in 2024.
- ***Office Networking Equipment*** – This includes network switching and routing equipment located at end points of the connected network, i.e. the MGN office locations that provides a secure and private network connection to the central AGIG data centres within which the MGN applications are hosted and run. Office Networking equipment is typically replaced every 5 years in line with asset depreciation cycles. The current office networking equipment was implemented in 2019 and is due for replacement in 2024.
- ***Operating Systems*** – This comprises the virtualised server operating systems (Windows Server and Linux Redhat). A staged program of replacement is typically performed over a number of years to opportunistically align with application upgrades or replacements. The version of a particular IT or OT application will often dictate the version of server operating system upon which it can run to ensure it will function as designed. This is why it is imperative to holistically consider operating system upgrades in line with application version upgrades or replacements.
- ***Databases*** – This comprises the database software products upon which business and infrastructure related applications are reliant. Typically, databases are updated or replaced every 3-4 years to remain current and take advantage of new functionality, efficiencies and performance improvements. Database upgrades can be performed independently of application upgrades, though it is also generally the case that a database version upgrade will accompany an application upgrade or replacement. The version of a particular IT or OT application will often dictate the version of database software upon which it can run to ensure it will function

as designed. This is why it is imperative to holistically consider database upgrades in line with application version upgrades or replacements.

- ***Infrastructure Management Tools*** – This element of the infrastructure incorporates the suite of tools required to manage the technology environment and includes things such as monitoring software, backup hardware and software, the software distribution system for deployment of security updates, process orchestration software, the mobile device management platform, and secure file transfer services. Infrastructure tools are typically upgraded or replaced every 3-4 years to remain current and take advantage of new functionality to improve infrastructure management.
- ***Authentication and Identity Management*** – This element involves the setup, management and maintenance of AGIG's multiple Active Directory (AD) instances which facilitate user identity authentication as well as access to applications and computing resources through policies and security groups. Like other infrastructure technologies, the functional version of AD needs to be upgraded or replaced every 3-4 years to remain current, take advantage of new or improved functionality and remain supported by the product vendor. AGIG has multiple corporate Active Directory instances, of which MGN is one. A program to consolidate and upgrade the disparate Active Directory environments is required to drive standardisation of user experience, efficiencies of AD management and optimise the foundational component of the technology landscape through which all access is governed and controlled.
- ***End User Computing*** – This comprises all end-point physical equipment, workstation operating systems, optimisation technologies and collaboration tools required by end users to function effectively. This includes the following components.
  - Physical equipment:

    – Desktops and laptops, mobile phones, tablet devices, telephony tools such as handsets and headsets, network printers, and peripheral equipment such as monitors, docking stations, keyboards, mouse, etc.

  - Standard Operating Environment (SOE) image:

    – Base windows operating system, preferred web browsers, embedded end-point client software such as Adobe Reader, SAP GUI, Citrix Workspace, file compression software, etc., and standard productivity tools such as Microsoft Office365.

  - Optimisation and Collaboration Tools:

    – SharePoint platform and sites, Office365 platform and features, Citrix farms and Microsoft Teams services.

Physical equipment is typically maintained and replaced every 3 years in line with warranty and asset depreciation cycles or as required due to failure, breakage or loss. MGN's physical equipment has been replaced on a continuous cycle in the current AA period with a proportion of the end user fleet of devices replaced every year. This approach is expected to continue in the next AA period.

Typically, the SOE image is updated and replaced every 3-4 years to optimise user productivity and leverage improved performance as well as new features and functionality. Any new SOE is developed and deployed to the fleet of end-point devices in a relatively short timespan to ensure standardisation of the user experience as quickly as possible. MGN's current SOE was deployed during 2020 and will be due for replacement with a new Windows version by 2023/24 and then again towards the end of the next AA period.

The software components that make up a suite of products to optimise the end user experience or provide platforms for collaboration are typically upgraded or replaced every 3-4 years. For subscription-based services like Office365 or Teams, it is possible to benefit from iterative development by Microsoft on a more frequent basis, but care needs to be taken when releasing new capability to the user population to ensure compatibility of these tools with applications, and that MGN's security and operating conditions are not compromised. Optimisation technology like Citrix and collaboration platforms like SharePoint require a more structured approach to manage upgrades and replacements which would also typically be every 3-4 years.

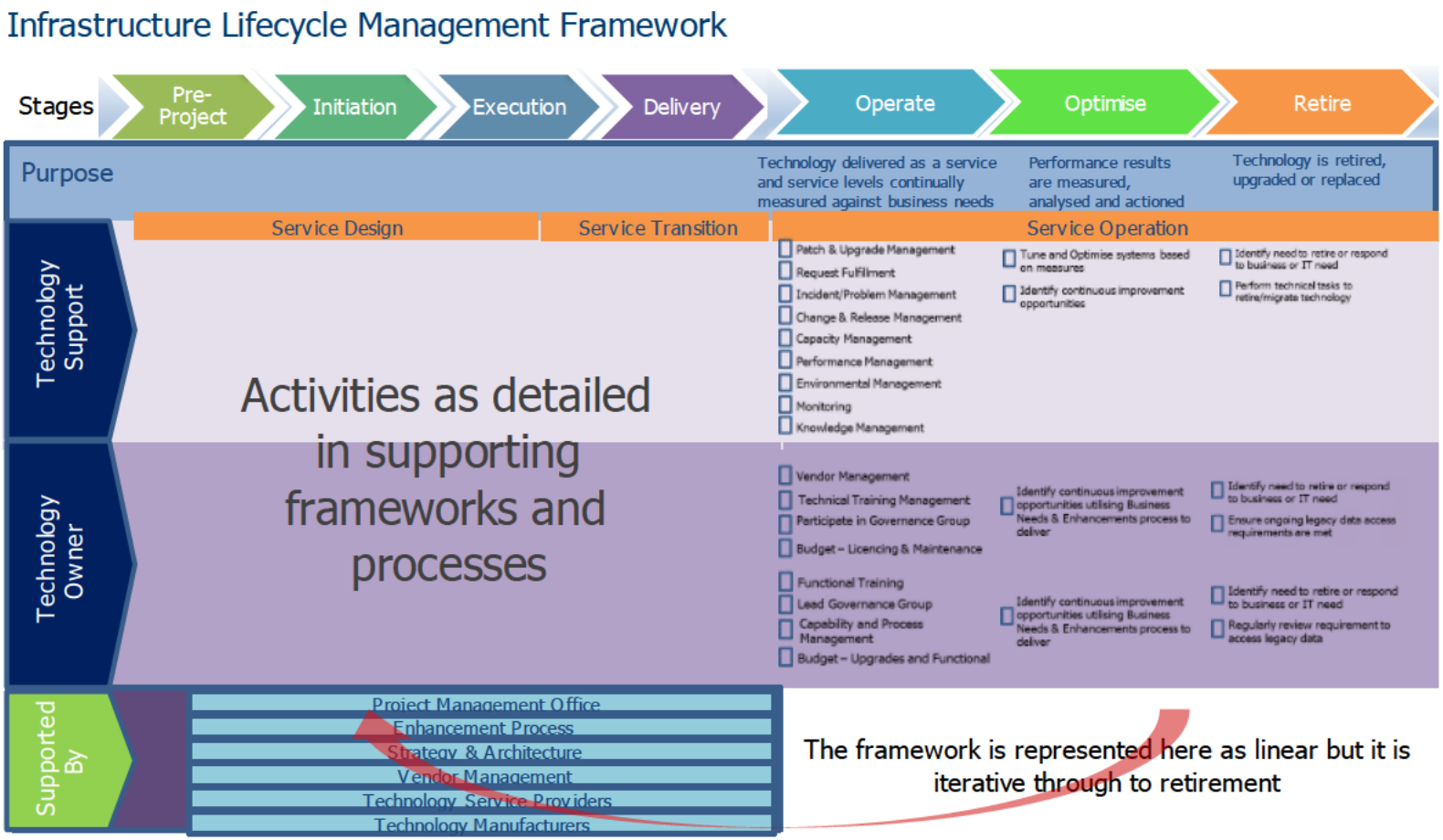
Appendix B – Comparison of risk assessments for each option

Untreated	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Frequency	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Severity	Severe	Major	Minimal	Severe	Severe	Major	
Risk Level	Intermediate	High	Negligible	Intermediate	Intermediate	High	

Option 1	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Frequency	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Severity	Severe	Major	Minimal	Severe	Severe	Major	
Risk Level	Intermediate	High	Negligible	Intermediate	Intermediate	High	

Option 2	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Frequency	Remote	Remote	Remote	Remote	Remote	Remote	Intermediate (ALARP)
Severity	Severe	Major	Minimal	Severe	Severe	Major	
Risk Level	Low	Intermediate	Negligible	Low	Low	Intermediate	

Appendix C – Lifecycle management framework



3 Capex V.24.IT – AGIG One IT

3.1 Project approvals

Table 3-1: Project approvals

Prepared by	Kalpna Shukla, Head of Architecture
Reviewed by	Bill Fazl, Chief Information Officer
Approved by	Paul May, Chief Financial Officer

3.2 Project overview

Table 3-2: Project overview

Description of the problem / opportunity	This business case is for the continuation of the AGIG One IT program, specifically the program component to be delivered for the Multinet Gas Networks (MGN) distribution business. Developed in 2019, AGIG One IT is a program that will develop a stable and aligned Information Technology (IT) environment across all AGIG entities. This will enable all AGIG businesses to conduct its work more effectively, reduce inefficiencies, inconsistency and duplication between IT systems and processes, and provide a better overall service to gas customers. The program objectives are to: • better deliver the AGIG corporate strategy and individual business unit operating strategies and plans; • act on feedback from our stakeholders, regulators and customers that they value reliable and safe delivery of energy to our customers backed up by timely support when they need help; • address specific issues and risks common to all AGIG businesses, including cyber security, likelihood of errors and poor management decisions based on incorrect or untimely information, and employee frustration due to lack of access to data and ability to collaborate effectively; and • achieve economies of scale in purchasing and support costs. The program is split into two stages. Stage 1, which started in 2020, is delivering a foundational program to ensure effective collaboration, appropriate management of cyber risks and leveraging economies of scale across the AGIG businesses. It includes initial components of the larger transformational programs (being delivered in Stage 2) to improve financial reporting capabilities, empowering management with more accurate and timely information. Stage 2 builds on the foundational program by delivering several transformational initiatives. For MGN, this transformational program involves the extension of the 'OneERP' project to the MGN business – delivering a standardised enterprise resource planning (ERP) system across the AGIG group and advancing the Data Architecture, Reporting and Governance initiative established in the current Access Arrangement (AA) period. Having a standard ERP system will allow us to remove the heavy customisation, cumbersome manual processes, the need to consolidate data from multiple disparate systems for reporting and decision making purposes and therefore the substantial risks, associated with local finance systems. Phase 1 of the work to implement that standard ERP system (SAP S4/HANA) has already commenced with configuration complete and testing underway to be rolled out to AGN and Dampier to Bunbury Pipeline (DBP) in the current AA period. The majority of Stage 1 work is being completed in the current AA period. The remainder of Stage 1, along with Stage 2, is planned for the next AA period. To facilitate delivery and better align with external timelines such as system end-of-life and contractual arrangements, some of the Stage 2 initiatives, as well as extension of the transformational initiatives, will continue past 2025/26.

Untreated risk

As per risk matrix = **Intermediate (not ALARP)**

Options considered

- **Option 1** – Do nothing more, halt the AGIG One IT investment and continue to run disparate IT environments across AGIG. ($0 upfront capex).
- **Option 2** – Complete foundational AGIG IT initiatives only ($2 million capex, $3 million opex step change)
- **Option 3** – Complete foundational and undertake transformational AGIG IT initiatives in line with the AGIG One IT program ($37 million capex, $3 million opex step change)

Proposed solution

Option 3 is proposed. This includes completing the foundational and cyber initiatives underway, establishing enterprise data governance, and delivering OneERP. Completing the AGIG One IT program initiatives in line with the plan developed will:

- improve our ability to respond to and mitigate cyber risks;
- improve access to accurate and timely data and information, building greater user trust and collaboration;
- ensure our decisions concerning information use are in line with AGIG's data governance framework and information security requirements.
- streamline enterprise data architecture, reporting and governance through an enterprise data model and data integration;
- optimise our licensing and operational costs, through consolidating and negotiating ongoing maintenance and support contracts with select strategic vendors;
- standardise and streamline finance and decision making processes across AGIG; and
- ensure our finance and decision making processes are delivered in line with AGIG's financial and governance controls.

Estimated cost

The forecast direct capex (excluding overhead) during the next five-year period (2023/24 to 2027/28) is $37 million.

$'000 real 2021	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Capex	9,169	20,251	6,672	226	246	**36,565**

We are also proposing an opex step change in the next AA period for the uplift in cyber security requirements of approximately $3 million.

$'000 real 2021	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Cyber opex step change	522	522	622	839	839	**3,345**

Basis of costs

All costs in this business case are expressed in real unescalated dollars at June 2021 unless otherwise stated.

Alignment to our vision

This project aligns with the *Delivering for Customers* aspect of our vision as it ensures our employees and digital platforms can provide timely and relevant information to support our customer service functions.

This project also aligns with our vision objective of being *A Good Employer*, as it addresses employee frustrations highlighted in a number of our annual Employee Engagement Surveys by delivering rationalised, fit-for-purpose IT systems across AGIG that enable collaboration and timely access to accurate data and information.

It is also *Sustainably Cost Efficient* as it standardises finance systems and processes across AGIG reducing the likelihood of errors, streamlining processes and introducing economies of scale in the procurement and management of these systems through combined purchasing power. It provides for a cohesive approach to managing cyber risks across AGIG by uplifting cyber capabilities and ensuring continued investment to maintain good practice cyber risk

	management in line with the Australian Energy Sector Cyber Security Framework and Security of Critical Infrastructure obligations.
Consistency with the National Gas Rules (NGR)	This project complies with the following National Gas Rules (NGR): **NGR 79(1)** – the proposed foundational and transformational IT initiatives that will be pursued are consistent with good industry practice, several practicable options have been considered, and we have received independent expert advice as well as tested market rates across initiatives to ensure this project reflects the lowest sustainable cost of providing services. There has been significant internal consultation and use of independent experts to ensure that the individual initiatives pursued within this project are prudent, efficient, consistent with accepted good industry practice and achieve lowest sustainable cost of delivering services. **NGR 79(2)** – proposed capex is justifiable under NGR 79(2)(c)(ii), as it is necessary to maintain the integrity of services. **NGR 74** – the forecast costs are based on the latest market rate testing and independent expert costing of project options considered in the AGIG One IT program. The estimates have therefore been arrived at on a reasonable basis and represents the best estimates possible in the circumstances.
Treated risk	As per risk matrix = **Low**
Stakeholder engagement	We are committed to operating our networks in a manner that is consistent with the long-term interests of our customers. To facilitate this, we conduct regular stakeholder engagement to understand and respond to the priorities of our customers and stakeholders. Feedback from stakeholders is built into our asset management considerations and is an important input when developing and reviewing our expenditure programs. Our customers have told us their top three priorities are price/affordability, reliability of supply, and maintaining public safety. They also told us they expect timely customer service by knowledgeable staff who demonstrate empathy and understanding in responding to queries or resolving issues. Further our IT systems are integral in supporting our day-to-day operations and it is important that our employees are equipped with the right tools to do their jobs effectively. In our last four Annual Employee Surveys, the disjointed IT systems that exist across the AGIG group have been highlighted as a key frustration of our employees. These frustrations centred around the disparate systems between the AGIG business units. For example, at the start of COVID-19 stay at home requirements, AGN employees could not join other AGIG employees on Microsoft Teams meetings, they had to use Microsoft Skype and sharing documents has to be done through dedicated network shares creating multiple instances of documents. The proposed AGIG IT Strategy & Roadmap will provide rationalised, fit-for-purpose IT systems across AGIG. This will be more cost effective over the medium to long term and will help us to realise greater efficiencies across the group, ultimately benefitting our customers through lower prices.
Other relevant documents	Attachment 9.9 IT Investment Plan

3.3 Background

The Multinet natural gas distribution networks deliver gas to over 700,000 consumers across metropolitan Melbourne and South Gippsland. To maintain integrity of services, and to allow us to manage data, communicate with customers, and conduct our day-to-day business, we rely heavily on IT systems, processes and infrastructure. Our stakeholders, regulators and customers have made it clear they value a reliable and responsive service, backed up by timely support and secure data handling. Having robust IT systems is integral to this.

In 2017, Australian Gas Networks (AGN), MGN and Dampier Bunbury Pipeline came together to form Australian Gas Infrastructure Group (AGIG). AGIG operates across multiple Australian jurisdictions, bringing together a wealth of expertise and experience that allows its various businesses to share knowledge, information and resources for the benefit of customers. This

business case relates to the proposed IT Strategy & Roadmap expenditure for the MGN business only.[19]

AGIG's scale and breadth of resources presents opportunity to deliver benefits for our customers in Victoria and Albury. Not least, it allows us to review and rationalise our IT systems and infrastructure across the group, moving to shared platforms where practicable.

We have already begun the IT rationalisation journey. In 2019, we developed the AGIG One IT strategy and roadmap (see Appendix A) to deliver stable and aligned IT management processes, architectures, procurement and certain core technology platforms across AGIG.

The process to develop the AGIG One IT program considered our needs as a group, the external context we operate in, technology drivers in our industry and the needs of each AGIG business based on the current IT landscapes and pre-planned initiatives. The individual initiatives within AGIG One IT were developed with input from technology specialists, business stakeholders and independent experts, and consideration of alignment to our vision, values and consistency with the NGR.

Our aim is to achieve economies of scale, while keeping pace with technological advances. This has required a focus on applications renewals, replacement and upgrades (see Application Renewals Business Case) to bring some of our legacy systems up to a reasonable standard.

The AGIG One IT program initiatives have been prioritised and allocated to each of the AGIG businesses. Wherever possible direct costs are allocated directly to the business incurring them. Shared costs are apportioned based on the benefit to each business, typically represented by either the proportion of overall AGIG revenue or FTEs, or shared equally – depending on the driver of the investment. In some cases, other drivers that better reflect the expected effort or benefits related to shared costs are used.

[19] Program expenditure for the AGN Victoria and Albury business is covered in a separate business case provided with the AGN Final Plan.

Figure 3-1: AGIG One IT Initiatives and basis for allocation

		Allocation Basis
Foundational Initiatives		
T4T-01	Rationalise and Consolidate Data Centre and Infrastructure Devices	Direct
T4T-02	Consolidate & Modernise Networks	Direct
T4T-03	Optimise End User Environment	FTE
T4T-04	Enhance the Collaboration and Communication Platform	FTE
T4T-05	Uplift Cyber Security Technology & Capabilities	Mix of equal & direct
T4T-06	Rationalise Application Integration Platforms	Direct
T4T-07A	Establish Data Architecture, Reporting & Governance: Improve Reporting Capabilities	Mix of revenue & direct
T4T-10	Uplift IT Operating Model and Governance	Revenue
Transformational Initiatives		
T4B-01	OneERP Stage 1 (DBP & AGN Finance)	Direct based on project
T4T-07	Establish Data Architecture, Reporting & Governance: Improve Reporting Capabilities, Optimise Data Management and Operations	Mix of revenue & direct
T4B-02	OneERP Stage 2 (MGN)	Direct
T4B-03	AGN Transition (inc OneERP Stage 3)	Direct

As at 31 December 2021, MGN accounted for 18.2% of overall revenue and 19.0% of overall FTE. MGN accounts for 20.0% of the effort for the AGIG operational technology cyber security activities, with the other 80.0% allocated to DBP. A summary of applicable allocators for shared AGIG One IT initiative costs over the next AA period is provided in Table 3-3

Table 3-3: Summary of AGIG shared cost allocators

Allocator	AGN			MGN	DBP
Equal	33.3%			33.3%	33.3%
Revenue	50.7%			18.2%	31.1%
FTE	18.5%			19.0%	62.5%
Customer numbers	Vic & Alb	SA	Other		
	56.7%	35.3%	8.1%		
OT				20.0%	80.0%

Table 3-4 outlines the initiatives in the AGIG One IT program, the estimated implementation timeframes, and the percentage of costs for each initiative allocated to MGN over the next AA period.

Table 3-4: MGN share of AGIG One IT program in the next AA period

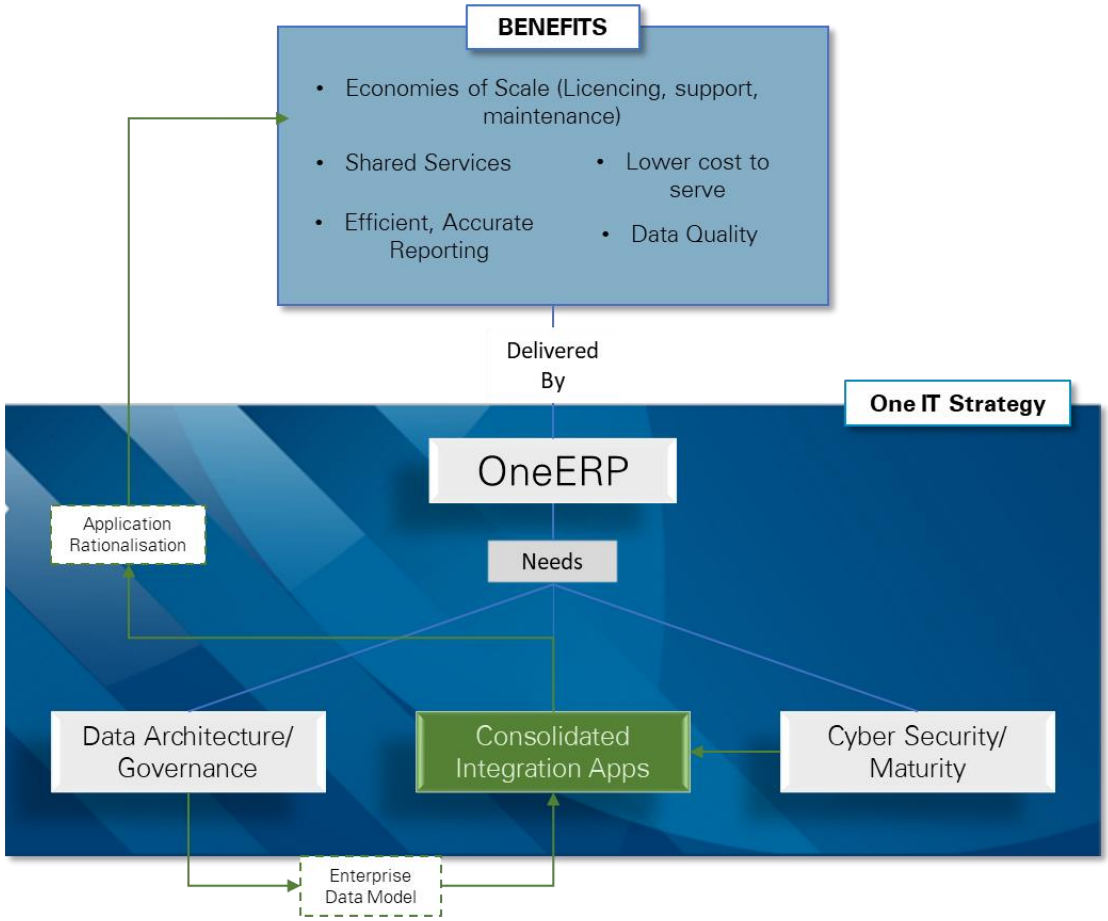
		MGN Allocation	2020	2021	2022	2023	2024	2025	2026	2027	2028	2029
Foundational Initiatives												
T4T-01	Rationalise and Consolidate Data Centre and Infrastructure Devices	N/A										
T4T-02	Consolidate & Modernise Networks	N/A										
T4T-03	Optimise End User Environment	N/A										
T4T-04	Enhance the Collaboration and Communication Platform	N/A										
T4T-05	Uplift Cyber Security Technology & Capabilities	16.5%										
T4T-06	Rationalise Application Integration Platforms	N/A										
T4T-07A	Establish Data Architecture, Reporting & Governance: Improve Reporting Capabilities	N/A										
T4T-10	Uplift IT Operating Model and Governance	N/A										
Transformational Initiatives												
T4B-01	OneERP Stage 1 (DBP & AGN Finance)	N/A										
T4T-07	Establish Data Architecture, Reporting & Governance: Improve Reporting Capabilities, Optimise Data Management and Operations	27.8%										
T4B-02	OneERP Stage 2 (MGN)	100%										
T4B-03	AGN Transition (inc OneERP Stage 3)	0%										

Work has already commenced, with AGN South Australia and DBP the most progressed in some of the key transformational initiatives such as OneERP. The foundational initiatives are well underway across the Group, with MGN's proportion of costs in the current AA period (including the six month extension) for initiatives underway totalling $12 million.

IT allowances for the current AA period were set in 2017, and therefore did not contemplate any of the AGIG IT Strategy & Roadmap activities. Despite this, we have been able to deliver some of these initiatives alongside those approved in the period.

For many of the initiatives underway, the remaining scope of work and investment over the next five years is key to deliver on the outcomes of the strategy and to realise any medium and long term benefits from the investment already undertaken. Figure 3-2 sets out the key benefits that will be delivered by the AGIG One IT program.

Figure 3-2: Benefits deliverable by the One IT program



Each of the initiatives are dependent on capabilities delivered by the other initiatives in order to achieve the full benefits of the broader strategy. For example, further benefits of the SAP S/4HANA ERP software become available when coupled with application integration and data management capabilities.

As shown in Table 3-4 above, most of the foundational activities will have been delivered by the end of the current AA period. During the next AA period, three initiatives (one foundational, two transformational) will be delivered:

- Foundational initiative:
  - Uplift Cyber Security Technology and Capabilities
- Transformational initiatives:

- OneERP
- Data Architecture, Reporting and Governance

Each of these initiatives will address some significant challenges across the MGN business. Table 3-5 summarises what each of the initiatives proposed for the next AA period will deliver, expressed across six themes.

Table 3-5: AGIG One IT themes

	Cyber Security Uplift	OneERP	Data Architecture, Reporting & Governance
Single Source of Truth 	Allows identity management of personnel and control of access rights to data and information. This also enables availability, confidentiality and integrity.	An enterprise wide ERP solution captures core business information necessary for decision making and smooth running of the business. Enables simpler, cheaper integration by simplifying the technology landscape and streamlines the consolidations of applications.	Enterprise Data Model (EDM) supports a common data language and ensures data is captured and consumed consistently using a federated implementation model to provide trusted and authoritative data
Standard Business Processes 	Enables consistent business continuity planning and disaster recovery for cyber events across the AGIG business entities.	Enables the consolidation of resources and the transferability of skills across the Group. Enables simpler, cheaper integration by transforming inefficient ad hoc processes for efficient ones and allows simpler, more cost effective integration.	Standardised information governance and content management practices enabled by group wide policy and processes to remove current challenges of the growing cost of data integration and information
Compliance & Risk Management 	Ensures alignment with regulations set by the Australian Energy Sector Cyber Security Framework (AESCSF), Australian Energy Market Operator (AEMO) and the Security of Critical Infrastructure (SOCI) Act.	Permits the abidance of standard regulatory requirements under AER and ASD. Facilitates adherence to regulatory requirements and optimisation of cyber security risk profiles. Reduces the risk of multiple data conversion and transformation processes.	Enables document and data security categorisation and retention. Facilitates secure access to information and reduces risks of data privacy and poor data quality.
Shared Resource Efficiencies 	A single consistent approach to cyber security reduces replication of infrastructure and processes across the group.	Limits resource discrepancies across the Group, maintaining a central hub for all users. Sharing of fixed costs granting access to high end functionality not otherwise available.	Single point of document management enables easier access to and sharing of information across the Group. Logical data warehouse based on data virtualisation for reuse of data and shared data access.

	Cyber Security Uplift	OneERP	Data Architecture, Reporting & Governance
		All entities receive access to resources in a consolidated space. Reduced complexity delivers lower operating and maintenance costs.	
Strategic Imperative 	Compliance with new critical infrastructure legislation and ongoing mitigation of the cyber threat landscape.	OneERP central to the group wide IT strategy of consolidating and sharing IT resources. Implementation of SAP PO is an integral part of the OneERP project enabling the overall Group strategy.	Strategic need to efficiently and effectively manage and share information internally and externally in compliance with our legal, regulatory and ethical obligations.
Customer 	Maintains integrity and security of the gas pipe network.	Quicker access to consolidated information enables provision of timely information to customers and improves customer service.	Easier access to timely and accurate information in response to customer requests and feedback. Also agile and efficient adoption of the new privacy legislation changes.

The three key initiatives are discussed in the following sections.

3.3.1 Uplift Cyber Security Technology and Capabilities program

All IT systems and technology infrastructure are exposed to cyber threats. The confidentiality, integrity and availability of information and information technology systems is critical to ensure our business can deliver its services effectively and in line with our various regulatory obligations and requirements, such as Critical Infrastructure Act, Security of Critical Infrastructure Act, Privacy Act and FIRB reporting obligations. This requires investment to ensure our systems are secure and remain resilient to external threats.

A consultation paper released by the Department of Home Affairs on 6 August 2020 outlined proposed amendments to the Security of Critical Infrastructure Act 2018 (SOCI Act), which were to require businesses in critical infrastructure sectors such as AGIG to meet baseline security and resilience standards. These proposed amendments were based on the following key findings:

- highly sophisticated nation states and state-sponsored actors continue to target governments and critical infrastructure providers;
- around 35% of incidents the ACSC responded to in the year to 30 June 2020 impacted critical infrastructure providers; and
- despite the Government's efforts to introduce reforms in 2018 to manage threats to its gas assets, "the threat environment is worsening".

On 2 December 2021 the SOCI Act was amended to apply new reporting obligations to critical assets. [20] This was followed by the introduction of the Security of Critical Infrastructure (application) Rules 2022, which took effect on 8 April 2022. 'Critical gas assets' are specified as being covered by this legislation.

Two new security obligations now apply to critical infrastructure assets:

1. the provision of operational and ownership information to the Register of Critical Infrastructure Assets (Part 2 of the SOCI Act); and
2. mandatory cyber incident reporting (Part 2B of the SOCI Act) for certain assets.

The rules related to cyber security contained in the legislation are as follows:

Rule 1 - Cyber and Information Security hazards

1. Responsible entities for critical infrastructure assets must, within 6 months of the commencement of this rule, ensure that their risk management program includes details of a risk based plan that outlines strategies and security controls as to how cyber and information security threats are being mitigated.

2. Responsible entities for critical infrastructure assets must, within 18 months of the commencement of this rule, ensure that their risk management program includes details of how the responsible entity complies with at least one of the following standards and frameworks:

(a) The Australian Cyber Security Centre's Essential Eight Maturity Model at maturity level one;
(b) AS ISO/IEC 27001:2015;
(c) The National Institute of Standards and Technology (NIST) Cybersecurity Framework;
(d) The Cybersecurity Capability Maturity Model (C2M2) at Maturity Indicator Level 1;
(e) Security Profile 1 of the Australian Energy Sector Cyber Security Framework; or
(f) an equivalent standard.

AGIG, being a critical infrastructure asset owner in the energy sector, has adopted the Australian Energy Sector Cyber Security Framework (AESCSF) as the compliance assessment framework most appropriate for our entity. The AESCSF has been developed through collaboration with industry and government stakeholders, including the Australian Energy Market Operator (AEMO), Australian Cyber Security Centre (ACSC), Cyber and Infrastructure Security Centre (CISC), and representatives from Australian energy organisations.

The AESCSF leverages recognised industry frameworks such as the US Department of Energy's Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2) and the National Institute of Standards and Technology Cyber Security Framework (NIST CSF), and references global best-practice control standards (e.g. ISO/IEC 27001, NIST SP 800-53, COBIT, etc.). The AESCSF also incorporates Australian-specific control references, such as the ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents, the Australian Privacy Principles (APPs), and the Notifiable Data Breaches (NDB) scheme.[21]

Under the current guidance from the 2022 framework, Security Profile 3 is the target state for organisations with an overall criticality rating of high. The AESCSF framework classifies AGIG, and each of its regulated pipeline and distribution businesses as a high criticality assets. This is because

[20] https://www.homeaffairs.gov.au/reports-and-publications/submissions-and-discussion-papers/protecting-our-critical-infrastructure-reforms-engagement

[21] https://aemo.com.au/en/initiatives/major-programs/cyber-security/aescsf-framework-and-resources

AGIG is a gas transmission and distribution business serving over 2 million customers across Australia. Achieving Security Profile 3 is identical to achieving Maturity Indicator Level (MIL) 3.

In 2022, the AESCSF is being reviewed to ensure that it remains fit for purpose and aligned with international best practice. A working group has been established to guide the review and update the AESCSF. The working group includes representation from electricity, gas and liquid fuels sub-sectors, AEMO, and governments. The revised AESCSF (version 2) is expected to be finalised in late2022. The Commonwealth Government expects to consult industry and states and territories about the future of the AESCSF in the second half of 2022.[22] Based on engagement to date on the AESCSF 2022 Assessment, it is expected energy sector critical infrastructure entities with this AESCSF criticality rating will be required to meet the AESCSF MIL-3 (Security Profile 3) level of compliance at some stage in the next AA period (2023/24 – 2027/28).

Using the maturity level framework outlined in the AESCSF, we have assessed the cyber security risks we face, and are targeting a state of MIL-3 by 2025. In 2020, we engaged EY to identify current gaps in achieving full implementation of all MIL-2 and MIL-3 practices within our IT architecture, and design a prioritised remediation roadmap that is fit-for-purpose.

EY's key findings and recommendations are summarised in Figure 3-3.

Figure 3-3: EY's key findings and recommendations in relation to AGIG's IT Security

Australian Government 2020 Strategy's "Actions by Businesses"	AGIG's Current Gaps	Proposed Roadmap Solutions
Improve baseline security for critical infrastructure	AGIG rates itself at MIL 1 which indicates that most baseline security practices have been implemented, but are only performed in an ad-hoc manner and lack the management characteristics that drive governance and continuous improvement.	▸ Reach MIL 3 by the end of 2025.
Uplift the cybersecurity of SMEs	AGIG's outsourced service providers are lacking the required skillset to continue to effectively protect AGIG from well-resourced and trained adversaries that conduct persistent intrusion campaigns targeting Australian critical infrastructure.	▸ Develop training for SMEs in respective cybersecurity domains. ▸ Enforce compliance with training requirements.
Provide secure products and services	AGIG's lack of visibility and accountability over its many organisational assets and reliance on outsourced service providers who do not consistently comply with AGIG's policies and procedures does not provide assurance that AGIG can secure its products and services.	▸ Develop a security framework that will include the development of a comprehensive asset register. ▸ Enforce compliance with AGIG's security framework across the organisation including external service providers.
Grow a skilled workforce	AGIG's IT function is currently under-resourced, comprising two FTEs responsible for the safe operation of AGIG's entire environment, and it is unable to continue to effectively develop and implement initiatives to improve AGIG's security posture.	▸ Onboard additional FTEs to support proposed uplift and BAU initiatives.
Take steps to block malicious activity at scale	AGIG's lack of an overarching SOC that facilitates an immediate and 24/7 response capability, reliance on outsourced service providers that do not share or aggregate risk, threat and vulnerability information, and a wide footprint means that AGIG may not be able to effectively detect and protect itself from malicious activity at scale.	▸ Establish an organisation-wide SOC that will monitor and respond to any anomalous or malicious activity.

Based on EY's recommendations, we have developed a 'Security Roadmap' (see Appendix B). This roadmap focuses effort on those areas of the business requiring uplift or improvement in cyber security as measured against the AESCSF.

The Uplift Cyber Security Technology and Capabilities program ensures all elements of the AESCSF can be established and maintained at the MIL-3 level. The work program comprises the following key initiatives:

- Workforce management – onboard additional internal resources to support the establishment and operationalisation of roadmap initiatives and subsequent BAU activities.

22 https://aemo.com.au/-/media/files/initiatives/cyber-security/aescsf/aescsf-framework-overview.pdf?la=en

- Incident management – establish and implement an organisational incident management framework to detect, analyse, and respond to cybersecurity events and build resilience.
- Identity and access management – establish and implement a comprehensive identity and access management framework to control access to AGIG's assets and protect the IT and OT infrastructures.
- Threat and vulnerability management – establish and implement an organisational threat and vulnerability program to detect, identify, analyse, manage and respond to threats and vulnerabilities.
- Situational awareness – develop a framework to manage situational awareness capabilities to form a common operating picture.
- Third party risk management – establish and implement a third party risk management framework to manage the cybersecurity risks associated with services and assets that are dependent on external entities.

The costs of this program will be shared between each of the AGIG businesses, with shared costs allocated based on total revenue.

3.3.2 OneERP

The OneERP initiative seeks to develop and implement consistent processes across AGIG, moving all businesses on to a single enterprise resource planning (ERP) platform. This initiative will see the establishment of finance shared services. This will help improve organisational agility and productivity by providing standardised business processes, and a central location for finance data that will enable consistent and effective reporting processes.

OneERP commenced in 2020/21, with development of Stage 1 (focused on DBP and AGN Finance). This project focuses on developing and implementing consistent finance processes, reporting and reporting procedures, budgeting and auditing. It will also build capability for statutory, tax, regulatory and other special purpose accounting and allow business performance monitoring functions to be automated and consistently applied across AGIG.

The project will replace the existing disparate ERP systems (DBP's Microsoft Dynamics and AGN's SAP Business One) with the new industry-standard SAP S/4 HANA and will provide the platform that MGN and AGN Operational will also transition to, leveraging and building on work already completed in DBP and AGN Finance.

The AGIG One IT program proposed to commence the project to replace ERPs for:

- DBP from 2021;
- AGN from 2022; and

A.1 Multinet Gas Networks by 2025.

More detailed project planning done for the first phase found there were benefits in combining the DBP and AGN Finance ERP replacements. The DBP and AGN Finance project is due to be completed in 2022/23, at which point planning will begin on the MGN project.

The OneERP initiative is expected to be completed by 2026/27 and will achieve an aligned finance environment across AGIG which will provide supporting tools and standardised processes in line with good industry practice. MGN's existing SAP ERP and ISU Billing systems reach end of support in 2025 and 2027 respectively, we have therefore designed the program timing and upgrades to enable a seamless transition to SAP S/4 HANA as these systems roll off.

More information on the OneERP initiative is provided in Appendix C.

3.3.3 Data Architecture, Reporting and Governance

To enable any business to operate more effectively, it is important to have a single source of the truth for critical business core data. When several business come together under one umbrella (as per AGIG in 2017), one of the most important IT challenges is to standardise and consolidate the different suite of applications, data and integration approaches that exist across each of the entities. While this is often a complex exercise, consolidating data and data governance offers some of the greatest opportunities for efficiency and improving service outcomes for customers. Having a single source of the truth enables businesses to share costs, reduce risk exposure, improve the quality and efficiency of reporting, and provide consistent and timely information to customers.

The Data Architecture and Governance program will deliver an enterprise data model (EDM) and associated data governance framework, which will apply to AGN, DBP and MGN. An EDM describes the types of information that are important to an enterprise, allowing more efficient application implementations, integration, and business reporting. An EDM eliminates the need to source, aggregate and reconcile data manually. This is particularly beneficial for regulatory reporting, as it reduces the potential for errors, discrepancies, and the costs associated with addressing those discrepancies.

AGIG's proposed data architecture will be consistent with the OneERP initiative. Data governance will be implemented and supported by data foundation capabilities including:

- Data risk management – identification of regulatory, legislative and business drivers for data retention, as well as data protection driven by information classification
- Metadata management – cataloguing, classifying and tagging data enabling informed data migration, archiving and storage needs, also enabling dynamic metadata to improve usability and efficiency of data
- Data quality management – developing data standards and associated data quality metrics to enable data quality to be assessed, improved and monitored on an ongoing basis. Technology enabled master data management (MDM) ensures the uniformity, accuracy and accountability of shared master data assets. There is a great opportunity for AGIG to introduce MDM while it is implementing common ERP system for all entities. This program of work triggers important decisions on authoring systems for each of master data entities and even their attributes

As AGIG develops OneERP, there will be a growing demand for this corporate data, particularly for business reporting and analytics. The long-term strategic goal is to implement the data architecture based on the principle for AGIG data to reside only in two places: the source system (e.g., CRM) and the data analytical platform (e.g. data lakehouse). However, AGIG needs to establish mature data management processes, standardise reporting tools, and develop a federated model with overlaying data governance before achieving that long-term strategic goal.

A logical data warehouse with the help of data virtualisation will allow AGN to pull data from multiple systems and store it in a structured manner. The predefined relationships between the data sets (utilising the EDM) will allow information from solutions such as SAP, EAM and GIS to be collated to provide insights and comprehensive analytics as well as limited trending capability.

As part of this program, we will also uplift AGIG's content management capabilities. As part of the foundational initiatives we consolidated multiple Microsoft SharePoint versions across the business entities and archived unsupported systems. The next step is to implement information classification and metadata management on SharePoint online. Our long-term goal is to reduce or completely eliminate the use of shared drives and Outlook folders as storages, and instead fully utilise modern capabilities provided in SharePoint, Teams and OneDrive.

Implementing an enterprise content management (ECM) solution will bring all content together, boosting productivity and effective decision making. We can drive operational efficiencies by our

staff knowing where they need to look for information, allowing us to spend more time in analysis rather than sourcing and connecting the information.

In summary, the Data Architecture, Reporting and Governance initiatives will allow AGIG to:

- stay compliant and improve data-driven decision making;
- access fully traceable and documented evidence to respond to regulatory information requests;
- streamline business processes by having greater ability to coordinate and identify efficiencies in operations (e.g. asset maintenance);
- reduce the cost of information through improved productivity and reduction in manual effort required to gather and collate data from disparate and siloed sources (for example, we expect that a quality information management approach will streamline and therefore reduce cost and risk associated with audits); and
- improve user experience by introducing a consolidated technology platform for managing AGN's content, allowing for rigorous information management.

Further information on the data architecture, reporting and governance initiative is provided in Appendix D.

3.4 Risk assessment

Risk management is a constant cycle of identification, analysis, treatment, monitoring, reporting and then back to identification (as illustrated in Figure 1.2). When considering risk and determining the appropriate mitigation activities, we seek to balance the risk outcome with our delivery capabilities and cost implications. Consistent with stakeholder expectations, safety and reliability of supply are our highest priorities.

Figure 3-4: Risk management principles

Our risk assessment approach focuses on understanding the potential severity of failure events associated with each asset and the likelihood that the event will occur. Based on these two key inputs, the risk assessment and derived risk rating then guides the actions required to reduce or manage the risk to an acceptable level.

Our risk management framework is based on:

- AS/NZS ISO 31000 Risk Management – Principles and Guidelines,
- AS 2885 Pipelines-Gas and Liquid Petroleum; and
- AS/NZS 4645 Gas Distribution Network Management.

The Gas Safety Act 1997 and Gas Regulations 2012, through their incorporation of AS/NZS 4645 and the Work Health and Safety Act 2012, place a regulatory obligation and requirement on us to reduce risks rated high or extreme to low or negligible as soon as possible (immediately if extreme). If it is not possible to reduce the risk to low or negligible, then we must reduce the risk to as low as reasonably practicable (ALARP).

When assessing risk for the purpose of investment decisions, rather than analysing all conceivable risks associated with an asset, we look at credible, primary risk events to test the level of investment required. Where a credible risk event has an overall risk rating of intermediate or higher, we will undertake investment to reduce the risk.

Six consequence categories are considered for each type of risk:

1. **People** – injuries or illness to employees and contractors or members of the public
2. **Supply** – disruption in the provision of services/supply, impacting customers
3. **Environment** (including heritage) – impact on the surroundings in which the asset operates, including natural, built and Aboriginal cultural heritage, soil, water, vegetation, fauna, air and their interrelationships
4. **Reputation** – impact on stakeholders' opinion of MGN/AGIG, including personnel, customers, investors, security holders, regulators and the community
5. **Financial** – financial impact on MGN/AGIG
6. **Compliance** – the impact from non-compliance with operating licences, legal, regulatory, contractual obligations, debt financing covenants or reporting / disclosure requirements

Note that risk is not the sole determinant of what investment is required. Many other factors such as growth, cost, efficiency, sustainability, and the future of the network are also considered when we develop technology solutions. The risk management framework provides a valuable tool to manage our assets, and prioritise our works program, however it is not designed to provide a binary (yes/no) trigger for investment. As prudent asset managers, we apply our experience and discretion to manage and invest in our technology for our distribution networks in the best interests of existing and potential customers.

A summary of our Risk Management Framework, including definitions, has been provided as Attachment 9.5 to our Final Plan.

The primary risk event being assessed is that maintaining disparate or legacy IT systems, management and procurement arrangements across AGIG (or in AGN/MGN compared to the other AGIG businesses) will compromise our ability to maintain an IT environment that is robust and resilient to cyber threats (and effectively deliver cyber security training that accurately covers the breadth of our IT environment to our employees). This could leave us vulnerable to a cyber-attack, resulting in system failure with the potential to impact customer services and at significant remediation costs. It could also result in release of sensitive information, which would breach our regulatory obligations and negatively affect our reputation.

Security breaches, unavailability of corporate or operational systems and release of sensitive information gives rise to people, customer/reputational, compliance and financial consequences, as follows:

- *People* – a security breach resulting from a successful phishing attack on an employee can have an impact on employee security, morale and mental wellbeing. There is also the ongoing risk of employee frustration as a result of not being able to access and share information across AGIG efficiently.
- *Reputation and customer* – a security breach may result in confidential customer data being compromised which in turn can impact on our reputation. There also remains an ongoing reputational risk resulting from having disparate, incompatible IT systems across the businesses within AGIG, meaning consumers receive a varying customer experience in each jurisdiction.
- *Financial* – a security breach rendering our corporate or operational systems unavailable may result in us incurring significant remediation costs.

- *Compliance* – a security breach rendering our corporate systems unavailable may result in us not complying with a range of legal and regulatory reporting obligations, for example service standards set out in the Gas Distribution System Code.[23]

We estimate the overall risk rating if the risk to corporate and operational systems is not addressed is intermediate. While the likelihood of most risks occurring are rated unlikely, the ongoing issues with disparate systems lead to a people and reputational risk likelihood of occasional. The risk consequences for people, reputation, financial and compliance are rated severe.

The untreated risk[24] rating is presented in Table 3-6.

Table 3-6: Risk rating – untreated risk - MGN

Untreated risk	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Occasional	Unlikely	Unlikely	Occasional	Unlikely	Unlikely	Intermediate
Consequence	Severe	Minor	Trivial	Severe	Severe	Severe	
Risk Level	Intermediate	Low	Negligible	Intermediate	Intermediate	Intermediate	

3.5 Options considered

The following options have been identified to address the identified risks with maintaining disparate IT environments across AGIG, or within AGN compared to other AGIG businesses, as well as the opportunities to reduce medium and long term costs through rationalisation, streamlining, and access to economies of scale. These options have been assessed with consideration of the investment that has been undertaken/committed through to 31 December 2021.

- **Option 1** – Do nothing more, halt AGIG One IT investment and continue to run disparate IT environments across AGIG;
- **Option 2** – Undertake foundational AGIG IT initiatives only; or
- **Option 3** – Undertake foundational and transformational initiatives in line with the AGIG One IT program.

These options are discussed in the following sections.

3.5.1 Option 1 – Do nothing more

Option 1 would see cessation of all AGIG One IT program initiatives currently under way and we would continue to run disparate IT environments across AGIG.

In particular, under this option we would not complete the following initiatives that are underway:

- Uplift Cyber Security Technology & Capabilities
- While we would complete the Phase 1 of the OneERP project to deliver a single ERP platform for DBP and AGN, we would not implement the following transformational initiatives:
- AGIG wide OneERP capability; and
- Establish Data Architecture, Reporting and Governance: Improve Reporting Capabilities and Optimise Data Management and Operations.

[23] https://www.esc.vic.gov.au/sites/default/files/documents/Gas-Distribution-System-Code-version-14.pdf

[24] Untreated risk is the risk level assuming there are no risk controls currently in place. Also known as the 'absolute risk'.

This means the full benefits of the OneERP project (such as enabling improved reporting capabilities and optimising data management and operations) would not be delivered.

3.5.1.1 Cost assessment

As this option would see us implement no further AGIG One IT initiatives past 30 June 2023 it requires $0 upfront capex in the next AA period. In the medium to long term this approach would see us incur additional opex costs in the management of disparate IT systems, and forego the opportunity to rationalise and streamline our IT environments and corporate processes across AGIG.

For many of the AGIG One IT initiatives underway, the remaining scope of work and investment over the next five years is key to deliver on the outcomes of the strategy and to realise any medium and long term benefits from the investment already undertaken.

3.5.1.2 Risk assessment

Option 1 will not deliver the uplift cyber security technology and capabilities identified as required to ensure our corporate IT environment is robust and resilient to cyber threats. As such it leaves the untreated risk unchanged as shown in Table 3-7.

Table 3-7: Risk assessment – Option 1

Option 1	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Occasional	Unlikely	Unlikely	Occasional	Unlikely	Unlikely	Intermediate
Consequence	Severe	Minor	Trivial	Severe	Severe	Severe	
Risk Level	Intermediate	Low	Negligible	Intermediate	Intermediate	Intermediate	

This option is not consistent with the requirements of our risk management framework, which requires us to address high or intermediate risks to low or as low as reasonably practicable (ALARP).

3.5.1.3 Alignment with vision objectives

Table 3-8: Alignment with vision – Option 1

Vision objective	Alignment
Delivering for Customers – Public Safety	-
Delivering for Customers – Reliability	-
Delivering for Customers – Customer Service	N
A Good Employer – Health and Safety	N
A Good Employer – Employee Engagement	N
A Good Employer – Skills Development	-
Sustainably Cost Efficient – Working within Industry Benchmarks	N
Sustainably Cost Efficient – Delivering Profitable Growth	-
Sustainably Cost Efficient – Environmentally and Socially Responsible	N

Option 1 does not align with our objective of *Delivering for Customers*, as it will not allow us to uplift our IT capabilities and provide a level of service commensurate with that expected by our customers. It will not enable effective collaboration and access to timely and accurate information relating to customer service.

Option 1 also does not align with being *A Good Employer*. It would see continued employee frustration (as indicated in the 2019 engagement survey) that the current disparate systems do not allow for collaboration across AGIG entities and hinders access to timely and accurate information.

Further, it will compromise our ability to effectively deliver cyber security training that accurately covers the breadth of our IT environment to our employees. A security breach resulting from a successful phishing attack on an employee may have adverse effects to employee mental wellbeing.

Option 1 is not *Sustainably Cost Efficient* as it will not allow us to uplift our systems to a level commensurate with industry standards. More significantly, we will forego the opportunity to achieve economies of scale and leverage cost savings by having standard IT systems and processes rolled out across AGIG.

3.5.2 Option 2 – Foundational initiatives

This option would see us complete the foundational initiatives identified in the AGIG One IT program, but we would not deliver the transformational initiatives. In particular, under this option we would complete only the Uplift Cyber Security Technology & Capabilities initiative.

A number of foundational initiatives are underway, with many complete or to be completed by June 2023. Together these initiatives have:

- rationalised and consolidated data centre and infrastructure devices (T4T-01);
- consolidated and modernised networks (T4T-02);
- optimised end user environment and enhancement of the collaboration and communication platform (T4T-03 and 04);
- implemented a number of cyber security technologies and capabilities as part of a longer roadmap to reach MIL-3 level cyber risk management (T4T-05)
- development of AGIG content management, reporting and analytics and information governance strategies (T4T-07A);
- uplifted the IT operating model and governance (T4T-10) and;
- rolled out OneERP Stage 1 and rationalised application integration platforms for DBP and AGN Finance (T4B-02 Stage 1).

Finishing the foundational initiatives will bring the AGIG businesses into a more coherent and consolidated IT environment. However, if the subsequent transformational initiatives are not delivered, AGIG will not realise the full benefits of the Strategy, and sub-optimal data sharing, inefficient and inconsistent business processes and IT practices will remain.

From a business perspective, while ceasing the program at the foundational level is a practicable option, it makes little commercial sense not to follow through with the transformation aspect of the strategy. Moreover, if AGIG was to pause the program after the foundational initiatives, but then sought to continue the transformational aspects later, it is likely to result in re-work and additional costs from having to ramp-up resources, and re-test assumptions and technical solutions.

3.5.2.1 Cost assessment

The forecast direct capital cost of this option is $2.5 million over the next AA period. There is also an opex step change of $3.3 million. The profile of spend is provided in Table 3-9 and builds on the $12 million already invested on AGIG One IT initiatives for MGN in the current AA period.

Table 3-9: Cost estimate – Option 2, $'000 real 2021

Option 2	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Capex	605	825	582	226	246	2,484
Opex	522	522	622	839	839	3,345

Total	**1,127**	**1,347**	**1,204**	**1,065**	**1,085**	**5,829**

The key driver for this option is to ensure we uplift our cyber security technology and capability in line with legislative requirements, risk and good practice cyber risk management

3.5.2.2 Risk assessment

This option does not reduce the risk from intermediate. Delivering the foundational initiatives in the AGIG One IT program is only the first step in the IT improvement and consolidation journey, therefore the full suite of risk mitigations will not take effect.

The foundational initiatives will reduce the likelihood of people and reputational risk from rated occasional to unlikely, as it represents an improvement on the existing systems. We therefore expect instances of employee frustrations as well as the likelihood of reputational damage to decrease. However, this option does not fully implement rationalised and streamlined processes, therefore the risk likelihood would not be reduced to remote. The overall risk therefore remains intermediate.

Table 3-10: Risk assessment – Option 2

Option 2	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Intermediate
Consequence	Severe	Minor	Trivial	Severe	Severe	Severe	
Risk Level	Intermediate	Low	Negligible	Intermediate	Intermediate	Intermediate	

Option 2 is not aligned with our risk management framework as it does not reduce the currently intermediate risk to low or ALARP. We consider delivering the full suite of transformational initiatives is a practicable and affordable alternative to solely delivering the foundational initiatives, and that the transformational initiatives that would reduce the risk rating further. Therefore Option 2 is not considered ALARP.

3.5.2.3 Alignment with vision objectives

Table 3-11 shows how Option 2 aligns with our vision objectives.

Table 3-11: Alignment with vision – Option 2

Vision objective	Alignment
Delivering for Customers – Public Safety	-
Delivering for Customers – Reliability	-
Delivering for Customers – Customer Service	Y
A Good Employer – Health and Safety	Y
A Good Employer – Employee Engagement	N
A Good Employer – Skills Development	-
Sustainably Cost Efficient – Working within Industry Benchmarks	N
Sustainably Cost Efficient – Delivering Profitable Growth	-
Sustainably Cost Efficient – Environmentally and Socially Responsible	Y

Option 2 aligns with our objective of *Delivering for Customers* as it would provide robust and resilient corporate systems with a reduced risk of a security breach that could compromise sensitive customer information.

Completing the foundational AGIG One IT program initiatives would address employee health & safety risks associated with potential phishing attacks. However, it does not meet all known

employee frustrations that the current disparate systems hinders access to timely and accurate information. It therefore only partially meets our vision objective of being *A Good Employer*.

Option 2 partially aligns with being *Sustainably Cost Efficient*. It will deliver cyber technology and capabilities that are in line with good industry practice and aligned across AGIG. However, not delivering the OneERP and Data architecture, reporting and governance projects in full means we cannot streamline a number of core business processes that support business reporting and decision making, adding unnecessary complexity and cost over the medium to long term.

3.5.3 Option 3 – Foundational and transformational initiatives

This option would see the full delivery of foundational and transformational initiatives identified in the AGIG One IT program, plus further transformation initiatives that follow on from the completion of the current Roadmap. In particular, under this option we would complete the Uplift Cyber Security Technology & Capabilities that is underway.

We would also implement the following transformational initiatives:

- OneERP
- Establish Data Architecture, Reporting and Governance: Improve Reporting Capabilities and Optimise Data Management and Operations

As outlined under Option 2, a number of the AGIG IT Strategy initiatives are already completed or underway. This includes Stage 1 of the OneERP transformational initiative. In particular, the initiatives completed to June 2023 have:

- rationalised and consolidated data centre and infrastructure devices (T4T-01);
- consolidated and modernised networks (T4T-02);
- optimised end user environment and enhancement of the collaboration and communication platform (T4T-03 and 04);
- implemented a number of cyber security technologies and capabilities as part of a longer roadmap to reach MIL-3 level cyber risk management (T4T-05)
- development of AGIG content management, reporting and analytics and information governance strategies (T4T-07A); and
- uplifted the IT operating model and governance (T4T-10) and;
- rolled out OneERP Stage 1 and rationalised application integration platforms for DBP and AGN Finance, (T4B-02 Stage 1).

The OneERP project is the most significant cost component in this business case, accounting for 87 per cent of the capital cost of the overall program. OneERP commenced in 2020/21, with delivery of the DBP and AGN Finance project, with the focus of developing and implementing consistent finance processes, reporting and reporting procedures, budgeting and auditing. It will also build capability for statutory, tax, regulatory and other special purpose accounting and allow business performance monitoring functions to be automated and consistently applied across AGIG.

The next phase of the project will replace the existing end-of-life SAP ECC systems employed at MGN for ERP, EAM and ISU Billing with the new industry-standard SAP S/4 HANA and will leverage and build on work already completed in DBP and AGN Finance. The OneERP initiative is expected to be completed by 2026/27 and will achieve an aligned finance environment across AGIG, which will provide supporting tools and standardised processes in line with good industry practice.

3.5.3.1 Cost assessment

The forecast direct capital cost of this option is $37 million over the next AA period. There is also an opex step change of $3.3 million. The profile of spend is provided in Table 3-12 and builds on the $12 million already invested on AGIG One IT Roadmap initiatives for MGN in the current AA period.

Table 3-12: Cost estimate – Option 3, $'000 real 2021

Option 3	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Capex	9,169	20,251	6,672	226	246	36,565
Opex	522	522	622	839	839	3,345
Total	**9,692**	**20,773**	**7,295**	**1,065**	**1,085**	**39,910**

The key additional cost in this option is the OneERP initiative ($32 million).

3.5.3.2 Risk assessment

This option reduces the risk from intermediate to low. Delivering the full program of foundational and transformational initiatives identified in the AGIG One IT program reduces the likelihood of people, compliance, reputational and financial risks arising from unlikely to remote. This is because systems are integrated, information sharing capability between businesses is dramatically improved, and the robustness of corporate systems means a significant security breach is less likely to occur.

Table 3-13: Risk assessment – Option 3

Option 3	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Remote	Remote	Unlikely	Remote	Remote	Remote	Low
Consequence	Severe	Minor	Trivial	Severe	Severe	Severe	
Risk Level	Low	Low	Negligible	Low	Low	Low	

Option 3 therefore aligns with our risk management framework, as it reduces the current intermediate risk rating to low.

3.5.3.3 Alignment with vision objectives

Table 3-14 shows how Option 3 aligns with our vision objectives.

Table 3-14: Alignment with vision – Option 3

Vision objective	Alignment
Delivering for Customers – Public Safety	-
Delivering for Customers – Reliability	-
Delivering for Customers – Customer Service	Y
A Good Employer – Health and Safety	Y
A Good Employer – Employee Engagement	Y
A Good Employer – Skills Development	-
Sustainably Cost Efficient – Working within Industry Benchmarks	Y
Sustainably Cost Efficient – Delivering Profitable Growth	-
Sustainably Cost Efficient – Environmentally and Socially Responsible	Y

Option 3 aligns with our objective of *Delivering for Customers*. Specifically, it provides robust and resilient corporate systems with a reduced risk of a security breach that could compromise sensitive customer information. IT capability will be uplifted to a level commensurate with our customers'

expectations. It will also enable effective collaboration and access to timely and accurate information relating to customer service.

Completing the foundational and transformational AGIG One IT program initiatives would address a known employee frustration and provide a consistent IT experience and effective systems of collaboration for employees. It will also provide an improved toolset and consistent processes for key reporting functions. It therefore meets our vision objective of being *A Good Employer*.

Option 3 is consistent with being *Sustainably Cost Efficient* as it will deliver cyber technology and capabilities that are in line with good industry practice and aligned across AGIG. It will also provide effective systems of collaboration for employees, rationalise the costs of IT system management and procurement and streamline core business processes to support business reporting and decision making, removing unnecessary complexity and cost over the medium to long term. It will reduce manual data manipulation and allow more dynamic analysis, which is likely to lead to improved productivity and better-informed decision making.

3.6 Summary of costs and benefits

Table 3-15 presents a summary of how each option compares in terms of the estimated cost, the treated risk and alignment with our vision objectives.

Table 3-15: Comparison of options

Option	Estimated cost ($ million 2021)	Treated residual risk rating	Alignment with vision objectives
Option 1	0	Intermediate (not ALARP)	Does not align with *Delivering for Customers, A Good Employer* or *Sustainably Cost Efficient*
Option 2	$2.5m capex $3.3m opex step change	Intermediate (not ALARP)	Aligns with *Delivering for Customers* , partially aligns with being *A Good Employer* and is not as S*ustainably Cost Efficient* as Option 3.
Option 3	$36.6m capex $3.3m opex step change	Low	Aligns with *Delivering for Customers, A Good Employer* and is more *Sustainably Cost Efficient* than Option 2.

3.7 Recommended option

Option 3, to implement the full program of foundational and transformational AGIG One IT program initiatives in the next AA period is the proposed solution.

Under this option we will invest $37 million on the following initiatives:

- Foundational initiative:
  - Uplift Cyber Security Technology and Capabilities
- Transformational initiatives:
  - OneERP
  - Data Architecture, Reporting and Governance

These initiatives will be delivered through a mix of internal and external resources under the governance and management of the AGIG Group IT project controls.

3.7.1 Why is the recommended option prudent?

Option 3 is recommended because:

- it aligns AGN's IT environment to standardised architectures, platforms, management and support processes across AGIG which will;
  - ensure consistency for employees, management and customers when accessing and using information to make decisions;
  - enable effective collaboration across AGIG which was identified as a frustration in a number of our recent annual employee engagement surveys;
  - reduce the risks associated with unmanaged document control caused by the current file sharing, rather than collaboration, systems;
  - align our systems to a standardised and industry good practice approach to cyber security which will ensure that systems are robust and resilient to threats, that threats can be appropriately mitigated or rectified and that the costs of managing cyber technology and capabilities are as low as possible; and

- allow for our corporate finance processes to be standardised and delivered through an industry leading enterprise resource planning system that can deliver dynamic, automated, accurate and timely reporting across a number of accounting needs, reducing complexity and ongoing costs in subsequent AA periods;

- reduces the untreated risk to low in line with our risk management framework;
- is consistent with stakeholder requirements and our vision;
- the delivery of the scope of works is achievable in the time frame envisaged;
- builds on investments already made in the current AA period; and
- unlocks the medium to long-term benefits of economies of scale and being able to leverage cost savings from having standard IT systems and processes rolled out across AGIG.

3.7.2 Estimating efficient costs

The AGIG One IT program project developed high level costing estimates for each of the identified initiatives. These cost estimates were developed by an independent expert and were informed by significant engagement with internal stakeholders to understand the current environment and business requirements, sourcing market and vendor quotes and advice, industry norms and historical costs of delivering similar projects (both within AGIG businesses and with other clients of the independent expert).

We continue to update our cost estimates as the program of work progresses to incorporate new information including what we have learned from the delivery of initiatives to date, as well as further planning work undertaken for individual initiatives.

The total costs for each of the initiatives is summarised in Appendix F.

All costings in the body of this business case represent MGN's proportion of total cost. The proportion of cost allocated to each AGIG business has been determined based on the relative value each receives from the project (typically represented by proportion of overall revenue or FTE).

As at 31 December 2021, MGN accounted for 18.2% of AGIG revenue and 19.0% of AGIG FTE.

The total project costs consider the internal labour, external labour and materials/other costs to deliver the project. The forecast capital cost breakdown by initiative is shown in Table 3-16 below.

Table 3-16: MGN AGIG One IT initiatives for the next AA period, $'000 real 2021

Code	Initiative	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Foundational initiatives							
T4T-05	Uplift Cyber Security Technology & Capabilities	605	825	582	226	246	2,484
Total foundational		605	825	582	226	246	2,484
Transformational initiatives							
T4T-07A&B	Establish Data Architecture, Reporting & Governance	1,598	615	-	-	-	2,213
T4B-02	OneERP	6,966	18,811	6,091	-	-	31,867
Total transformational		8,564	19,426	6,091	-	-	34,081

Total all initiatives	**9,169**	**20,251**	**6,672**	**226**	**246**	**36,565**

A detailed forecast cost breakdown of each initiative is provided in the Appendices.

There is also an opex step change of $3 million associated with the Uplift in Cyber Security Technology and Capabilities aspect of this project in the next AA period. The opex step change is calculated in Table 3-17.

Table 3-17: Cyber opex step change, $'000 real 2021

	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Cyber opex IT (A)	1,168	1,168	1,268	1,385	1,385	6,373
Cyber opex OT (B)	-	-	-	100	100	200
Cyber opex base year (C)	646	646	646	646	646	3,228
Opex step change (A + B - C)	**522**	**522**	**622**	**839**	**839**	**3,345**

3.7.3 Consistency with the National Gas Rules

In developing these forecasts, we have had regard to Rule 79 and Rule 74 of the NGR. With regard to all projects, and as a prudent asset manager/network business, we give careful consideration to whether capex is conforming from a number of perspectives before committing to capital investment.

NGR 79(1)

The proposed solution is prudent, efficient, consistent with accepted and good industry practice and will achieve the lowest sustainable cost of delivering pipeline services:

- **Prudent** – The investment is necessary in order to maintain the integrity of IT systems. The proposed initiatives are the most practical and effective option to appropriately support our employees and management in prudently managing our networks, and provide timely customer support. It is therefore of a nature that a prudent service provider would incur.
- **Efficient** – The proposed initiatives were developed by an independent expert with significant engagement with internal stakeholders across AGIG. They will rationalise and streamline IT environments and associated business processes across AGIG reducing medium to long term costs (of both system support costs and associated business processes). The cost estimates reflect independent expert costing and market information available at the time. The expenditure is therefore of a nature that a prudent service provider acting efficiently would incur.
- **Consistent with accepted and good industry practice** – The proposed initiatives will deliver enterprise resource planning and cyber technology and capabilities that are consistent with accepted and good industry practice. In particular, highly customised financial and reporting processes is not recognised as good industry practice, and owners of critical infrastructure are increasing their understanding, management and investment in cyber security to reduce the risk of adverse impact of a cyber-attack to the environment and customers.
- **To achieve the lowest sustainable cost of delivering pipeline services** – The OneERP initiative is necessary to simplify the management of finance across AGIG and avoid future risks and costs associated with heavily customised finance operations. Failure to address cyber risk would increase the likelihood and impacts of an adverse impact of a cyber event that could cause significant people, compliance, reputational and financial impacts for us and our customers. Improved collaboration, data management and reporting is also likely to enable

efficiencies in future AA periods. This project is therefore consistent with the objective of achieving the lowest sustainable cost of delivering services.

NGR 79(2)

The proposed capex is justifiable under NGR 79(2)(c)(ii), as it is necessary to maintain the integrity of services. Cyber risk is increasing in our industry and having aligned cyber technology and capabilities across AGIG ensures our systems are robust and resilient to cyber-attack. Differing IT environments does not lend well to a coordinated and effective approach to cyber security at the lowest possible cost. It is therefore important that IT environments and cyber technology and capabilities are aligned.

Our OneERP initiative will introduce more automated, accurate, dynamic and timely reporting across a number of business needs, improving management's access to information when making decisions. The medium to long term costs and risks associated with disparate finance processes and systems across AGIG are likely to be material in terms of extra staffing costs, re-work, additional training and errors (which could lead to less optimal decisions that impact the integrity of other network assets).

We therefore consider Option 3 best meets the requirements of NGR 79(2).

NGR 74

The forecast costs are based on the latest market rate testing and project options were developed by an independent expert as part of the AGIG One IT process. The estimates continue to be updated for new information such as actual cost incurred to date and further planning work on individual initiatives. The estimates have therefore been arrived at on a reasonable basis and represent the best estimate possible in the circumstances.

Appendix A AGIG One IT program

Appendix B Uplift Cyber Security Technology and Capability

B.1 Initiative overview

The AGIG cyber security uplift program is in progress. It has been designed to implement and embed uplifted cyber security capabilities throughout all AGIG entities. Delivering these capabilities nationally will ensure we, at a minimum, efficiently:

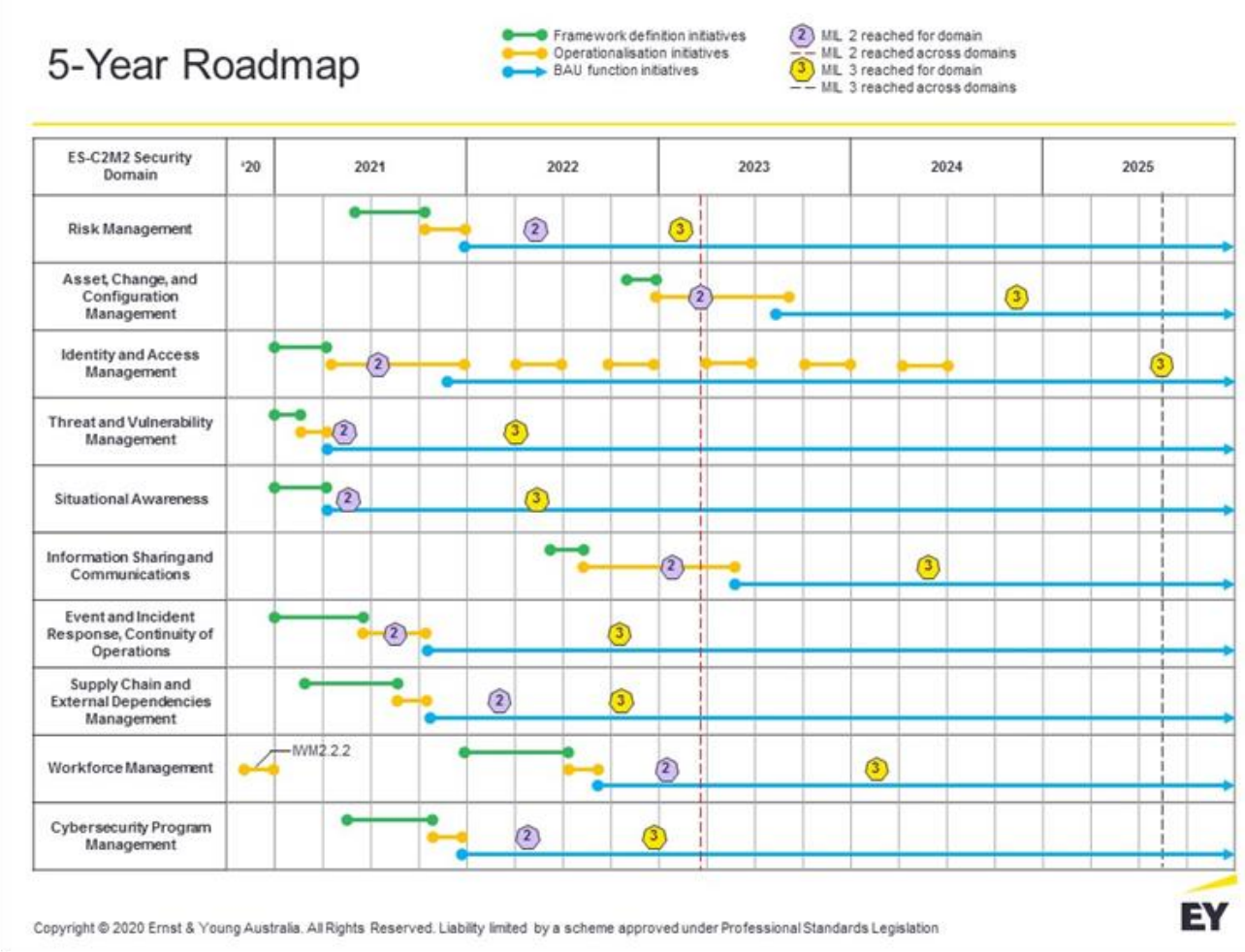
- meet the regulatory compliance obligations of the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 on gas infrastructure entities; and
- meet cyber security related obligations under our Foreign Investment Review Board (FIRB) conditions; plus
- achieve MIL-3 (Security Profile 3) capabilities under the AESCSF in the next AA period
- ensure cyber security risks are managed appropriately across all AGIG entities.

We will achieve MIL-3 (Security Profile 3) by continuing our AGIG Cyber Security 5 Year Roadmap activities to 2025, and putting in place an ongoing program to maintain good practice cyber security risk management capability. These activities represent an ongoing uplift in people, process and technology to mitigate the cyber security risks we, and indeed all businesses, face. The key benefit of the AGIG cyber security uplift program is consolidation and optimisation of cyber security technology and processes across AGIG entities.

The uplift in capabilities will ensure AGIG not only meets the minimum legislative obligations as currently stated, but also effectively manages risk and meets any increase in requirements reasonably expected during the next AA period.

The AGIG Cyber Security 5 Year Roadmap was developed with the assistance of EY, who assessed AGIG's cyber security risk management capabilities in July 2020. The program has been designed to uplift AGIG's cyber risk management capabilities to MIL-3 standard (as defined in the AESCSF) over the period 2021-2025. From there, the program embeds ongoing investment to ensure continuous improvement and good practice Cyber Risk Management is maintained as the threat landscape and legislative requirements continue to evolve. The roadmap and initiatives are shown in the figure below.

AGIG Cyber Security 5 Year Roadmap



B.2 Summary of options considered

The following options were identified to address cyber security risk across all AGIG entities:

- **Option 1** – Do nothing more, stop any further uplift in cyber security risk management capabilities;
- **Option 2** – Complete the remaining cyber security program activities required to achieve Security Profile 2 under the AESCSF (Security Profile 2 requires a mix of MIL-2 and MIL-3 across domains and controls); or
- **Option 3** – Establish good practice cyber security risk management; reach MIL-3 under AESCSF requirements, continue to meet FIRB conditions.

Table Appendix 1provides a summary of the AGIG-wide costs and benefits of each option.

Table Appendix 1: Comparison of cyber security options

Option	Estimated total AGIG cost ($ m)	Treated residual risk rating	Alignment with vision objectives	Activities to be undertaken
Option 1	Nil capex $10.7 opex	High	Does not align with *Delivering for Customers, A Good Employer* or *Sustainably Cost Efficient*	• Maintenance of existing capabilities only, no further uplift program
Option 2	$7.4 capex $21.6 opex	Intermediate	Some alignment with *Delivering for Customers, A Good Employer* and *Sustainably Cost Efficient*, but does not reduce risk to Low or ALARP	• Technology refresh of existing and newly established cyber security technology. • Implementation of technology and process uplift for a specific Threat and Vulnerability Management solution in AGIG (OT) environments. • Establishing processes to ensure critical application risk is assessed and remediation activities undertaken on a regular basis. • Establishing an Enterprise Security Reference Architecture. • Creation of critical asset registers and security baselines. • Manual record keeping and processes for Third Party Security Risk Management practices, Cyber Operational Risk Management practices and identification and management of vulnerabilities and threats in the field based Industrial Control System (ICS) environments • Simple approach to mitigation and response to detected threats and vulnerabilities. • Simple processes and capabilities for management of identity and privileged accounts in both IT and OT environments.
Option 3	$15.0 capex $26.4 opex	Low	Aligns with *Delivering for Customers, A Good Employer* and *Sustainably Cost Efficient*, and reduces risk to Low	• Establishing technology and processes to ensure secure access to and data security cloud based applications is appropriately managed. (e.g., Cloud Access Security Broker (CASB)) • Technology refresh of existing and newly established cyber security technology. • Implementation of technology and process uplift for a specific Threat and Vulnerability Management solution in AGIG (OT) environments. • Establishing processes to ensure critical application risk is assessed and remediation activities undertaken on a regular basis. • Establishing and maintaining an Enterprise Security Reference Architecture. • Uplift and maintenance of critical asset registers and security baselines with appropriate integration and automation to ensure ongoing accuracy and completeness. • Specific risk management tools for Third Party Security Risk Management practices, Cyber Operational Risk Management practices and identification and management of vulnerabilities and threats in the field based Industrial Control System (ICS) environments

Option	Estimated total AGIG cost ($ m)	Treated residual risk rating	Alignment with vision objectives	Activities to be undertaken
				• Enhanced and automated approach to mitigation and response to detected threats and vulnerabilities, utilising the various platforms established in both the IT and OT environments. • Enhanced processes and capabilities for management of identity and privileged accounts in both IT and OT environments. • Implementation of Data security management controls, Data Leakage Protection (DLP) and Data Classification (Information Classification) • Ongoing updates to Cyber Risk Management Strategy, Threat Profiles and Program Strategy to ensure ongoing management of cyber risk. • Consolidation of OT Cyber technologies and capabilities across the three entities. • Establishment of ongoing review and updates of Cyber Security Strategy, threat profile, and program strategy to ensure ongoing Cyber Risk Management is appropriately managed. • Ongoing background checking of critical employees.

B.3 Proposed solution

The proposed investment in the next AA period enables AGIG to continue the existing cyber security uplift program and fully embed appropriate cyber risk management capabilities throughout all entities. Work will continue to enhance the capabilities across all AESCSF domains working towards ensuring a common capability in the various parts of the AGIG business, thus requiring specific uplift in some business units compared to others.

This investment will result in the following four specific outcomes for AGIG:

1. Uplift AGIG cyber security risk management capabilities to MIL-3 standard. This capability uplift will meet the initial requirements of the Security Legislation Amendment (Critical Infrastructure) 2022 and extend to MIL-3 (Security Profile 3) capabilities to ensure appropriate cyber risk mitigation for AGIG.
2. Implement cyber security capabilities designed to mitigate additional key cyber security risks as assessed by AGIG, particularly with respect to data security.
3. Optimise the AGIG cyber security environment by consolidating capabilities, technologies and processes in use across three entities.
4. Refresh, maintain and optimise the existing and to be implemented suite of cyber security technology solutions.

These investment activities will continue the progress made across AGIG with respect to capabilities required in the AESCSF. The chief benefit of delivering Option 3 compared to Option 2 are the additional risk reduction resulting from a greater level of cyber security management maturity (MIL-3 vs MIL-2). Achieving MIL-3 is a cumulative process, requiring an uplift in maturity across all domains. This means AGIG and its business entities will have a greater overall resilience to cyber attack, reducing the risk of data breaches and impact to services. Achieving MIL-3 also means we are maintaining compliance with AESCSF requirements, reducing the compliance risk rating from intermediate to low.

Further information on the AESCSF and associated cyber security maturity levels is provided in section B.4.

They key deliverables under Option 3 compared to Option 2 are:

- Implementation of Data security management controls, Data Leakage Protection (DLP) and Data Classification (Information Classification).
- Specific risk management tools for Third Party Security Risk Management practices, Cyber Operational Risk Management practices and identification and management of vulnerabilities and threats in the field based Industrial Control System (ICS) environments, where Option 2 would require ongoing manual record keeping and processes.
- Establishment of ongoing review and updates of Cyber Security Strategy, threat profile, and program strategy to ensure ongoing Cyber Risk Management is appropriately managed.
- Consolidation of OT Cyber technologies and capabilities.
- Enhanced and automated approach to mitigation and response to detected threats and vulnerabilities, utilising the various platforms established in both the IT and OT environments.
- Enhanced processes and capabilities for management of identity and privileged accounts in both IT and OT environments.

- Ongoing background checking of critical employees.

Table Appendix 2 provides further details of the cyber security uplift proposed in the next AA period for each of the AGIG entities.

Table Appendix 2: Summary of cyber security uplift required across AGIG entities

AESCSF Domain	Current AA AESCSF key capabilities established in current AA	Next AA AESCSF MIL-3 Uplift	Next AA Business Unit Uplift Required		
			MGN	AGN	DBP
Risk Management (RM)	• AGIG Cyber Security Team. • Cyber Security Risk Management Strategy. • Cyber Security Risk Assessments – Regular Review and update of cyber risks. • Operations Cyber Security Risk Register established.	• Ongoing update of Cyber Security Risk Management Strategy – including updates to reflect the changing threat environment • Risk taxonomy established • Cyber security architecture established and maintained.			
Cybersecurity Program Management (CPM)	• Cyber Security Program Strategy • Cyber Security Program – External Review	• Ongoing update of the Cyber Security Strategy • Cyber Program performance measurement and reporting • Ongoing update cyber security architecture • Secure Software Development Policies and practices established.			
Workforce Management (WM)	• Cyber Security Awareness Program • Cyber Security Team Training • Cyber Security vetting – AGIG critical employee background checks • Profile based cyber security awareness training	• Cyber Security Awareness – Effectiveness measurement and reporting • Ongoing review Cyber Team responsibilities, reflecting change in environment • Risk designation assigned to roles with access to Critical Assets • Ongoing background checks of critical employees.			
Identity and Access Management (IAM)	• AGIG wide identity provisioning and deprovisioning practices established. • Privileged account management practices established. • Identity and credentials review processes conducted.	• Regular identity repository and access reviews conducted. • Authentication and Access controls informed by organisation risk. e.g. requiring MFA for privileged actions. • Processes to ensure access to all systems is granted by Asset Owner. • Enhanced capabilities for management of Privileged Accounts			
Asset, Change, and Configuration Management (ACM)	• Inventory of critical assets. • Configuration Security baselines established. • Asset Criticality Review and Inventory. • Changes reviewed for Cyber Impact.	• Configuration change monitoring – compared to baseline • Ongoing configuration baseline review • Asset Inventory periodic review requirements established and undertaken			
Threat and Vulnerability Management (TVM)	• Threat Profile established • Cyber Security vulnerability information sources established • Internet facing assets periodically assessed • High priority threats analysed and responded to • Vulnerabilities are addressed according to assigned priority	• Regular Threat Profile review • Risk monitoring activities to validate mitigation of vulnerabilities • Integration and automation of ICS Specific Threat and Vulnerability Management solutions. • Cyber Security Incident Response Plan informed by changes to the Threat Profile			
Event and Incident Response, Continuity of Operations (IR)	• Cyber Incident Response Plan in place with ongoing training for participants • Participation in Joint Cyber Security exercises with other organisations • Reporting to external bodies documented • Recovery Time Objectives (RTO) and recovery point objectives (RPO) incorporated in recovery plans	• Business Impacts Assessment regularly reviewed and impact to cyber security capabilities assessed • Continuity plans are evaluated and exercised, and learnings incorporated in updated recovery plans • Common Operating Picture (COP) updated based on Cyber Incident learnings • Incident response plans informed by Threat Profile changes			
Situational Awareness (SA)	• Centralised security logging and alerting • Ongoing proactive review of security logs • Security Logging/Monitoring Policy • Common Operating Picture (COP) established	• Common Operating Picture (COP) updated based on external threat monitoring • Predefined state of operation for the Common Operating Picture. (e.g. Red, Amber, Green)			

AESCSF Domain	Current AA AESCSF key capabilities established in current AA	Next AA AESCSF MIL-3 Uplift	Next AA Business Unit Uplift Required		
			MGN	AGN	DBP
		• Periodic testing and update of security monitoring capabilities based on specific IOC's and attack techniques.			
Australian Privacy Management (APM)	• Privacy Policy and practices in place. • Privacy Information documented. • Privacy Management Plan • Privacy Risk captured in Risk Register	• Incident response plan tested for data breach scenarios at least annually.			
Supply Chain and External Dependencies Management (EDM)	• Third Party Security Risk Management Framework in place • Significant Cyber Security risk due to suppliers are identified and addressed and captured in the Risk Register • Cyber Security requirements are addressed in agreements with suppliers, including breach notification				
Informational Sharing and Communications (ISC)	• Cyber Security incident reporting obligations are assigned and documented – ACSC • Cyber Security Reporting assigned and conducted periodically. • Cyber Security threat intelligence agencies are identified and engaged for specialist advise • Participation in external information sharing groups (e.g. JCSC)	• Threat Intel is shared with agreed and appropriate external parties. • Information sharing requirements defined with agreed timeframes.			

The proposed AGIG program activities and costs over the next AA period are summarised in Table Appendix 3.

Table Appendix 3: Summary of AGIG cyber security uplift program expenditure, $'000 real 2021

Activity	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Cyber Team and Program Resourcing	2,638	2,638	2,638	2,638	2,638	13,188
Cyber Governance and Risk Management	1,054	1,054	1,054	1,154	1,154	5,470
Cyber Technology – Licensing & Maintenance	1,841	1,841	2,141	2,391	2,391	10,605
Cyber Technology – Refresh	150	650	250	150	150	1,350
Cyber Uplift Projects	2,476	2,576	2,226	1,620	1,720	10,618
Total	**8,159**	**8,759**	**8,309**	**7,952**	**8,052**	**41,231**

The program is prudent because:

- it is required to sufficiently reduce risk and sustain cyber risk management capabilities at an acceptable level:
  - if AGIG were not to continue with the existing cyber security uplift activities it would result in key risks not being appropriately mitigated; and
  - if AGIG were to only meet existing minimum legislative obligations equivalent to MIL-1, many key risks identified for our business will not be fully mitigated, in particular risks related to data security.
- it is consistent with our vision of being a good employer and will support lower overall costs of delivering cyber security services by ensuring capabilities are able to be established across all AGIG entities. This ensures service can be delivered in a sustainably cost efficient manner and is therefore in the long term interests of customers; and
- it is deliverable and appropriately designed to establish capabilities required by the AESCSF, specifically established for energy sector critical infrastructure entities, and provides for AGIG specific requirements such as FIRB compliance obligations.

Table Appendix 4: Alignment with vision

Vision objective	Alignment
Delivering for Customers – Public Safety	Y
Delivering for Customers – Reliability	Y
Delivering for Customers – Customer Service	Y
A Good Employer – Health and Safety	Y
A Good Employer – Employee Engagement	Y
A Good Employer – Skills Development	Y
Sustainably Cost Efficient – Working within Industry Benchmarks	Y
Sustainably Cost Efficient – Delivering Profitable Growth	-

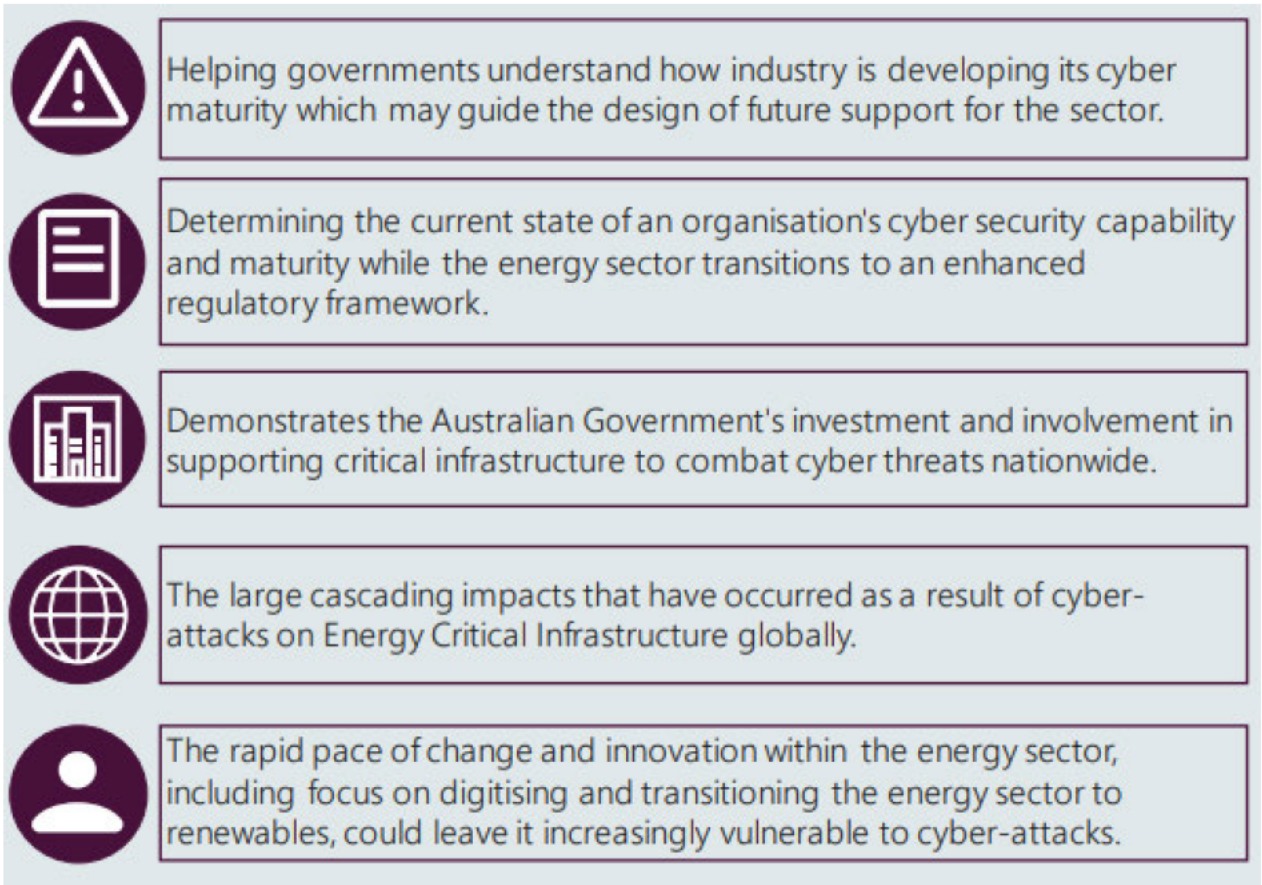
Vision objective	Alignment
Sustainably Cost Efficient – Environmentally and Socially Responsible	Y

B.4 Australian Energy Sector Cyber Security Framework

The AESCSF has been developed through collaboration with industry and government stakeholders, including the AEMO, ACSC, CIC, and the CSIWG, which includes representatives from Australian energy organisations.

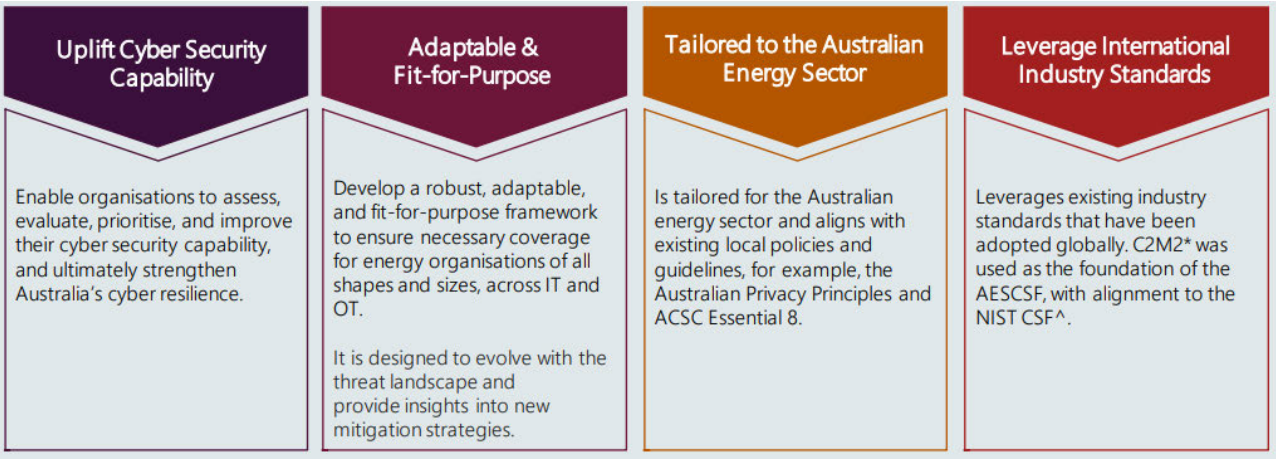
The AESCSF leverages recognised industry frameworks such as the US Department of Energy's Cybersecurity Capability Maturity Model (ES-C2M2) and the NIST Cyber Security Framework (CSF), and references global best-practice control standards (e.g. ISO/IEC 27001, NIST SP 800-53, COBIT, etc.). The AESCSF also incorporates Australian-specific control references, such as the ACSC Essential 8 Strategies to Mitigate Cyber Security Incidents, the Australian Privacy Principles, and the Notifiable Data Breaches scheme (NDB).

The 2022 AESCSF is being led by the Department of Industry, Science, Energy and Resources (DISER) and AEMO. The drivers for continued uplift are:



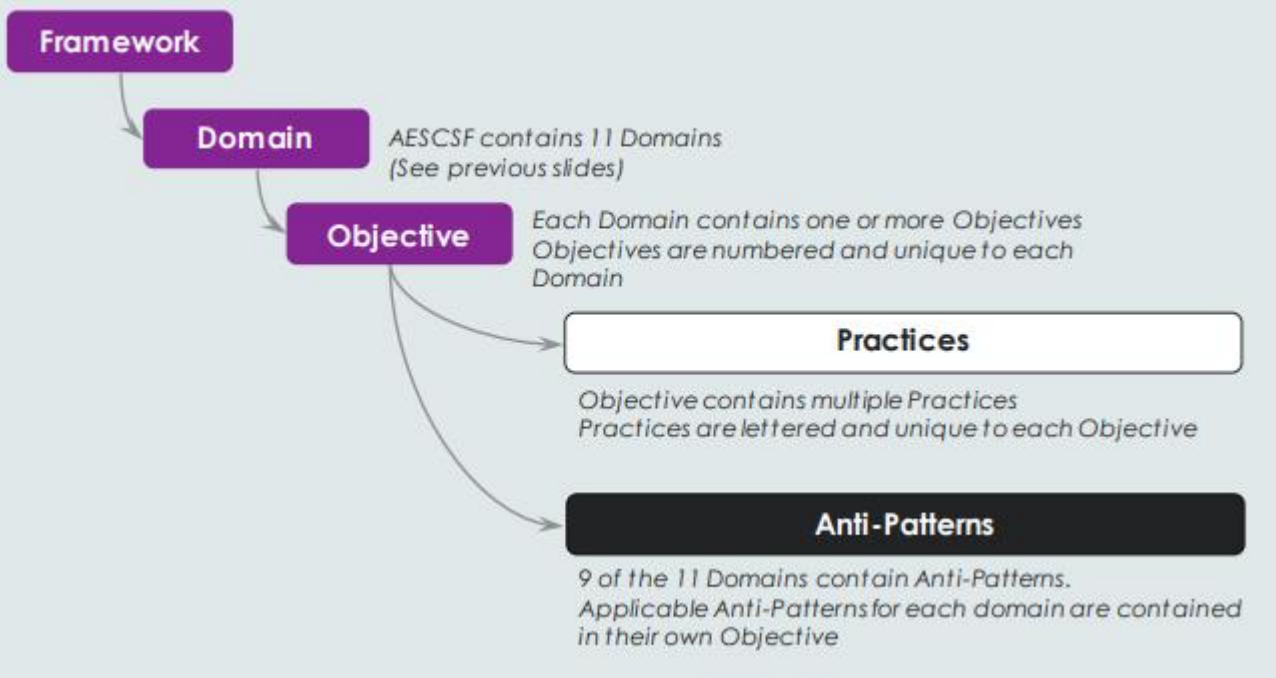
Guiding principles

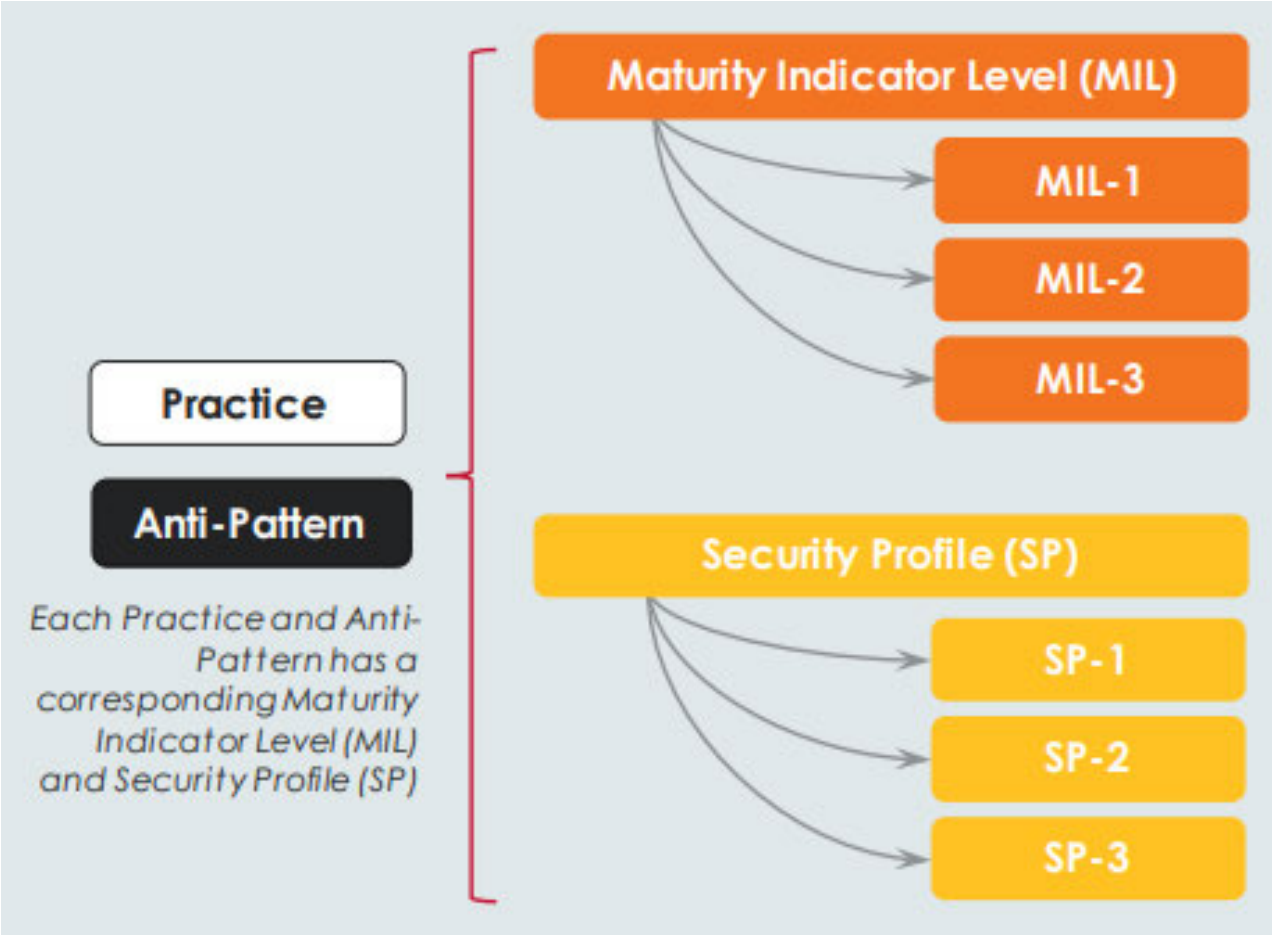
The guiding principles of the AESCSF are:



Framework structure

The practices within a domain are grouped by objective – target achievements that support the domain. Within each objective, the practices are ordered by MIL – Maturity Indicator Level.





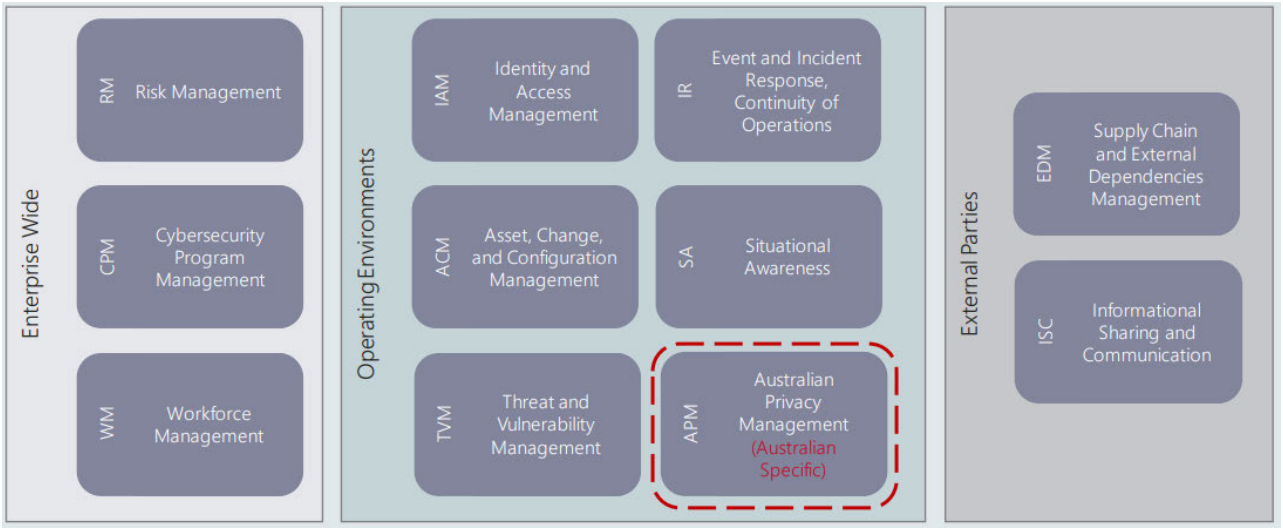
Anti-patterns are included in the AESCSF to enable identification of behaviours/practices that hinder an organisation from achieving a higher maturity and they have remained in subsequent AESCSF versions. Anti-Patterns were developed in consultation with AEMO, industry and government stakeholders. In essence, they are 'bad' activities that undermine the effectiveness of a cyber-security capability. Therefore, additional focus is given to them to encourage organisations to fix these behaviors.

Each practice and anti-pattern has been assigned a MIL (MIL-1, MIL-2 or MIL-3) that indicates its maturity relative to other Practices. Each MIL has specific characteristics which impact assessment for practices. The 2020-21 AESCSF has 282 practices and anti-patterns.

The framework has three alternate groupings of practices and anti-patterns referred to as security profiles (SPs). The SPs have been defined by the Australian Cyber Security Centre, in consultation with AEMO and industry representatives, as a measure of target state maturity. The target state maturity SP a participant should pursue is determined based on their overall criticality result (per the CAT). MILs apply independently to each domain. As a result, entities may be operating at different MIL ratings for different domains. SPs apply collectively across all domains. As a result, entities only achieve a SP if they have completed all practices in the SP across all domains. The MILs and SPs are cumulative; to earn a MIL or SP, an organisation must perform all of the practices, and not exhibit any of the anti-patterns, in that level and its predecessor level(s).

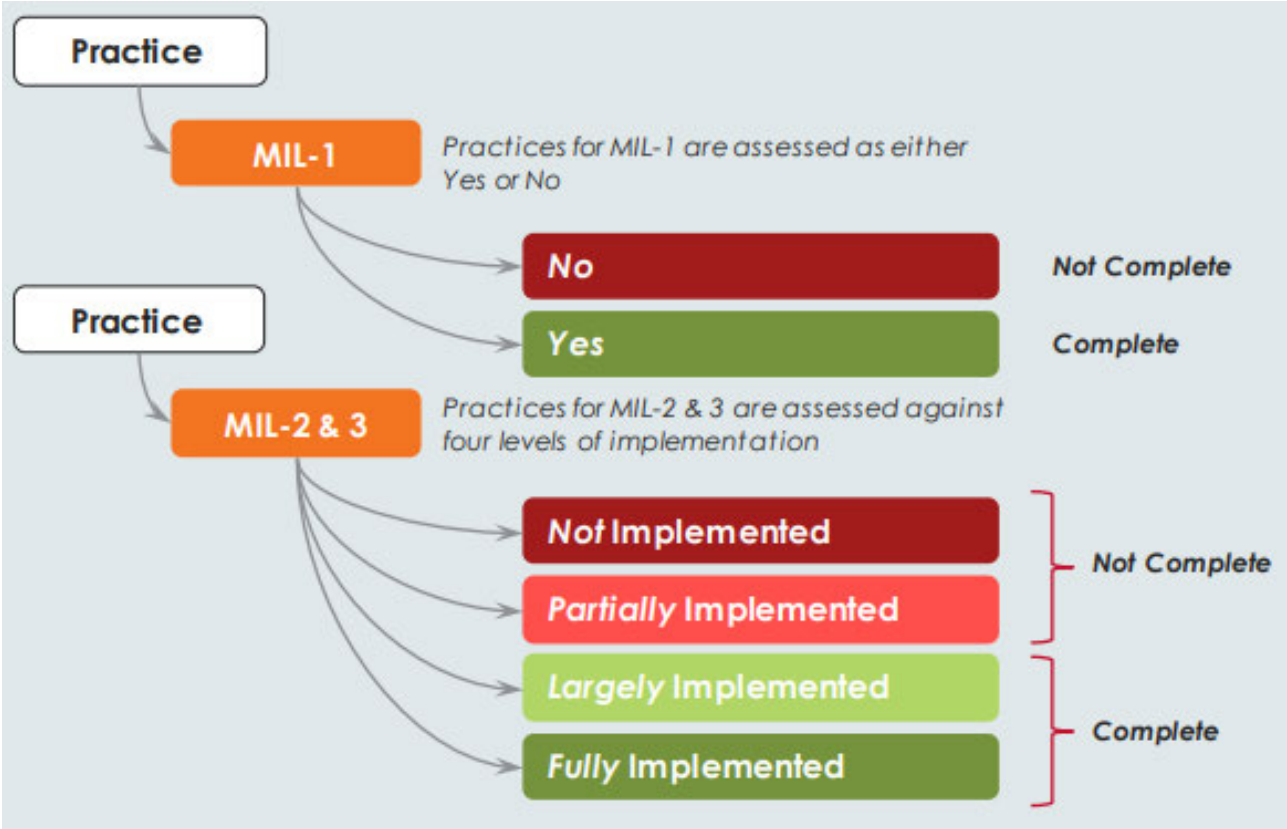
AESCSF domains

The AESCSF is divided into 11 domains - 10 C2M2 domains and the Australia Privacy Management domain. The domains are logical groupings of cyber security practices. Each domain has an acronym that cross references across the AESCSF toolkit and guidance artefacts.



Scoring model

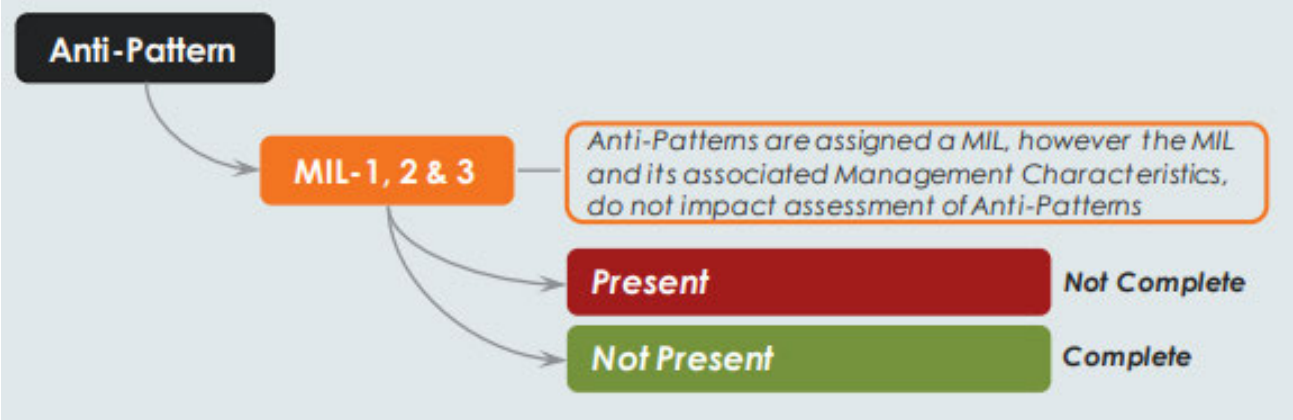
The framework is supported by a maturity scoring model that enables organizations to assess their current and desired future states with any gaps between the two being a key input into the organization cyber strategy roadmap.



MIL-1 can be described as initiated – initial practices are performed, but may be ad-hoc. MIL-2 can be described as performed – practices are more complete or advanced than at MIL-1 with the introduction of management characteristics that drive consistency and repeatability. MIL-3 can be

described as managed. Practices are more complete or advanced than at MIL-2 with the addition of further management characteristics that drive governance and continuous improvement.

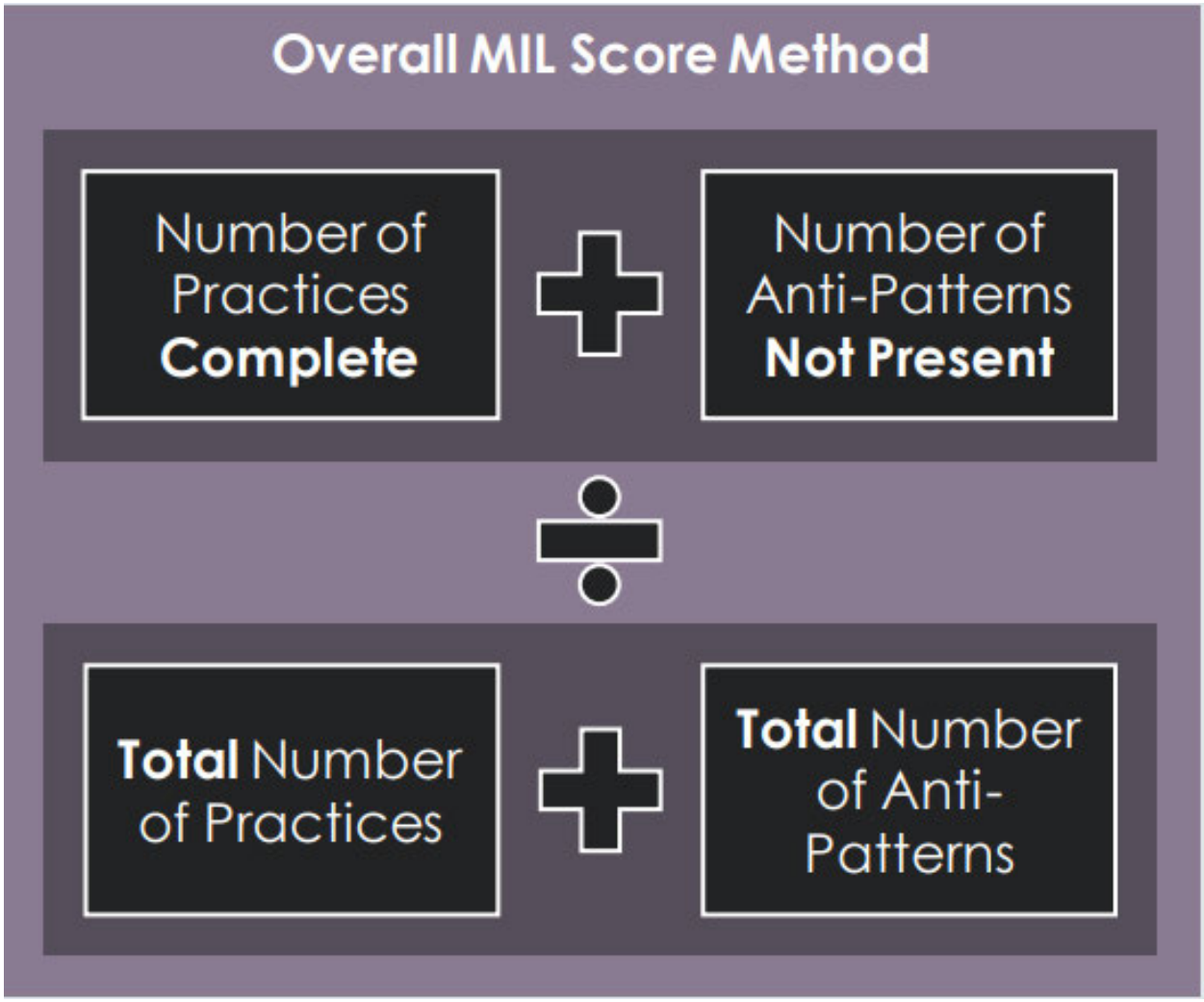
A Practice is 'complete' if it is assessed as 'largely implemented' or 'Fully implemented'. A MIL is 'achieved' if all practices within it are 'complete'. Scoring is based on a combination of 'practice implementation" and "management characteristics'.



Anti-patterns are either present or not present. There are no management characteristics that need to be considered when scoring anti-patterns. Instead, the rating depends on whether the anti-pattern activity is present with the entity. Anti-patterns are assigned a MIL rating from 1 to 3. However, the MIL rating does not impact the assessment approach for anti-patterns. This means. a MIL-3 anti-pattern is assessed as either present or not present, the same as a MIL-1 anti-pattern.

Per the framework structure section, AESCSF results can be expressed either in terms of Maturity Indicator Level (MIL) or Security Profiles (SP).

There are three MILs (MIL-1, MIL-2 and MIL-3) that are assigned to all practices in all the domains in the framework and define the maturity progression. The MILs apply independently to each domain and are cumulative. For a participant to gain a MIL in each domain, they must complete all practices, and not exhibit any anti-patterns, at that MIL in that Domain. For example, to achieve a MIL-3 the participant would have to perform all Practices and not exhibit any of the anti-patterns, in MIL-1, MIL-2, and MIL-3.



SPs cannot be applied to each domain unlike MIL. For a participant to be recognised for a SP, they need to have achieved 100% of all the practices. SPs follow the same cumulative nature of MILs. (i.e., SP-2 can only be achieved if SP-1 has been achieved.

Security Profile (SP)	Participant criticality	Practices and anti-patterns			Total required to achieve SP
		MIL-1	MIL-2	Mil-3	
Security Profile 1 (SP-1)	Low	57	27	4	88
Security Profile 2 (SP-2)	Medium	0	94	18	200 (112+88 from SP-1)
Security Profile 3 (SP-3)	High	0	0	82	282 (82+200 from SP-2)

Criticality bands by market sub-sector – gas

The G-CAT scopes which market roles an entity operates in. Entities can operate in more than one market role – production, transmission, storage, distribution, retailer, and market operator.

Appendix C OneERP

C.1 Initiative overview

C.1.1 AGIG OneERP program

AGIG has commenced the roll out of the OneERP program in DBP and AGN, utilising SAP solutions. The core platform and implementation for DBP and AGN will be completed during 2022/23. The second stage of the OneERP program is to roll out the same SAP solutions for MGN.

MGN is currently operating on SAP version ECC6, using modules such as ISU Billing and CRM, which will become unsupported from 2025. Therefore, MGN's adoption of SAP S/4HANA is twofold; to align its corporate processes with the rest of the AGIG business and to maintain current, fit-for-purpose and supported systems.

In developing the AGIG One IT program, it was recognised that a standardised ERP across the Group that has a common data model will deliver efficiencies for customers through shared service arrangements enabled by standardised processes and transparent and reliable data across the three business entities, in an environment where customer, regulatory and industry requirements are continually maturing. In addition, completion of the OneERP program will:

- address problems associated with disparate systems and siloed operations;
- ensure data is captured at the right level and in the right format in the ERP and therefore limit the number of workarounds and manual processing required to filter and extract data at the right level;
- consolidate licenses and reduce administrative overhead associated with managing multiple corporate systems;
- unlock economies of scale and leverage cost savings; and
- improve reporting capability.

Key areas derived from the One IT program and the OneERP project in particular, from which we expect to gain material efficiency benefits over the longer term, are summarised in the following table.

Table Appendix 5: Summary of efficiency benefits from One IT / OneERP

Key area	Benchmark efficiency gain[1]
Business process improvement and automation (standardisation and simplification of processes across the group with reduction in manual effort through automation where possible)	5 – 10%
Strategic sourcing and consolidated vendor management	5 – 20%
Group wide shared services	10 – 50%
Organisational design optimisation (centralisation to reduce duplication of processes and effort and improve collaboration)	5 – 10%

These efficiency gains can only be achieved through a group wide effort that benefits all AGIG's customers. Sharing the cost of these initiatives across the group also allows the customers in each jurisdiction to benefit from processes and technology that they would be unable to access if each group member was on its own.

C.1.2 MGN OneERP Stage 2

The MGN OneERP Stage 2 project will implement SAP S/4HANA at MGN for ERP, CRM and ISU Billing). The ISU upgrade has been factored into the MGN OneERP project due to interdependencies with ERP, and also being on ECC6 which will not be supported after 2025. The overall scope of the upgrade is summarised below: The planning for this project has utilised an external consultancy ([redacted]) to assist in validating and updating the scope of the project as well as providing indicative costs to replace the high-level estimates originally developed with the AGIG One IT program.

The overall scope of the OneERP Stage 2 project is to:

- Upgrade MGN's existing ECC6 to S/4HANA, and:
  - Adopt existing OneERP business processes and configuration (from Stage 1);
  - Develop additional finance reports;
  - ISU technical upgrade and extension; and
  - CRM implementation (this is considered in the MGN Digital Customer Experience Business Case); and
- minimise integration touch points across the MGN IT environment through the adoption of SAP's PO integration platform.

C.2 Summary of options considered

Following development of the AGIG One IT program, a single ERP solution to enhance and streamline our operations to drive efficiencies and cost savings across AGIG was developed. In the business case for OneERP Stage 1 (submitted to the ERA and approved for DBP in 2021) three options were considered:

- Option 1 – Microsoft Dynamics 365
- Option 2 – Oracle
- Option 3 – SAP S/4 Hana

SAP was identified as the preferred solution for a single ERP system to support the AGIG businesses and help drive efficiencies across the group. The decision to select SAP S/4 Hana was chosen on the basis of:

- common usage across the group with each of the businesses using or having used SAP;
- security in line with our role as a critical infrastructure provider;
- ability to support a common data language and a way to seamlessly connect all three businesses via access to a reliable, common data source, enabled by a SAP ERP;
- enable common business processes to be established across the group;
- ability to comply with our regulatory obligations across the group, and
- SAP S/4 Hana is designed for the energy and natural resources sector meaning the number of manual and systematic workarounds is significantly reduced compared to any other solution.

This option was identified as the most prudent and efficient for our organisation.

For OneERP Stage 2, to roll out SAP S/4HANA for MGN, we have considered the following options:

- **Option 1** – Stop or delay the OneERP Stage 2 project

- **Option 2** – Upgrade MGN's ECC6 ERP to S/4HANA by 2025, followed by ISU by 2027 and adopt SAP's PO integration platform
- **Option 3** – Upgrade MGN's ECC6 ERP and ISU to S/4HANA simultaneously and adopt SAP's PO integration platform

Option 1 was not progressed as it is not feasible to stop or delay the OneERP Stage 2 project as MGN's existing ECC6 ERP, CRM and ISU Billing will no longer be supported from 2025 and 2027 respectively, resulting in a high risk to critical business operations. Stopping or delaying also does not align with our vision objectives of:

- Delivering for Customers – unsupported ERP and ISU systems which support all of our asset management, customer management and customer billing functions will impact our ability to maintain safety, reliability and customer service.
- A Good Employer – unsupported, legacy and unaligned systems will overtime increase manual workarounds required and lead to ongoing employee frustration (a key area of feedback in our annual employee engagement surveys), potentially impacting employee health & safety.
- Sustainably Cost Efficient – Through OneERP Stage 1, AGIG and its delivery partners have developed substantial intellectual property and capability that is beneficial to the successful delivery of OneERP Stage 2. Any material pause or delay in the OneERP program risks loss of this intellectual property that would lead to additional costs and effort. It also inhibits AGIG's ability to realise the benefits of a standardised ERP.

Table Appendix 6 provides a summary of the costs and benefits of each option.

Table Appendix 6: Comparison of options

Option	Estimated cost ($ million 2021)	Treated residual risk rating	Alignment with vision objectives
Option 2	$33.4M capex	Low	Aligns with *Delivering for Customers* and being *A Good Employer* but is not as S*ustainably Cost Efficient* as Option 3.
Option 3	$31.9M capex	Low	Aligns with *Delivering for Customers*, *A Good Employer* and is more *Sustainably Cost Efficient* than Option 2.

C.3 Proposed solution

The proposed OneERP Stage 2 project is to upgrade MGN's existing ECC6 to S/4HANA and minimise integration touch points across the MGN IT environment through the adoption of SAP's PO integration platform.

Specifically, the project scope includes:

- **Enterprise structure update:** Include all MGN Enterprise Organisational structures in S4/HANA system.
- **Additional configuration in finance/procurement:** Assume re-use of existing OneERP business processes and configuration, retain Promaster for expense management, re-use purchase requisitions, Orders, Goods Receipt, invoice receipt processes and configuration for procurement.
- **Implement all EAM functionality:** Setup plant maintenance functionality with appropriate MGN user involvement, integration required to Comdain systems for replication of all maintenance activity, setup of project systems for high level cost capture of capital spend as services work outsourced to panel, significant effort for migration of data.

- **SAP security:** Include all additional EAM roles, mapping of all MGN business roles to system roles.
- **Integration:** Re-use OneERP integration to Promaster and Payglobal, Gas Meters and regulators to continue being manually created, new integrations expected for Comdain SAP to OneERP for maintenance transactions.
- **Reporting:** Develop 10 additional finance reports for MGN, stand-alone HANA reporting database to be retained for ISU reporting.
- **Implement advanced reporting functions:** Implement advanced analytics and payment management processes.
- **MGN SAP ISU upgrade:** Technical upgrade of the ECC6 system to S/4HANA, setup dual landscapes, with no changes required for security.

There are two further aspects of MGN's ECC6 to S/4 HANA upgrade that are contemplated in the MGN Digital Customer Experience Business Case:

- **Implement CRM processes:** Include all MGN CRM processes in S/4HANA or C/4HANA system to replace CRM
- **Implement SAP marketing cloud:** Configure Marketing processes in SAP Marketing Cloud (SMC) for B2B and B2C.

The costs for each system are summarised below in Table Appendix 7 below.

Table Appendix 7: Summary of costs for each OneERP system, real $'000

	2023/24	2024/25	2025/26	2026/27	2027/28	Total
OneERP Phase 2	4,388	12,163	4,463	-	-	21,014
ISU Tech Upgrade	2,578	6,648	1,628	-	-	10,853
TOTAL	**6,966**	**18,811**	**6,091**	-	-	**31,867**

[redacted], one of our support partners for OneERP Stage 1, was engaged to assist with planning, scoping and costing the OneERP Stage 2 project. The following sections provide more information on the activities and costs associated with each aspect of the project.

C.3.1 ERP

The ERP upgrade for MGN involves re-platforming of the current SAP system so that the items currently on ECC6 will be updated to SAP S/4HANA on an IaaS[25] cloud. Further, it will update existing processes and structures to align with the standardised processes and data model established in Stage 1. This includes standardisation of corporate processes, such as procurement, accounts payable, general ledger processing, and treasury. By aligning these areas that are similar across AGIG, we enable more shared services which will lower costs to our customers, through the achievement of business wide efficiencies.

A breakdown of the activities and costs associated with the OneERP upgrade component of the project is provided in the table below.

Table Appendix 8: Summary of OneERP costs, $'000 real 2021

Cost type	Activities	Total

[25] Infrastructure as a service (IaaS) is a form of cloud computing that provides virtualised computing resources over the internet. It is one of the three main categories of cloud computing services, alongside software as a service (SaaS) and platform as a service (PaaS). https://searchcloudcomputing.techtarget.com/definition/Infrastructure-as-a-Service-IaaS

Systems Implementor costs	Design, Build, Test, Data Migration, Training and Training Documentation	12,000
SAP Licenses	S/4HANA user licences	1,000
Azure costs	Azure licence (capitalizable during project phase)	1,611
Internal staff and project costs	Internal and External costs for planning and tender, MGN and AGIG personnel time on project, project manager and support partner, Infrastructure and services effort for test environments for legacy applications to be integrated, Comdain time for integrated testing required	6,174
Other	Tableau remediation	230
Post go-live support		**21,014**

C.3.2 ISU

MGN currently utilises SAP's ISU Billing application which operates on a standalone ECC6 instance. The current ISU Billing ECC6 solution will be supported by SAP until 2027. While this alleviates some of the urgency of upgrading to S/4HANA (compared to SAP's ERP solution which comes off support in 2025), there are advantages to upgrading the ISU Billing simultaneously with an SAP S/4HANA implementation. The biggest advantage is the project management cost savings realised through implementing on a single ERP platform, which are in the order of $1-1.5 million.

Unlike the ERP upgrade, the ISU Billing upgrade is largely a technical upgrade which will deliver the existing functionality of the ISU employed in MGN on the ECC6 platform on to the S/4HANA platform.

A breakdown of the activities and costs associated with the ISU upgrade component of the project is provided in the table below.

Table Appendix 9: Summary of ISU costs, $'000 real 2021

Cost type	Activities	Total
Systems Implementer costs	Design, Build, Test, Data Migration, Training and Training Documentation	8,100
SAP Licenses	S/4HANA user licences	500
Internal staff and project costs	Internal and External costs for planning and tender, MGN and AGIG personnel time on project, project manager and support partner, Infrastructure and services effort for test environments for legacy applications to be integrated, Comdain time for integrated testing required	1,543
Other	SAP Smart Data Access and Solution Manager, retire existing MGN Solution Manager	710
Post go-live support		**10,853**

C.4 Summary

The program will be delivered utilising a mix of internal or external resources, managed centrally via the AGIG PMO. The proposed OneERP Stage 2 project incorporating upgrades for ERP and ISU, is prudent as:

- MGN currently operates on SAP ECC6 and, due to its ending support in the near future, requires a structured plan to replace it;
- a technical upgrade from ECC6 to S/4HANA will align to the SAP environment that will exist across the rest of the business;
- continuing with a SAP based platform will also maintain a degree of familiarity, which will assist in minimising the change impact within MGN;
- it is consistent with our vision of delivering for customers, being a good employer and sustainably cost efficient. It will support lower overall costs of delivering services by standardising corporate processes across all AGIG entities; and
- it is deliverable.

The table below shows how the proposed option aligns with our vision objectives.

Table Appendix 10: OneERP Stage 2 alignment with vision

Vision objective	Alignment
Delivering for Customers – Public Safety	-
Delivering for Customers – Reliability	Y
Delivering for Customers – Customer Service	Y
A Good Employer – Health and Safety	-
A Good Employer – Employee Engagement	Y
A Good Employer – Skills Development	Y
Sustainably Cost Efficient – Working within Industry Benchmarks	Y
Sustainably Cost Efficient – Delivering Profitable Growth	Y
Sustainably Cost Efficient – Environmentally and Socially Responsible	-

Appendix D Data architecture, reporting and governance

D.1 Initiative overview

The gas utilities industry faces a number of challenges causing fundamental shifts in the regulatory, operating and market environments. These include:

- networks with more connected devices;
- greater information and transparency demanded by customers, regulators and external partners;
- enhanced consumer expectations in relation to gas supply and information; and
- more intensive scrutiny on safety and maintenance policies and procedures.

The increasing use of technologies, the digitisation of business processes, along with technological innovation is driving the proliferation of data. This explosion in data volumes and the tendency of business to retain greater amounts of data obscures the value of information. The increased volume of data creates large variances in the type and quality of data available. Information quality (completeness, integrity, accessibility etc.) is fundamental to the success of the business. High quality information is the foundation for good decision making and effective collaboration.

The Data Architecture, Reporting and Governance initiative is about driving a common language for data (as well as the understanding of data flows) across AGIG with the objectives of staying compliant and sustainable. The term "data" is inclusive of all enterprise content (i.e. information that is readable, relevant and useful to end-users). Appropriate and standardised categorisation and management of AGIG content across its lifecycle is imperative for:

- cyber risk management – cyber controls, such as identity and access controls, are only effective when the controlled content is appropriately categorised and managed;
- compliant reporting - fragmented, disparate and inconsistent content management results in unreliable information and manual manipulation, making it difficult to be transparent with our regulators, customers and internal business stakeholders;
- good decision making – ensuring simple access to quality information in a timely manner (i.e. the right information in the right format) supports good decision making; and
- efficiency through streamlining business processes – standardising systems and processes (i.e. OneERP) and improving and automating more of our content management, will create synergies across AGIG, reduce duplication of effort and allow less time to be spent collecting and collating information to support business decisions, and more time undertaking value-add analysis activities.

The focus of foundational activities is to improve reporting capabilities through:

- developing a data governance operating model;
- developing an enterprise data model, policies and standards;
- metadata management and information classification (including data quality and risk monitoring); and
- raw data storage and operational reporting.

Work is already underway on the foundational activities. By June 2023, we will have:

- developed strategies for AGIG content management, reporting and analytics and information governance;
- undertaken AGIG enterprise content management review and recommendations; and

- completed the consolidation of multiple versions of Microsoft SharePoint into a Microsoft Sharepoint online instance.

Building on the foundational activities outlined above will bring about much needed improvements in reporting capabilities, including:

- implementing a standard data warehouse for core data;
- establishing enterprise reporting self-service;
- implementing a data virtualisation and analytics platform for non-core data; and
- implementing an enterprise content management (ECM) system.

In 2020 we engaged an independent expert, [redacted] to review the current state of our content management capabilities and provide recommendations for an ECM program to further inform the data architecture, reporting and governance activities. The findings and recommendations are summarised in Table Appendix 11.

Table Appendix 11: Summary of [redacted] findings and recommendations

Findings	Recommendations
Lack of governance structures and processes.	Enhance information management governance and processes to include content management.
Insufficient ease of access, especially to legacy content.	Develop ECM solution to enable authorized access to content along with searchable index (Metadata) of content. Migrate digitized artefacts into ECM.
No enterprise archiving strategy and function.	Enhance / develop storage architecture along with automated data / content lifecycle policies and procedures.
Lack of consistent access auditing across the 3 entities/companies.	Mandate AGIG Enterprise security policies, processes and controls based on information classification.
Low support for collaboration in areas like version control, single point of "truth" and simultaneous editing of document.	Develop ECM architecture to encompass "single source of truth", version control for content and capability for document collaboration.
Lack of a centralised search function to locate content.	Develop ECM architecture for to enable the capability implementing indexed artefact content searchability.
Lack of classification of some content to ensure appropriate handling and storage in accordance with regulatory requirements.	Enhance / publish / maintain information classification policy along with appropriate procedures and controls to ensure compliance with regulatory requirements.
Lack of Policies for content-specific aspects such as unique identification of documents, storage, retention, access to legacy files and asset information, etc.	Evolve appropriate policies for content identification, metadata creation and indexing per content object. Define information lifecycle policy along with access controls based on information classification.
Potential risk to assurance of privacy, for example, Personally Identifiable Information (PII) customer information and data along with regulatory compliance related to Content management.	Enhance / publish / maintain information classification policy for PII along with appropriate procedures and controls to ensure compliance with regulatory requirements and AGIG policy.
No central repository to store various extracts of data taking place from different systems to produce desired reports.	Define business requirements and compelling business cases in existence to efficiently and effectively handle raw data for use by reporting or analytics.
Multiple systems with specific business use, such as LawVu, CVMail, CVCheck, Work Pro, Sharepoint (multiple versions of software in operations), Maximo, Microsoft Planner, CRM, Alliance Hubs, One Net, etc.	Perform deep-dive analysis of existing systems to determine "fit-for-purpose" functionality and roadmap appropriate strategy for each system.
Workflow is usually manual, "clunky and messy" with limited knowledge and documentation of operational procedures of function.	Document the business-critical workflows and investigate improvements to workflows considering potential for automation. Create a knowledge base for transparency.

Ensure adequate training programs and documentation with periodical review exist for all operational procedures

D.2 Summary of options considered

Following the development of the AGIG One IT program, we considered three options for data architecture, reporting and governance:

- **Option 1** – Enterprise Data Model (EDM) and Governance structure.
- **Option 2** – Standard Data Warehouse and Virtualisation and Analytics platform - EDM, governance structure, classifying and categorising historical data, archived data store, Enterprise Content Management solution (ECM), Raw Data Storages/Staging repositories, Standard Data Warehouse and Virtualisation and Analytics platform.
- **Option 3** – Lakehouse - EDM, governance structure, classifying and categorising historical data, archived data store, ECM, Standard Data Warehouse, market study & implementation of a data lake house.

Table Appendix 12: Comparison of options

Option	Estimated cost ($ million 2021)	Treated residual risk rating	Alignment with vision objectives	Activities
Option 1	$0.5 capex $0.1 opex	Intermediate	Does not align with *Delivering for Customers, A Good Employer* or *Sustainably Cost Efficient*	Implement data governance operating model Develop EDM, policies and standards
Option 2	$11.5 capex $3.1 opex	Negligible	Aligns with *Delivering for Customers, A Good Employer* and is more *Sustainably Cost Efficient* than Option 3.	Implement data governance operating model Develop EDM, policies and standards Metadata management and information classification (including Data Quality and Risk Management) Raw data storage and operational reporting Implement standard data warehouse Establish Enterprise Reporting self-service Implement Data Virtualisation and Analytics Platform Implement ECM
Option 3	$13.9 capex $1.9 opex	Intermediate	Aligns with *Delivering for Customers* and being *A Good Employer* but is not as *Sustainably Cost Efficient* as Option 2.	Implement data governance operating model Develop EDM, policies and standards Metadata management and information classification (including Data Quality and Risk Management) Implement standard data warehouse Undertake market study and implement data lakehouse

D.3 Proposed solution

The proposed solution is Option 2. This will include:

- developing a data governance operating model;

- developing an enterprise data model, policies and standards;
- metadata management and information classification (including data quality and risk monitoring);
- raw data storage and operational reporting;
- implementing a standard data warehouse for core data;
- establishing enterprise reporting self-service;
- implementing a data virtualisation and analytics platform for non-core data; and
- implementing an ECM system.

The total costs of the data architecture, reporting and governance activities in the next AA period are shown in Table Appendix 13 below.

Table Appendix 13: Data architecture, reporting and governance activities in next AA period, $'000 real 2021

	2023/24	2024/25	2025/26	2026/27	2027/28	Total
1a Data Governance Operating Model	-	-	-	-	-	-
1b Enterprise Data Model, Policies and Standards	-	-	-	-	-	-
1c Metadata Management and Information Classification (including Data Quality and Risk Monitoring)	-	-	-	-	-	-
1c Metadata Management and Information Classification - MGN only	933	-	-	-	-	933
2a Raw data storage and Operational Reporting	1,704	484	-	-	-	2,188
2b Implement Standard Data Warehouse	-	2,195	-	-	-	2,195
2c Establish Enterprise Reporting self-service	-	698	-	-	-	698
2d Implement Data Virtualisation and Analytics Platform	983	-	-	-	-	983
3 Implement ECM	963	-	-	-	-	963
Total	**4,584**	**3,377**	**-**	**-**	**-**	**7,962**

The following sections discuss each activity in more detail.

D.3.1 Enterprise information management

Enterprise information management (EIM) is a key enabler for AGIG sustainability. Enterprise information is the lifeblood of all AGIG business processes, as it drives decision making at every level and defines the business outcomes. Currently, the AGIG data architecture includes a mishmash of three divisions' data systems, interfaces, and reports.

To support business objectives (Delivering for Customers, A Good Employer, Sustainably Cost Efficient), AGIG will uplift the EIM capabilities in three parallel streams of work:

- Enterprise Information Governance
- Reporting and Analytics

- Enterprise Content Management

D.3.2 Information governance

Current information governance is done informally and in siloes with inconsistent efficiency. However, siloed data governance won't cope with the rapidly growing volume and variety of data created and used across AGIG. The demand for self-service information is growing prodigiously requiring a balance between control and agility. Ungoverned development leads to duplication of effort, increased costs, and analytical silos resulting in a lack of confidence in data assets due to clunky inconsistent information management and creation practices.

Enterprise information governance can help AGIG leaders to shift conversations away from tools and techniques towards decision making as a business competency. This approach will remediate many current challenges including manual reconciliation of data, meeting deadlines for compliance and regulatory reporting, the growing cost of application integration and information.

D.3.3 Reporting and analytics

AGIG has an abundance of data but scarce information and insights. Six reporting and analytics categories have been identified at AGIG, however, the biggest impact currently comes from mandatory and regular reporting, which we have labelled standard reporting.

Enterprise data warehouse implementations are challenging and often have a low success rate. To manage this risk, AGIG prioritises the standard data warehouse that will be a backend data repository for all business-critical standard reporting.

Trusted and authoritative data in the SDM will be used as a reference point for all future analytics. As the next level of maturity, AGIG will adopt inexpensive data virtualisation to simplify data interoperability and discovery for information self-service.

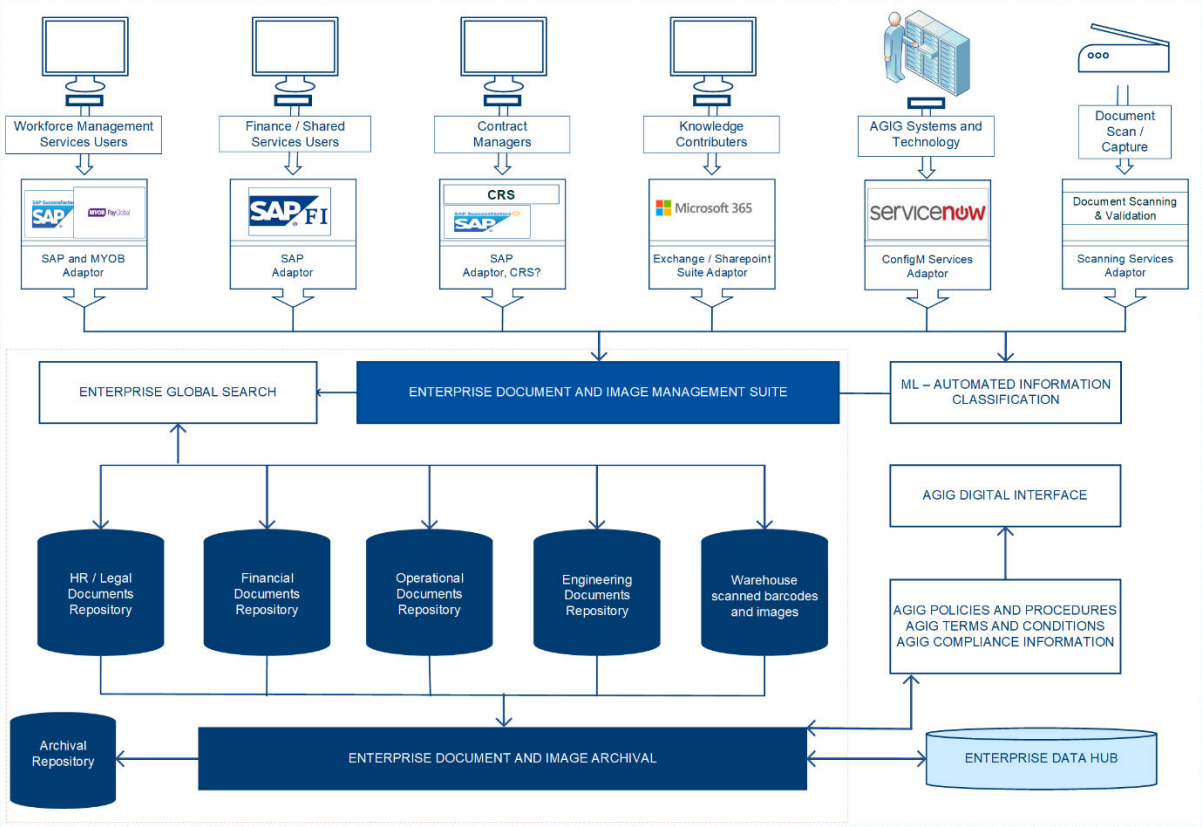
There are a number of emerging opportunities and obligations requiring the need for quality information for reporting and decision-making purposes. The hydrogen energy initiative is an example where emerging and disruptive technologies are highly dependent on data for sustainability and competitive advantage. As a good corporate citizen, AGIG has identified several UN Sustainable Development Goals that it will measure and action. Effective reporting is at the heart of these initiatives.

D.3.4 Enterprise content management

The AGIG enterprise is content-rich. Different types of data require different levels of protection and may create different levels of risk to the organisation, as well as different data lifecycle management. The development of enterprise content management capabilities aims to resolve most of the content management challenges, which are related to usability constraints, efficiency, effectiveness, and information risks. The strategic goal is to build a platform that consistently displays the following characteristics:

- the ability to scale up and out whenever new requirements come along from within AGIG or external ecosystem of customers, suppliers, and partners;
- embedded intelligent information governance to protect AGIG content and data;
- a mobile user experience consistent across devices that drives adoption and benefits realisation; and
- intelligent content management to enable innovation in business process improvements with flexibility and expected speed of delivery.

ECM reference architecture



AGIG enterprise utilises several SharePoint environments for content management. However, only Microsoft 365 is a strategic platform that AGIG will invest into. AGIG has recently completed an IT project to consolidate multiple SharePoint systems. The outcome of this project is archiving all unsupported legacy SharePoint environments and migrating active business content to SharePoint Online as part of the M365 platform. M365 provides strong capabilities for modern content management and the recent SharePoint Consolidation project is an important milestone for this strategic direction. Mature enterprise content services is an evolution of enterprise content management, which AGIG aims to achieve in stage three.

D.3.5 Summary

The program will be delivered utilising a mix of internal or external resources, managed centrally via the AGIG PMO. The proposed data warehouse and feasibility study is prudent because it:

- reduces the risks associated with cyber security (including release of sensitive information), regulatory reporting non-compliance, staff frustration, manual handling and poor-quality data (both of which can lead to substandard decision-making);
- is the most cost-effective way to uplift data architecture, reporting and governance across AGIG and provides the ability to manage all types of data and information (structured, unstructured, digital and physical);
- is sustainably cost efficient as it enables standardisation and synergies in the collection, storage, management and reporting of information (both historical and ongoing) across AGIG;
- provides a flexible foundation for future investment in and optimisation of automation and analytical tools that drive better processes and insights; and
- is deliverable. It uses existing and mature technology that can be readily implemented using a mix of internal and external resources.

Table Appendix 14 shows how the proposed option aligns with our vision objectives.

Table Appendix 14: Alignment with vision – Option 2 – Data architecture, reporting and governance

Vision objective	Alignment
Delivering for Customers – Public Safety	Y
Delivering for Customers – Reliability	Y
Delivering for Customers – Customer Service	Y
A Good Employer – Health and Safety	Y
A Good Employer – Employee Engagement	-
A Good Employer – Skills Development	-
Sustainably Cost Efficient – Working within Industry Benchmarks	-
Sustainably Cost Efficient – Delivering Profitable Growth	-
Sustainably Cost Efficient – Environmentally and Socially Responsible	Y

Appendix E Comparison of risk assessments for each option

Untreated risk	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Occasional	Unlikely	Unlikely	Occasional	Unlikely	Unlikely	Intermediate
Consequence	Severe	Minor	Trivial	Severe	Severe	Severe	
Risk Level	Intermediate	Low	Negligible	Intermediate	Intermediate	Intermediate	

Option 1	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Occasional	Unlikely	Unlikely	Occasional	Unlikely	Unlikely	Intermediate
Consequence	Severe	Minor	Trivial	Severe	Severe	Severe	
Risk Level	Intermediate	Low	Negligible	Intermediate	Intermediate	Intermediate	

Option 2	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Intermediate
Consequence	Severe	Minor	Trivial	Severe	Severe	Severe	
Risk Level	Intermediate	Low	Negligible	Intermediate	Intermediate	Intermediate	

Option 3	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Remote	Remote	Unlikely	Remote	Remote	Remote	Low
Consequence	Severe	Minor	Trivial	Severe	Severe	Severe	
Risk Level	Low	Low	Negligible	Low	Low	Low	

Appendix F Cost estimates

Option 2 – Foundational Initiatives

AGIG One IT Strategy Capex Program		Total AGIG cost 2023/24 to 2027/28	Allocation Basis	MGN Portion	MGN Allocation					
					2023/24	2024/25	2025/26	2026/27	2027/28	Total
Real $2021		Forecast	Allocator	MGN Portion	Forecast	Forecast	Forecast	Forecast	Forecast	Forecast
Foundational initiatives										
T4T-05	Uplift Cyber Security Technology & Capabilities (IT)	**$ 6,222,200**	**Equal**	33.3%	$ 469,000	$ 719,000	$ 485,667	$ 200,200	$ 200,200	$ 2,074,067
T4T-05	Uplift Cyber Security Technology & Capabilities (OT)	**$ 2,049,000**	**Direct**	20.0%	$ 135,960	$ 105,960	$ 95,960	$ 25,960	$ 45,960	$ 409,800
T4T-05	Uplift Cyber Security Technology & Capabilities (IT & OT) - AGN specific	**$ 6,765,000**	**Direct**	0.0%	$ -	$ -	$ -	$ -	$ -	$ -
Total Foundational initiatives		**$ 15,036,200**			**$ 604,960**	**$ 824,960**	**$ 581,627**	**$ 226,160**	**$ 246,160**	**$ 2,483,867**

Option 3 – Foundational and Transformational Initiatives

AGIG One IT Strategy Capex Program		Total AGIG cost 2023/24 to 2027/28	Allocation Basis	MGN Portion	MGN Allocation					
					2023/24	2024/25	2025/26	2026/27	2027/28	Total
Real $2021		Forecast	Allocator	MGN Portion	Forecast	Forecast	Forecast	Forecast	Forecast	Forecast
Foundational initiatives										
T4T-05	Uplift Cyber Security Technology & Capabilities (IT)	**$ 6,222,200**	**Equal**	33.3%	$ 469,000	$ 719,000	$ 485,667	$ 200,200	$ 200,200	$ 2,074,067
T4T-05	Uplift Cyber Security Technology & Capabilities (OT)	**$ 2,049,000**	**Direct**	20.0%	$ 135,960	$ 105,960	$ 95,960	$ 25,960	$ 45,960	$ 409,800
T4T-05	Uplift Cyber Security Technology & Capabilities (IT & OT) - AGN	**$ 6,765,000**	**Direct**	0.0%	$ -	$ -	$ -	$ -	$ -	$ -
Total Foundational initiatives		**$ 15,036,200**			**$ 604,960**	**$ 824,960**	**$ 581,627**	**$ 226,160**	**$ 246,160**	**$ 2,483,867**
Transformational initiatives										
T4T-07	Data Architecture, Reporting & Governance: Metadata Management and Information Classification - MGN only	**$ 933,400**	**Direct based on project**	100.0%	$ 933,400	$ -	$ -	$ -	$ -	$ 933,400
T4T-07	Data Architecture, Reporting & Governance: Raw data storage and Operational Reporting	**$ 2,188,480**	**Revenue**	18.2%	$ 310,441	$ 88,152	$ -	$ -	$ -	$ 398,593
T4T-07	Data Architecture, Reporting & Governance: Implement Standard Data Warehouse	**$ 2,195,040**	**Revenue**	18.2%	$ -	$ 399,788	$ -	$ -	$ -	$ 399,788
T4T-07	Data Architecture, Reporting & Governance: Establish Enterprise Reporting self-service	**$ 698,440**	**Revenue**	18.2%	$ -	$ 127,209	$ -	$ -	$ -	$ 127,209
T4T-07	Data Architecture, Reporting & Governance: Implement Data Virtualisation and Analytics Platform	**$ 983,359**	**Revenue**	18.2%	$ 179,102	$ -	$ -	$ -	$ -	$ 179,102
T4T-07	Data Architecture, Reporting & Governance: Implement ECM	**$ 962,820**	**Revenue**	18.2%	$ 175,361	$ -	$ -	$ -	$ -	$ 175,361
T4B-02	OneERP Phase 2 (MGN)	**$ 21,014,117**	**Direct based on project**	100.0%	$ 4,388,302	$ 12,162,982	$ 4,462,833	$ -	$ -	$ 21,014,117
T4B-02	MGN ISU Tech Upgrade	**$ 10,853,405**	**Direct based on project**	100.0%	$ 2,577,684	$ 6,647,711	$ 1,628,011	$ -	$ -	$ 10,853,405
T4B-02	OneERP Phase 3 (AGN), plus AGN Transition	**$ 38,465,210**	**Direct based on project**	0.0%	$ -	$ -	$ -	$ -	$ -	$ -
Total Transformational initiatives		**$ 78,294,271**			**$ 8,564,289**	**$ 19,425,841**	**$ 6,090,844**	**$ -**	**$ -**	**$ 34,080,974**
Total AGIG One IT Program		**$ 93,330,471**			**$ 9,169,249**	**$ 20,250,801**	**$ 6,672,470**	**$ 226,160**	**$ 246,160**	**$ 36,564,840**

4 Capex V.21.CS – Digital Customer Experience

4.1 Project approvals

Table 4-1: Project approvals

Prepared by	Chris Fidler, Head of Customer & Market Services
Reviewed by	Stephanie Judd, Head of Stakeholder Engagement
Approved by	Paul May, Chief Financial Officer

4.2 Project overview

Table 4-2: Project overview

Description of the problem / opportunity	As part of our regulatory submission process, MGN conducts a regular and thorough customer engagement process. Customer preferences and expectations are explored and assessed through a series of workshops. During the customer engagement process for MGN customers told us, among other things, that they expect an improvement in our digital communication capability. Customers said they expect we will have digital capabilities consistent with other energy sector participants (e.g. electricity distributors), including: • support for vulnerable customers; • the ability to communicate with them digitally, rather than the current one-way, manual and paper based approach; • some important notifications or updates via SMS; and • opportunities for website self-service. These expectations are consistent with findings from previous customer engagement processes in Victoria, and in other jurisdictions. The customer engagement process completed as part of the most recent AGN South Australia (AGN SA) access arrangement (AA) resulted in the development (and AER approval) of a vulnerable customer assistance program and the establishment of modern digital communication capabilities. Fundamental to both of these programs is the introduction of a customer relationship management (CRM) system. MGN has an existing CRM system as part of the SAP ECC6 platform. However, it has limited functionality and is at the end of its technical design life, with support ceasing during the next AA period. Consistent with AGIG's 'One IT' strategy, the plan is to develop an organisation-wide CRM system. Earlier this year, we began work on the foundational components of a CRM system for AGIG. This will deliver the capability that is currently provided by our end of life SAP CRM system. Developing an AGIG-wide CRM system will provide significant efficiencies in design and development, and will continue to deliver efficiencies in maintenance and support over the life of the system. This business case describes the IT investment required to complete development of the CRM system in the next AA period, as well as providing the digital customer communication capabilities that our customers have requested, and better support our vulnerable customers. We consider that this proposed investment is consistent with customer expectations and the actions of a prudent service provider. The investment will enable MGN to meet changing customer and regulatory needs, and customer expectations that our digital services are as easily accessible as those provided by other energy sector participants.

Untreated risk	As per risk matrix = **Intermediate (not ALARP)**
Options considered	• **Option 1** – Complete the development of a CRM system to enable the Priority Services Program (previously vulnerable customer assistance program) and digital communication capability, and develop SMS and website self-service functionality ($3 million) • **Option 2** – Complete CRM system foundational elements only, replacing existing CRM functionality and enabling the Priority Services Program ($0.2 million)
Proposed solution	Option 1 is the recommended option. It provides for the delivery of a flexible and consistent modern digital communication solution that reflects customer priorities and expectations. It will also allow us to improve our service for vulnerable customers and ensure ongoing compliance and proactive reporting that reflects the shift in customer and regulatory expectations.
Estimated cost	The forecast direct capital cost during the next access arrangement (AA) period (July 2023 to June 2028) is $3 million.

real 2021 $'000	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Capex	869	1,095	1,002	-	-	2,965

There is also approximately $1 million opex associated with developing the system, along with ongoing operating costs of approximately $0.3 million per annum. This expenditure will be absorbed by MGN and recovered through ongoing operational efficiencies expected to be achieved via this project.

Basis of costs	All costs in this business case are expressed in real 2021 unescalated dollars unless otherwise stated. Some tables may not tally due to rounding.
Alignment to our vision	This investment aligns with the *Delivering for Customers* aspect of our vision, as it will dramatically improve our customers' ability to interact with us, and will enhance the overall quality of our service that customers have told us they expect, allowing us to engage with them effectively and process their queries efficiently. It also aligns with our objective to remain *Sustainably Cost Efficient*, as the proposed solution is designed to be scalable, meaning it can grow and be efficiently modified to meet our requirements and those of our customers as they change over time. Improving our digital capabilities also brings us into line with what is becoming industry standard for network businesses in Australia. Conscious of our impact on tariffs, we have sought to roll out programs and systems nationally allowing us to deliver greater benefits to Victorian customers by sharing costs across the AGIG businesses.
Consistency with the National Gas Rules (NGR)	This project complies with the following National Gas Rules (NGR): **NGR 79(1)** – the proposed solution is consistent with good industry practice, several practicable options have been considered, and market rates have been tested to achieve the lowest sustainable cost of providing this service. **NGR 79(2)** – proposed capex is justifiable under NGR 79(2)(c)(iii) and (iv). Our recent customer engagement process shows that there is existing demand for digital communication capabilities such as SMS that are available from other energy providers and outside of our current technological capabilities. In addition, the CRM system and modern digital capabilities are necessary to allow us to comply with our regulatory obligations. There is a growing focus from regulators to provide increased protection for vulnerable customers and to limit the practice of disconnection of supply for non-payment, as evidenced by:

	• AER initiation of the Consumer Policy Research Centre (CPRC) to investigate regulatory approaches to consumer vulnerability; • ESCV implementation of the Payment Difficulty Framework; and • the AER Statement of Expectations of energy businesses: Protecting consumers and the energy market during COVID-19[26]. **NGR 74** – the forecast costs are based on typical vendor market rates, published licence fees and standard implementation costs. We sought independent scope verification and cost estimation. Therefore, the estimate has been arrived at on a reasonable basis and represents the best estimate possible in the circumstances. **NGR 91** – the proposed solution is consistent with good industry practice, and is consistent with what a prudent service provider acting efficiently to achieve the lowest sustainable cost of service delivery would do, with two options having been considered to address the identified risks and the least cost option being selected.
Treated risk	As per risk matrix = **Low**
Stakeholder engagement	We are committed to operating our networks in a manner that is consistent with the long-term interests of our customers. To facilitate this, we conduct regular stakeholder engagement workshops to understand and respond to the priorities of our customers and stakeholders. Feedback from stakeholders is built into our asset management considerations and is an important input when developing and reviewing our expenditure programs. Customer preferences and expectations have been explored and assessed through a series of workshops. Insights from these workshops highlighted that our customers expect our communication channels and service options to reflect broader market trends, which increasingly means offering a variety of digital communication channels. Customers expressed their interest in online options for engaging with us on topics of: • outages (planned and unplanned); • maintenance and works, including mains replacement; • establishing new gas connections; • raising queries about metering and meter reading; and • submitting feedback to us. Feedback from our workshops emphasise that customers expect we will find a balance between concerns regarding gas prices, and technology solutions that enable better communication through a variety of channels.
Other relevant documents	• Attachment 8.2 (V.26.CS) Opex Business Cases, Priority Services Program • Attachment 9.9 IT Investment Plan

4.3 Background

Previous customer engagement processes both in Victoria and other jurisdictions have highlighted the need for us to improve our digital communication. Our digital communication capabilities across all AGIG businesses are well short of the modern standards customers have told us they expect.

Regulators also expect network businesses to be able to communicate more effectively. For example, the Australian Energy Regulator's (AER) *Statement of Expectations of energy*

[26] Though the AER's Statement of Expectations was released in response to the COVID-19 crisis, it is reasonable to assume the same expectations around customer communication and protecting vulnerable customers will apply going forward (post-COVID).

businesses: Protecting consumers and the energy market during COVID-19[27] required energy businesses to:

- not disconnect any residential or small business customers who may be in financial stress except as a measure of absolute last resort;
- prioritise clear, up-to-date communications with customers about the issues addressed in this Statement, including by keeping website, social media and call centre waiting and hold messages up to date, so customers can readily access updates when they need them and relieve some pressure on affected call centres; and
- minimise the frequency and duration of planned outages for critical works, and provide as much notice and real time information as possible to assist households and businesses to manage during any outage.

This requirement set an important precedent with regard to protecting customers experiencing vulnerability or hardship, as well as keeping customers informed generally. We therefore consider it prudent to maintain practices consists with the AER's Statement of Expectations even as Victorian emerges from pandemic conditions.

4.3.1 Current customer communication process capabilities

Compared to Victorian electricity distributors, when it comes to customers, we are 'low touch'. Yet there are common circumstances where customers need to communicate with us and when we need to communicate with them. For example, customers regularly need to contact us regarding renovations and new connections. We also need to communicate frequently with consumers about issues such as planned and unplanned outages, new gas connections, customer enquiries and meter reading matters.

Historically, our communication services have been predominantly manual and paper based, resulting in the following outcomes for customers:

- *Connections:* The connection process is predominately one-way, with customers communicating with their retailer for their connection application and to obtain status updates. Customers do not receive status updates in real time.
- *Unplanned outages:* Existing systems are unable to quickly establish which gas customers are impacted by supply outages, with MGN typically only aware of an outage when a supply interruption is reported to the 24 hour faults and emergency centre. In addition, we do not have the necessary customer information or the capability to notify customers of an unplanned outage. As a result, gas customers do not receive notifications of outages or an estimated time for service restoration and may be lacking critical information to make operational business decisions.
- *Planned maintenance and meter changes:* Communication processes rely on a letter box notification addressed to the occupier/householder of the address. These paper-based notifications are often left unread and treated as junk mail. Communications about meter changes and resolving issues encountered during meter reading are facilitated through a physical card being left at the door. Each of these scenarios have resulted in customers not being aware of information relating to works at their premises or in their local community.

27 https://ww.aer.gov.au/publications/corporate-documents/aer-statement-of-expectations-of-energy-businesses-protecting-consumers-and-the-energy-market-during-covid-19

- *Meter readings:* A number of customers receive estimated gas bills, due to meter readers being unable to read gas meters due to locked premises or unrestrained dogs. This results because currently there is no cost effective means to provide advance notice of a meter read – the notification of the next scheduled meter reading day is listed on their most recent gas bill which is approximately two months prior. Moreover, meters are read within a two to three day window, so even if a customer had noted the date, their meter may be read on a different day.

- *Priority customers:* The current method of alerting our vulnerable customers to outages is highly manual and as a result prone to error.

- *Customer engagement management:* MGN currently uses our existing SAP (ECC6) CRM system as the core platform to support customer engagement management. This provides the capability to manage customer complaints, claims, compliments and enquiries. The SAP ECC6 platform (including our existing CRM) is end of life, with support ceasing during the next AA period.

4.3.2 Customer and stakeholder expectations

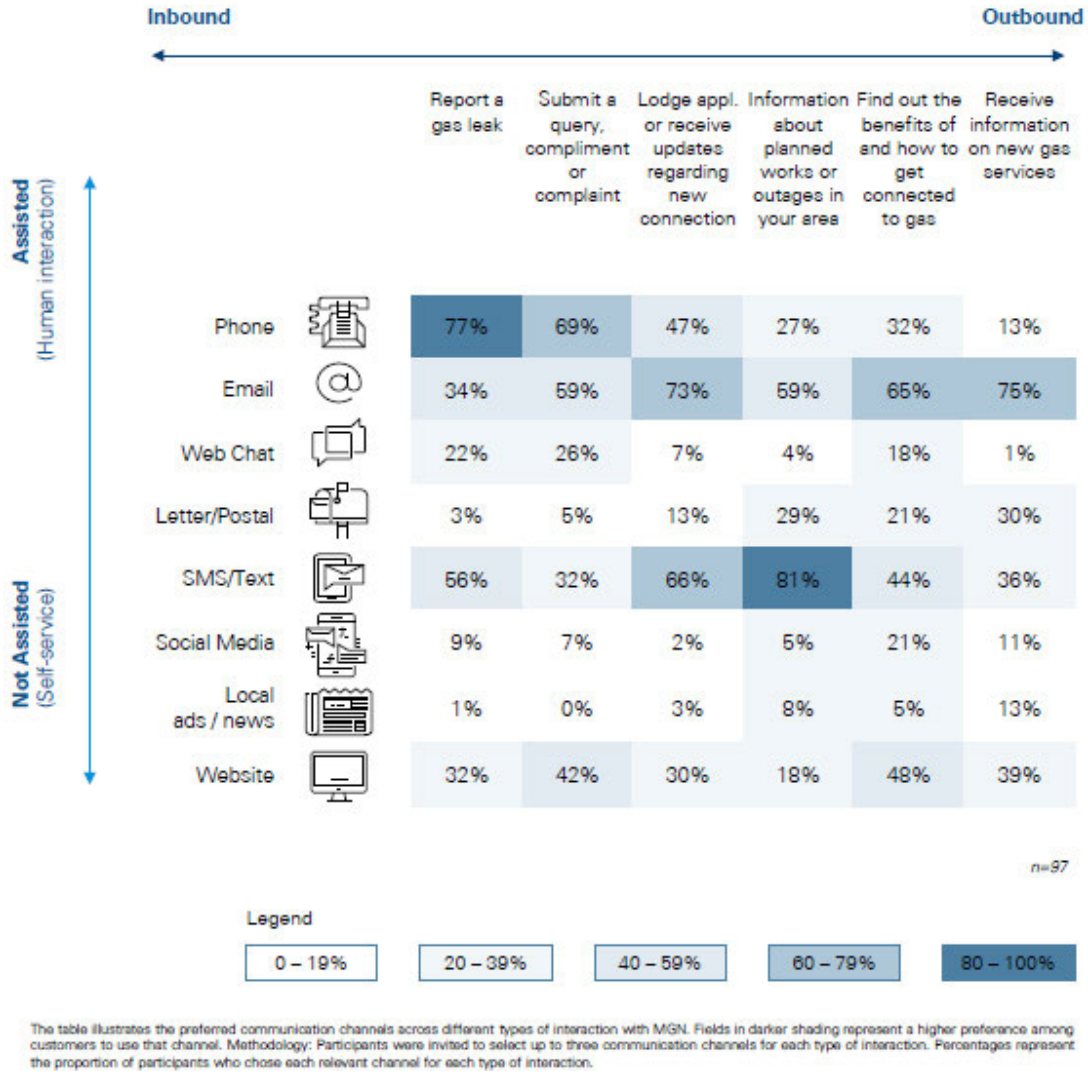
Shifts in technology are leading to changing expectations among our customers and our regulators. Customers expect communication processes to be simple and to utilise tools such as online and mobile technology, which they would use when communicating with any other supplier.

Over the past 18 months, MGN has conducted a comprehensive customer and stakeholder engagement program. This is outlined in Chapter 5 of our Final Plan. The objective of this program is to help ensure that investment priorities reflect customer and stakeholder needs now and over the longer term, to ensure our strategy has their support. All documentation from this extensive engagement is provided on our dedicated engagement website, Gas Matters[28]. Relevant findings from our engagement program are summarised below.

Our customer engagement encompassed a series of workshops across three phases of engagement that were conducted across several core topics. One of these topics, digital services, explored customers' views on channels and services that empower them through digital and support transparency of how they consume gas services. Phase 1 of the engagement process captured customers' channel preferences across a range of interaction types, and this is shown in Figure 4-1.

28 https://gasmatters.agig.com.au/victorian-engagement-plan

Figure 4-1: Customers' communication channel preferences



The table illustrates the preferred communication channels across different types of interaction with MGN. Fields in darker shading represent a higher preference among customers to use that channel. Methodology: Participants were invited to select up to three communication channels for each type of interaction. Percentages represent the proportion of participants who chose each relevant channel for each type of interaction.

Key findings are:

- Customers have a strong preference to receive updates via SMS, including for planned works or outages (81%), and for updates on connection applications (66%). Customers receive outage notifications and restoration SMS messages from their electricity distribution providers and they expect similar SMS notifications from their gas distributors.

- For interactions where time criticality or reassurance is required, customers prefer to use the phone (77% of customers prefer phone when reporting a gas leak and 69% when submitting a query, complaint or compliment).

- Customers prefer email across most interaction types, but particularly for outbound or information-based communications (70% of customers prefer email when receiving information on new gas services or lodging applications / receiving updates regarding a new connection).

- Website remains a strong function for communication, with 49% of customers preferring to find out the benefits of, and how to get connected to gas; and 42% of customers choosing websites to submit a query, compliment or complaint.

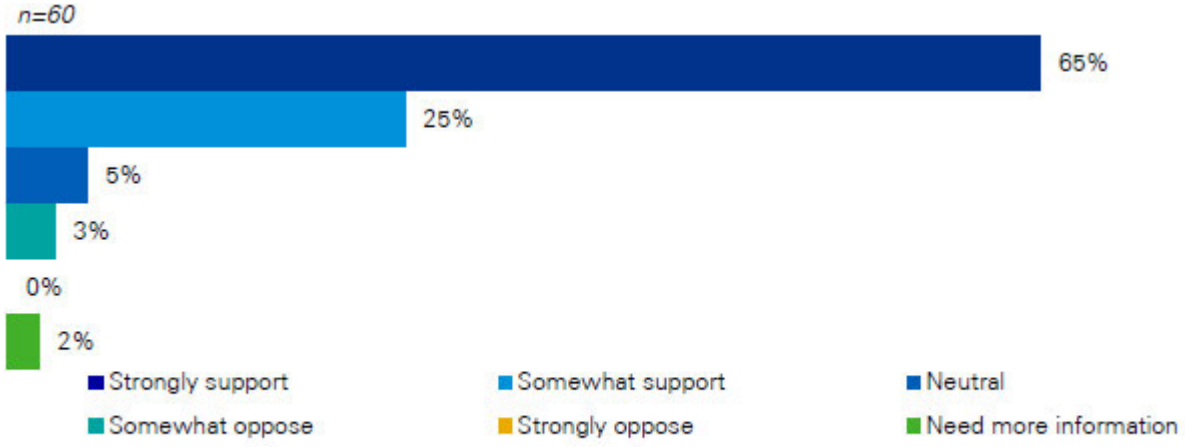
In response to the strong preference indicated for digital channels, in phase 2 we presented three digital package options with indicative pricing per user, per annum:

- More website services ($0.50);
- More website and email ($1.00); or
- More website, email and SMS ($2.50).

More than half of our customers (56%) supported the more website, email and SMS package.

Based on customer feedback from phase 2, and the strong preference for SMS communication from phase 1, we modified the phase 3 engagement process proposal. The revised proposal was to deliver a digital services package that included SMS capability for works updates/notifications and website enhancements, supported by a CRM system, but at the lower $1 per annum price point. The revised package saw a portion of customers who were previously supportive of lower priced packages (excluding SMS) become supportive of SMS in phase 3, indicating that they saw value in SMS at the reduced price point. Overall, 90% of customers supported the revised digital services package, of which 65% strongly supported this, as shown in Figure 4-2.

Figure 4-2: Support for digital services



Other areas of the customer engagement process also explored preferences in relation to digital capabilities. Key outcomes included:

- A significant proportion of customers prefer to not receive estimated bills (45%). Customers have expressed interest in receiving notifications from their distribution business on the day the meter reader will attend, as this enables them to make meter access more readily available. Customers have also expressed interest in being able to submit their own meter reads, to ensure the bill they receive is based on actual usage and to prevent bill shock in subsequent meter billing periods.
- Customers recognised the importance of us supporting vulnerable customers, in particular, the elderly and those with illness (92%).
- Culturally and Linguistically Diverse (CALD) customers were particularly interested in SMS communications as it made translation easier.

As can be seen from the above discussion, our customer consultation process has highlighted the desire for improved digital communication in relation to a variety of services.

4.3.3 Priority services program

In December 2021, the AER published a Draft Consumer Vulnerability Strategy, acknowledging the need for a whole of energy sector approach to addressing the issue of consumer vulnerability[29]. Specifically, this document outlines a range of outcomes, objectives and actions designed to achieve the AER's vision to 'see consumers experiencing vulnerability offered timely and effective support that works for both consumers and energy businesses, improving energy affordability, helping consumers stay connected and reducing energy businesses' cost to serve'.

MGNs systems have been modified in 2021 to accommodate the AEMC rule change for life support customers, ensuring that life support registers are accurate and up-to-date and support the AER's Life support registration guide[30].However this technology is only able to support life support customers and does not address risks associated with other customers experiencing vulnerability or hardship.

AGIG's response to this, and our ongoing commitment as a socially responsible organisation, has been the development of a Priority Services Program to support customers experiencing vulnerability (see Priority Services Business Case at Attachment 8.2). This program aims to improve the customer experience for our priority service customers and also reduce the financial barriers that some customers experiencing vulnerability may face in terms of utilising gas more efficiently and/or ensuring their appliances are operating in a safe and reliable manner.

A core requirement of the program is the development of a 'priority services register', which will form the basis for the provision of a range of priority services to our vulnerable customers, including the provision of advance notice of planned outages, priority support in an emergency and/or a dedicated liaison person where required. Development of this register will require a CRM system, which will then also be used to implement and monitor the delivery of the priority services.

4.4 Risk assessment

Risk management is a constant cycle of identification, analysis, treatment, monitoring, reporting and then back to identification (as illustrated in Figure 4-3). When considering risk and determining the appropriate mitigation activities, we seek to balance the risk outcome with our delivery capabilities and cost implications. Consistent with stakeholder expectations, safety and reliability of supply are our highest priorities.

Figure 4-3: Risk management principles

Our risk assessment approach focuses on understanding the potential severity of failure events associated with each asset and the likelihood that the event will occur. Based on these two key inputs, the risk assessment and derived risk rating then guides the actions required to reduce or manage the risk to an acceptable level.

Our risk management framework is based on:

- AS/NZS ISO 31000 Risk Management – Principles and Guidelines;
- AS 2885 Pipelines-Gas and Liquid Petroleum, and
- AS/NZS 4645 Gas Distribution Network Management.

[29] https://www.aer.gov.au/news-release/aer-takes-energy-companies-to-task-on-life-support
[30] https://www.aer.gov.au/retail-markets/compliance-reporting/aer-life-support-registration-guide-2021

The *Gas Act 1997* and *Gas Regulations 2012*, through their incorporation of AS/NZS 4645 and the Work Health and Safety Act 2012, place a regulatory obligation and requirement on us to reduce risks rated high or extreme to low or negligible as soon as possible (immediately if extreme). If it is not possible to reduce the risk to low or negligible, then we must reduce the risk to as low as reasonably practicable (ALARP).

When assessing risk for the purpose of investment decisions, rather than analysing all conceivable risks associated with an asset, we look at a credible, primary risk event to test the level of investment required. Where that credible risk event has an overall risk rating of intermediate or higher, we will undertake investment to reduce the risk.

Six consequence categories are considered for each type of risk:

1. **People** – injuries or illness of a temporary or permanent nature, or death, to employees and contractors or members of the public.
2. **Environment** (including heritage) – impact on the surroundings in which the asset operates, including natural, built and Aboriginal cultural heritage, soil, water, vegetation, fauna, air and their interrelationships
3. **Supply –** disruption in the daily operations and/or the provision of services/supply, impacting customers
4. **Compliance** – the impact from non-compliance with operating licences, legal, regulatory, contractual obligations, debt financing covenants or reporting / disclosure requirements
5. **Reputation** – impact on stakeholders' opinion of MGN, including personnel, customers, investors, security holders, regulators and the community
6. **Financial** – financial impact on MGN, measured on a cumulative basis

Note that risk is not the sole determinant of what investment is required. Many other factors such as growth, cost, efficiency, sustainability and the future of the network are also considered when we develop technology solutions. The risk management framework provides a valuable tool to manage our assets, and prioritise our works program, however it is not designed to provide a binary (yes/no) trigger for investment. As prudent asset managers, we apply our experience and discretion to manage and invest in our technology for our distribution networks in the best interests of existing and potential customers.

A summary of our risk management framework, including definitions, is provided in Attachment 9.5 to our Final Plan.

The primary risk event associated with not investing in developing a digital customer experience is the inability to appropriately triage and respond to client needs, particularly with regard to life support and vulnerable customers. This also translates into compliance risk as the regulatory demands evolve in response to changing conditions.

Specific risks include:

- a lack of, or miscommunication with customers on maintenance and outage information due to the current archaic communication methods. The consequences of this risk are heightened for vulnerable customers with the potential for a life-threatening situation in the event of outages or planned maintenance of which they are unaware;
- data and cyber security vulnerabilities associated with poor data storage capabilities resulting in the potential for a data breach and associated compliance and reputational consequences; and

- a formal complaint, resulting in poor reputation and the potential for compliance action and regulatory penalties.[31]

The resulting untreated risk rating is presented in Table 4-3.

Table 4-3: Untreated risk

Untreated risk	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Hypothetical	Hypothetical	Hypothetical	Occasional	Occasional	Occasional	Intermediate
Consequence	Trivial	Trivial	Trivial	Severe	Severe	Severe	
Risk Level	Negligible	Negligible	Negligible	Intermediate	Intermediate	Intermediate	

4.5 Options considered

We have considered the following options to improve our customer communication capabilities:

- **Option 1 –** Complete the development of a CRM system to enable the Priority Services Program (previously vulnerable customer assistance program) and digital communication capability, and develop SMS and website self-service functionality

- **Option 2 - Complete CRM foundational elements only, replacing existing CRM system functionality and enabling the** Priority Services Program **(MGN)**

Existing SAP ECC6 CRM functionality currently supports some self-service capabilities for MGN customers including making enquiries and claims, filing complaints and providing compliments via the website. We do not consider it inappropriate to reduce these capabilities from existing service levels, and as such, an option of discontinuing the development of the CRM for MGN has not been considered.

4.5.1 Option 1 – Complete the development of a CRM. Develop digital comms capability

This option involves:

- development of a CRM to support our priority service customer program, as well as implementing modern digital communications capabilities; and

- delivery of the key digital communication capabilities supported by customers during our stakeholder engagement program, namely SMS and website self-service capabilities.

In addition to supporting current customer communication requirements, it delivers the functionality required to position the business to meet near term customer expectations.

4.5.1.1 CRM system

As discussed above, our customer engagement processes have highlighted the need for us to continue to expand our digital capabilities and enable more of our customers to engage with us when and how they want to. A modern CRM system is necessary to support the digital engagement that our customers have said they expect, and provides the robust and secure back-end capability that underpins such improvements. In addition, a CRM system is necessary to provide the database capability that will support our vulnerable customer assistance program in Victoria.

---

31 https://www.smh.com.au/business/they-were-ridiculously-high-flood-of-complaints-over-eyewatering-gas-bills-20171011-gyygm4.html

Specifically, a CRM system provides the following benefits:

- the ability for customers to provide AGIG with information to allow better service provision, including preferences for communication channels; report their interest in specific energy related topics for ongoing provision of targeted information; accurate meter self-readings to ensure bills reflect actual usage and to prevent bill shock; and vulnerable customer information such as health related issues and details of appliances installed;
- the ability to capture, track, respond and update customers on their enquiries and requests at any point in time;
- improved customer experience through modernised capability and the delivery of a more personalised service; and
- the ability to categorise and segment customer information, and assign security roles to appropriate users, i.e. restricting access to sensitive vulnerable customer information to selected staff.

In 2019, we developed the AGIG IT Roadmap and Strategy to standardise the AGIG technology landscape, supporting an AGIG-wide consistent approach to IT. We consider this a prudent and efficient approach that provides a common platform and technology layer across AGIG while leveraging economies of scale in application development, maintenance and support. A core component of this strategy is the implementation of SAP, standardising shared service processes across AGIG. The first stage of our SAP One ERP project for AGN and DBP is well-progressed and Stage 2 (One ERP for MGN) commences in 2023 (see AGIG One IT Business Case in this Attachment).

Despite this, a non-SAP (standalone) CRM was proposed and approved by the AER as part of the AGN SA AA submission. At the time, it was considered that this approach could deliver comparable functionality to a SAP CRM system for a similar cost. However the CRM system was at this time in its early stages with specific requirements yet to be developed and integration issues having not been fully considered. Over the last two years, and in parallel with the customer engagement program, AGIG has performed significant further work including developing business requirements, understanding integration capabilities and reviewing potential solutions, and these are discussed further below.

Business requirements

Over the last 18 months we have engaged key business areas, as well as an external support partner, in order to develop high level CRM requirements. The key criteria for these requirements were to:

- enable the customer engagement process outcomes, including digital customer communication needs and the priority services program;
- provide all AGIG businesses with customer focussed CRM functionality that reflects modern good business practice across key areas; and
- leverage efficiencies from the system development, as well as ongoing maintenance and support.

The outcome of these engagements was a set of overarching requirements for the CRM system[32]. At a high level, these requirements include customer connection management, operational / services

[32] more detailed requirements are currently under development

workflow automation, customer interaction tracking and management, and operational information management.

Integration considerations

A key objective of the AGIG One IT Strategy is to reduce architectural complexity and risk by simplifying and standardising the technology landscape. This is achieved through minimising the breadth of technologies supported, and implementing solutions that are fit-for-purpose and where possible, able to be easily integrated with other systems-of-record. This will enable consistent business processes, improve trust in core data sets, reduce manual interventions and reduce risks associated with regulatory reporting, business continuity and cybersecurity.

Requirements and scoping work performed over the last 18 months (since the AGN SA business case approval) has highlighted that a non-SAP based CRM system would require development of a new integration platform to integrate the data and improve transfer between the SAP One ERP system and any non-SAP CRM. Data architecture subject matter experts consider that this would be a complex exercise that would come with significant risk and cost.

In contrast, an integrated and flexible SAP CRM system would:

- allow us to utilise SAP PO (Process Orchestration) to integrate the CRM solution into the existing SAP architecture, and allow for the gradual collection of customer data without large upfront costs, reducing any risk associated with non-provision of data or minimal customer adoption of self-service capabilities;
- provide the ability to easily connect the SAP CRM to other SAP modules[33]; and
- allow us to readily validate or confirm vulnerable customer status or life support requirements.

Product solution

At the time of development of the South Australian business case, the only SAP product that had been considered was SAP S4 HANA. Supporting our integrated SAP principle, SAP's Cloud for Customer (C4C) has now been thoroughly assessed as a potential solution.

SAP C4C is accessed via a modern, user-friendly interface that provides a much better user experience than the S/4HANA CRM, promising easier and more streamlined functionality. In addition, it provides desirable capabilities that are either not available or have limited functionality on the S/4HANA CRM system. For example, field crew can leverage the mobile C4C sale or service functionality to assist with work management. The cloud platform also enables streamlined automatic system updates and is better positioned to effectively mitigate the threats associated with potential cyber attacks.

The SAP C4C product provides for the ability to pick and choose modules as required to support desired functionality, allowing for the addition of modules in the future as necessary. It therefore supports the modern CRM functionality expected by our customers as well as setting the foundations for future customer digital communication requirements.

Development of a national SAP CRM capability leverages significant economies of scale. A large component of the project relates to the development of core technology that is required regardless of whether the system is implemented across a single business or multiple businesses.

[33] An example is the Enterprise Asset Management (EAM) module. Integration between EAM and our CRM would allow us to seamlessly access a holistic view of the customer, enabling a view of the number and type of service requests for a customer, regardless of the property.

A significant portion of system development costs can therefore be shared across AGIG businesses.

Following preliminary scoping and requirements elicitation for the system, we now estimate that the cost per business for this solution is less than half of our original estimate for an integrated SAP CRM. In addition, while the long-term costs of systems are difficult to quantify, it is expected that a SAP solution will result in lower maintenance and support costs on an ongoing basis. In particular this is due to:

- consistency with AGIG's SAP architecture and considerably simpler, less costly and less risky integration;
- the enhanced capabilities and future modules available through SAP C4C providing a much better long and short term product solution; and
- significantly reduced costing for a SAP CRM system that will be shared across AGIG, providing economies of scale in both application development and deployment as well as ongoing maintenance and support.

We now consider that a fully integrated customisable SAP solution that is consistent across AGIG is a considerably better long-term option than the standalone non-SAP solution proposed as part of the AGN SA AA submission.

On this basis, AGIG has begun work on the initial stage of integrated SAP CRM system development, delivering the foundational capabilities within the current AA period. This first stage utilises the $1.3 million funding endorsed for MGN in the current period SAP CRM Refresh business case (IT23).

4.5.1.2 SMS and website self-service

As discussed in section 4.3.2, key digital communication preferences stated as expected by our customers included:

- timely notifications via SMS, including for planned works, outages and restorations; updates on connection applications; and notifying customers as to when their meter will be read; and
- a preference not to receive estimated bills and the ability to submit their own meter reading.

This business case therefore includes investment for the delivery of such capabilities within the next AA period, supported by the CRM system, in particular including:

- SMS capability used to increase and improve communications with customers around unplanned and planned outages and works; new connections and alterations; and meter reading notification; and
- developing a number of customer-facing webforms to allow website self-service, such as enabling customers to submit their own meter reads if they choose to do so following notification their meter has not been able to be read by our meter readers.

Further information on these requirements is provided in Appendix B.

MGN submitted a similar business case for the current period (IT37 Customer Experience Improvements Program for $1.5 million), which was not approved in the AER's draft decision for this AA period. We accepted this decision and committed to undertake additional customer and stakeholder engagement during the current period before we implemented such a program. As described above, we have now engaged extensively with customers and stakeholders on their requirements around communication and their broader digital experience, and consider this more modest program to be consistent with customer and stakeholder expectations.

4.5.1.3 Cost assessment

As discussed above, the SAP CRM system is being developed nationally and rolled out across AGIG. This will provide significant economies of scale. A large component of the project is the development of core capability that will support either a single or multiple businesses.

The CRM system development has been separated into two components:

1. a foundational CRM system; and
2. CRM digital communication capabilities.

The foundational phase establishes a central CRM that can be leveraged across the organisation to deliver improved, responsive customer service and interactions. It will develop core customer management functionality, including providing functionality to support customers making enquiries and claims, filing complaints and providing compliments via our website. This will replace the existing functionality that is currently available to MGN customers through the end of life SAP ECC6 platform and delivered this on a modernised platform. In addition, it provides the functionality required to support the priority services program.

The CRM digital communication capabilities phase builds on the foundational CRM, delivering digital capabilities that enable greater self-service, along with more personalised and timely customer communications. It enables the outcomes that our customers expect from a contemporary energy business. This includes the ability to communicate via current and any future channels that customers desire. It also enables modern digital capabilities such as customer connection management, operational / services workflow automation, customer interaction tracking and management, and operational information management.

This option also includes estimated costs for the development of the key digital communication capabilities that customers have requested in our recent engagement process, namely SMS notifications and the provision of information to us through website self-service via webforms.

The cost of Option 1 for MGN is $3 million as shown in Table 4-4.

Table 4-4: Cost estimate – Option 1, $'000 real 2021

Option 1	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Foundational CRM	183	-	-	-	-	183
Comms capabilities	329	1,095	1,002			2,425
SMS and webforms	357	-	-	-	-	357
Total	**869**	**1,095**	**1,002**	**-**	**-**	**2,965**

There are additional operating costs associated with this option, as there will be an ongoing requirement to operate and maintain the enhanced digital capabilities and CRM system. This additional expenditure (of approximately $1 million) will be funded from within existing opex allowances.

The key benefits associated with this program have been outlined above. In addition, the new SAP CRM system will:

- achieve tighter service integration and provide greater service efficiencies through technology and process integration with retailers; and
- increase the frequency of reports and updates from field and operations teams, facilitating agile working practices through digitisation of key workflows.

4.5.1.4 Risk assessment

The solution proposed under Option 1 reduces the likelihood from occasional to remote for the compliance, reputation and finance risk categories as a result of responding to customer needs and expectations, and addressing risks associated with vulnerable customers. This reduces the overall risk rating from intermediate to low, which is consistent with our risk management framework.

Table 4-5: Risk assessment – Option 1

Option 1	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Hypothetical	Hypothetical	Hypothetical	Remote	Remote	Remote	Low
Consequence	Trivial	Trivial	Trivial	Severe	Severe	Severe	
Risk Level	Negligible	Negligible	Negligible	Low	Low	Low	

4.5.1.5 Alignment with vision objectives

Table 4-6 shows how Option 1 aligns with our vision objectives.

Table 4-6: Alignment with vision – Option 1

Vision objective	Alignment
Delivering for Customers – Public Safety	-
Delivering for Customers – Reliability	-
Delivering for Customers – Customer Service	Y
A Good Employer – Health and Safety	-
A Good Employer – Employee Engagement	-
A Good Employer – Skills Development	-
Sustainably Cost Efficient – Working within Industry Benchmarks	Y
Sustainably Cost Efficient – Delivering Profitable Growth	-
Sustainably Cost Efficient – Environmentally and Socially Responsible	Y

This investment aligns with the *Delivering for Customers* aspect of our vision, as it will dramatically improve our customers' ability to interact with us and will enhance the overall quality of our service that they have told us they expect, allowing us to engage with customers and address their requests efficiently.

It also aligns with our objective to remain *Sustainably Cost Efficient*, as the proposed solution is also designed to be scalable, meaning it can grow and be efficiently modified to meet our requirements and those of our customers as they change over time. Introducing better digital capabilities also brings us into line with what is becoming industry standard for network businesses in Australia. Conscious of our impact on tariffs, we have sought to roll out programs and systems nationally allowing us to deliver greater benefits to Victorian customers by sharing costs across the AGIG businesses. It is socially responsible, as development of a CRM system will enable implementation of the vulnerable customer program.

4.5.2 Complete CRM foundational elements only

This option entails only delivering the foundational elements of the SAP CRM. As described in Option 1, this would include development of functionality to support customers making enquiries and claims, filing complaints and providing compliments via our website. This replaces the

functionality that currently exists for MGN, prior to support for SAP ECC6 being discontinued during the next AA period. The new CRM system would also provide the capability required for the Priority Services Program being proposed (see Priority Services Program Business Case in Attachment 8.2 to the Final Plan).

However, the digital communication capabilities that our customers have stated they expect would not be developed, as the foundational elements of the new CRM system will not be digital communications capable.

4.5.2.1 Cost assessment

As discussed under Option 1, a large component of the SAP CRM system development costs are being shared nationally. The majority of the costs for the CRM system foundational elements are funded in the current AA period, with $0.2 million expected to be remaining to complete the project in the next AA period.

Table 4-7: Cost estimate – capex - Option 2, $'000 real 2021

Option 2	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Foundational CRM	183	-	-	-	-	183
Total	**183**	**-**	**-**	**-**	**-**	**183**

In addition to development of the vulnerable customer program, customers would benefit from functionality to support customers making enquiries and claims, filing complaints and providing compliments via our website.

4.5.2.2 Risk assessment

While Option 2 reduces the compliance risk associated with an inadequate response to life support and vulnerable customers, it does not address reputational / customer or potential associated financial risks related to an outdated and potentially flawed method of responding to our other customers' needs.

As a result, this Option retains the intermediate untreated risk rating. This is not considered ALARP, and as such, is inconsistent with the requirements of our risk management framework.

Table 4-8: Risk assessment – Option 2

Option 2	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Hypothetical	Hypothetical	Hypothetical	Occasional	Occasional	Remote	Intermediate
Consequence	Trivial	Trivial	Trivial	Severe	Severe	Severe	
Risk Level	Negligible	Negligible	Negligible	Intermediate	Intermediate	Low	

4.5.2.3 Alignment with vision objectives

Table 4-9 shows how Option 2 aligns with our vision objectives.

Table 4-9: Alignment with vision – Option 2

Vision objective	Alignment
Delivering for Customers – Public Safety	-
Delivering for Customers – Reliability	-
Delivering for Customers – Customer Service	N
A Good Employer – Health and Safety	-

A Good Employer – Employee Engagement	-
A Good Employer – Skills Development	-
Sustainably Cost Efficient – Working within Industry Benchmarks	N
Sustainably Cost Efficient – Delivering Profitable Growth	-
Sustainably Cost Efficient – Environmentally and Socially Responsible	N

Option 2 would not align with *Delivering for Customers*, as it does not provide any improvement in our current service for non-vulnerable customers, in particular, it does not deliver the SMS and website self-service capabilities expected by our customers. Current communication practices will remain for all customers who are not vulnerable customers.

Option 2 would also not be *Sustainably Cost Efficient*, as it fails to bring our customer communication capabilities up to industry standard and is likely only to result in costs to improve our digital customers solutions being deferred to future AA periods.

4.6 Summary of costs and benefits

Table 4-10 presents a summary of how each option compares in terms of the estimated capital cost in the next AA period, the residual risk rating, and alignment with our vision objectives.

Table 4-10: Comparison of options

Option	Estimated cost ($ million)	Treated residual risk rating	Alignment with vision objectives
Option 1	3.0	Low	Aligns with *Delivering for Customers* and aligns with *Sustainably Cost Efficient.*
Option 2	0.2	Intermediate / non-ALARP	Does not align with *Delivering for Customers* or *Sustainably Cost Efficient*, as it does not provide the digital communication capabilities expected by customers and consistent with modern standards.

4.7 Recommended option

Option 1 has been identified as the most prudent and efficient option. It represents the most efficient level of investment needed to ensure ongoing compliance and support for all customers, meeting the increasing regulatory and customer demands.

4.7.1 Why is the recommended option prudent?

Option 1 is the most prudent solution because it:

- provides a back-end capability (CRM system) to support both improvements in customer digital interactions, and our critical vulnerable customer assistance program, providing the ability to apply special security around our most vulnerable customers;
- is consistent with customer and stakeholder expectations and providing the digital communication capabilities desired by our customers, in particular, SMS communication and some website self-service capabilities;
- provides the capacity for future digital communication needs expected by customers;

- is an efficient long-term solution, with an architecture which will easily adapt and scale to our future needs as these change, without any loss in quality of service. Quick deployment of software plug-ins mean there is no need to invest in a complex integration layer;
- is the most efficient option for reducing risks to an acceptable level:
  - While Option 2 reduces the compliance risk associated with an inadequate response to life support and vulnerable customers, it does not address reputational / customer or potential associated financial risks related to an outdated and potentially flawed method of responding to our other customers' needs.
  - While a non-SAP CRM was proposed and approved in the AGN SA AA submission (SA137), further investigations have revealed this solution to be non-optimal and likely to introduce additional elements of risk, and ongoing cost, into AGIG's IT architecture. A new SAP solution has the benefits of being consistent with the rest of the AGIG One IT strategy and to provide the most cost-effective CRM solution over the long term;
- satisfies all regulatory obligations, including privacy legislation. Life support customers can be notified of maintenance activities in the required time with evidentiary justification provided; and
- is deliverable. The proposed implementation takes into account the other major programs of work going on. Each development stage considers resource availability and solution dependencies. It is well paced and within industry standards.

4.7.2 Estimating efficient costs

The planning for this project has utilised an independent expert consultant ([redacted] to assist in validating and updating the scope of the project as well as estimating the costs to replace the high-level estimates originally developed with the AGIG IT Strategy and Roadmap. The estimate assumes migration of 800,000 customers and 160,000 contacts in a single stage migration; and a low to medium quantity of customisations.

The cost estimate includes:

- labour costs, including project management, solution and infrastructure / cyber architects, business analysts, developers, testers, trainers, business as usual support. External labour reflects estimated market rates; Internal labour is based on salary and on-cost, and estimated effort; and
- relevant licencing and other vendor development and support costs.

4.7.2.1 CRM

Expenditure related to this project includes capex and opex and these costs will be shared nationally, leveraging significant cost efficiencies not only upfront in development, but also over the life of the system through operations and maintenance.

The estimated direct capital cost of the CRM system across AGIG is $10.5 million, as shown in Table 4-11.

Table 4-11: Cost estimate – Total AGIG capex, $'000 real 2021

	CY2022 & H1/2023	2023/24	2024/25	2025/26	2026/27	2027/28	Total Project
Foundational CRM	2,766	507	-	-	-	-	3,273

Comms capabilities	-	1,917	2,735	2,619	-	-	7,270
Total AGIG	**2,766**	**2,424**	**2,735**	**2,619**	**-**	**-**	**10,543**

The ongoing requirement to maintain the CRM solution for AGIG results in additional operating costs. The estimated additional costs will be absorbed within the current opex forecast. These are summarised in Table 4-12.

Table 4-12: Cost estimate – Total AGIG opex, real 2021 $'000

	2023/24	2024/25	2025/26	2026/27	2027/28	Total
CRM maintenance	493	537	537	537	537	2,643
Total AGIG	493	537	537	537	537	2,643

Shared capex and opex costs are allocated between the AGIG distribution businesses on the basis of customer numbers, with MGN attracting 35% of the expenditure. Direct costs, such as licence costs based on number of users and SMS costs based on number of SMS sent have been directly allocated to each of the AGIG distribution businesses. The resulting capital and operating forecast for MGN for the next Access Arrangement period is shown in Table 4-13.

Table 4-13: Cost estimate – MGN capex & opex, real 2021 $'000

	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Capex	512	1,095	1,002	-	-	2,608
Opex	202	220	220	220	220	1,082

4.7.2.2 Digital customer experience

The digital customer experience costs are business-specific. These capital and operating costs are shown in Table 4-14 and Table 4-15. As with the CRM system, opex costs are funded through existing opex levels.

Table 4-14: Cost estimate – Digital communication capex, $'000 real 2021

	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Webforms	298	-	-	-	-	298
Automated SMS	59	-	-	-	-	59
Total	357	-	-	-	-	357

Table 4-15: Cost estimate – Digital communication opex, real 2021 $'000

	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Automated SMS	34	51	51	51	51	237
Total	34	51	51	51	51	237

4.7.2.3 Total cost

The total capex associated with this business case is therefore shown in Table 4-16. As noted above, operating expenditure does not form part of the business case, as it is covered through business efficiencies.

Table 4-16: Cost estimate – Total capex, $'000 real 2021

	2023/24	2024/25	2025/26	2026/27	2027/28	Total
Foundational CRM	183	-	-	-	-	183
Comms capabilities	329	1,095	1,002	-	-	2,425
Digital Communication	357	-	-	-	-	357
Total	869	1,095	1,002	-	-	2,965

4.7.3 Consistency with the National Gas Rules

In developing these forecasts, we have had regard to Rule 79 and Rule 74 of the NGR. With regard to all projects, and as a prudent asset manager/network business, we give careful consideration to whether expenditure is conforming from a number of perspectives before committing to investment.

NGR 79(1)

The proposed solution is prudent, efficient, consistent with accepted and good industry practice and will achieve the lowest sustainable cost of delivering pipeline services:

- **Prudent** – The expenditure is necessary in order to continue to meet customer and regulatory expectations, and is of a nature that a prudent service provider would incur.
- **Efficient** – Implementing a CRM system is the most practical and effective option. It is also the most cost effective option. Given the nature of data that we are required to hold and the privacy and data legislation that surrounds it, a CRM system that is capable of plugging in to our existing architecture is the most efficient. Work will be carried out by internal staff and external contractors as skills demand requires. Any work carried out by external contractors will be based on competitively tendered rates. The expenditure is therefore of a nature that a prudent service provider acting efficiently would incur.
- **Consistent with accepted and good industry practice** – Whilst the nature of the electricity distributor in Victoria is different to our business, customers continue to expect similar digital capability. As conditions have evolved, the regulator expects more of us in dealing with vulnerable customers. This sets expectations of a minimum capability that we are unable to achieve with current systems and processes.
- To achieve the **lowest sustainable cost of delivering pipeline services** – The proposed solution (option 1) achieves the necessary risk reduction and improvement in customer capabilities. The other options considered do not deliver the required risk reduction or customer benefits. Therefore, the chosen option is consistent with the objective of achieving the lowest sustainable cost of service delivery.

NGR 79(2)

Proposed capex is justifiable under NGR 79(2)(c)(iii) and (iv). Our recent customer engagement process shows that there is existing demand for digital communication capabilities such as SMS

that are available from other energy providers and outside of our current technological capabilities.

In addition, the CRM system and modern digital capabilities are necessary to allow us to comply with our regulatory obligations. There is a growing focus from regulators to provide increased protection for vulnerable customers and to limit the practice of disconnection of supply for non-payment. For example, the the Australian Energy Regulator's (AER) *Statement of Expectations of energy businesses: Protecting consumers and the energy market during COVID-19*[34] set important and welcome precedents for the way gas distribution businesses should interact with customers, particularly those experiencing vulnerability and hardship.

As Victoria emerges from pandemic conditions, while the formal obligation to comply with the AER's Statement of Expectations falls away, we believe it is prudent and in keeping with customers' expectations to maintain this level of diligence with respect to vulnerable customers. Implementing an effective CRM will allow us to maintain this level of service and satisfy our ongoing obligations to communicate with all customers (vulnerable or otherwise) in a timely, sensitive, and consistent manner.

NGR 74

The forecast costs are based on typical vendor market rates, published licence fees and standard implementation costs. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.

NGR 91

The proposed solution is consistent with good industry practice, and is consistent with what a prudent service provider acting efficiently to achieve the lowest sustainable cost of service delivery would do, with four practicable options having been considered to address the identified risks and the least cost option being selected.

34 https://ww.aer.gov.au/publications/corporate-documents/aer-statement-of-expectations-of-energy-businesses-protecting-consumers-and-the-energy-market-during-covid-19

Appendix A Comparison of risk assessments for each option

Untreated risk	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Hypothetical	Hypothetical	Hypothetical	Occasional	Occasional	Occasional	Intermediate
Consequence	Trivial	Trivial	Trivial	Severe	Severe	Severe	
Risk Level	Negligible	Negligible	Negligible	Intermediate	Intermediate	Intermediate	

Option 1	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Hypothetical	Hypothetical	Hypothetical	Remote	Remote	Remote	Low
Consequence	Trivial	Trivial	Trivial	Severe	Severe	Severe	
Risk Level	Negligible	Negligible	Negligible	Low	Low	Low	

Option 2	People	Supply	Environment	Reputation	Financial	Compliance	Risk
Likelihood	Hypothetical	Hypothetical	Hypothetical	Occasional	Occasional	Remote	Intermediate
Consequence	Trivial	Trivial	Trivial	Severe	Severe	Severe	
Risk Level	Negligible	Negligible	Negligible	Intermediate	Intermediate	Low	

Appendix B Detailed digital program requirements

Priority Services Program

Development of a robust CRM system will support the establishment of our priority service program that targets Victorian customers and communities in vulnerable circumstances. This includes working closely with community groups and customer advocates to tailor the program to Victorian network customers. The program contains similar service deliverables to those being rolled out in the AGN (SA) and AGN (QLD) networks.

The development of a priority register will allow MGN to capture priority services customers' contact details to enable targeted communications and service delivery. These services will include advanced notice and ongoing provision of information concerning planned and unplanned supply interruptions, delivery of communication material in multiple languages and additional communication material targeted towards groups with low computer literacy. These customers will also be provided with tools to better understand and manage their expenditure on energy.

As part of the website self-service functionality, customers can provide details on their vulnerabilities if they so choose. They will be able to register through the portal enabling us to assess, for example, a disconnection request received from the retailer against the customer's information to determine if the disconnection is appropriate.

Implementing the MGN priority service customer register will enable the expansion of personalised services to our customers such as the establishment of a trade panel to further support the gas supply needs of priority service customers. Services will include gas appliance safety checks, emergency appliance repairs and targeted support during outages. The trade panel and MGN field crews will support vulnerable customers with emergency heating and cooking capabilities during extended outages.

SMS capability

SMS capability will be used to extend and improve communications with customers in the following scenarios:

Unplanned gas outages – Customers will receive an SMS notification, with a tracking reference number, as confirmation of their call to MGN's call centre. This notification will include estimated arrival time of the gas crew as well as pertinent information related to the type of gas fault. If the field crew are delayed or re-directed, whilst enroute, the customer will be advised of the delay along with a new estimated arrival time. Upon the repair of the gas fault, the customer will be informed their gas supply has been restored and provide information as to how further assistance can be provided, such as re-lighting appliances.

Planned outages and gas main works – Customers will be provided with an option to 'opt in' to receive SMS updates for any planned outages such as planned meter replacement or upgrades of gas mains. Customers currently receive hand delivered mail addressed to The Householder when planned works are expected to interrupt their gas supply. Many of these letters are not opened resulting in customers not being prepared for the planned works when they occur. SMS messages can provide advanced notice of mains works in the area and enable customers to be better prepared for dealing with the increased volume of traffic and potential restricted access where they live. Increased awareness and notice also allows residents to seek out field crews to discuss any concerns prior to the day in which road and footpath openings may occur. Similar to unplanned outages, the use of SMS can advise customers when all works have been completed in an area and provide information as to how MGN can assist them in areas such as appliance re-lights.

New homes, new gas connections and alterations – Connection of new gas services to new homes or amendments to existing homes can result in a multiple stakeholder involvement including Builders, Gas fitters and the customer. The installation of gas services and the fitting of gas meters also requires effective communications to limit to risk of delays in the process. SMS

notifications and confirmations will be provided at the various stage of the connection process. These will include: acknowledgement of the service request and advice if any additional information from the customer is required, the day and time the MGN representative will visit the site to finalise installation planning, requests to the builder or gas fitter for any additional requirements for a compliant site, notification of the service installation day (this allows the builder to ensure clear access is available for the gas service installation), updates on the status of the service installation and of the meter fit, and finally provision of information to the builder and customer that the connection has been completed.

Complaint Management – the implementation of SMS capability will allow the MGN customer resolutions teams to provide an alternative customer communication medium that best suits some customers. There are a number of customer complaints that may take some time to complete. These can include complaints regarding systemic gas supply or reinstatement works associate with road and footpath openings[35]. The use of SMS will allow more timely and more frequent notifications to be sent to customers regarding the status of rectification works as well as information regarding the completion of agreed outcomes with customers.

Meter reading notification – MGN will advise customers they can opt in to receive SMS notifications for the day their gas meter will be read. Currently gas retailers provide a gas reading window on the customer gas invoice of around 5 days for the customers next scheduled reading date. Not only is the 60 day cycle difficult for customers to remember, their gas meter may not even be read by their distributor on the NSRD. Providing a SMS notification with the actual date that the gas meter will be read provides the customer with greater control and confidence around areas such as unlocking gates or securing their dogs so that an actual meter read can occur. This provides the customer with greater assurance about people coming onto their property and will result in more customers receiving gas bills based on actual consumption and not based on an estimated calculation of usage.

Meter self-read

Option 1 will include the development of web-based capability that will enable residents to provide a customer self-read. Online meter reading capability will allow customers more personal control over their service and allow them to engage at a time, place and channel that suits. Customers can create an account and submit their meter readings, alleviating property access issues and potentially creating a tangible, financial benefit by reducing the number of meter readers required. The new capability on the MGN web site can be used by customers when they are not home when the meter reader attends their premise and they choose not to leave access gates unlocked, for customers who are anxious about unknown workers entering their properties or for installations that have traditionally been difficult to capture an actual meter read such as medium and high-density housing complexes.

Final functionality will be designed in conjunction with consumer advocates however it could be expected the self-meter reading capacity would have the capability to email the customer when a self-read is due and to notify the customer when they will be required to organise an appointment to meet actual meter reading regulatory requirements.

[35] The Victorian Ombudsman (EWOV) raised a systemic issue during 2020 on MGN, requiring improvement in the provision of restoration status communications