

Attachment 9.9

Capex Business Cases (IT)

July 2025

PUBLIC & SOCI ACT PROTECTED

Contents

SA217 - IT operational applications	1
1.1 Project approvals	1
1.2 Project overview	1
1.3 Background	3
1.4 Risk assessment	6
1.5 Options considered	8
1.6 Summary of options assessment	16
1.7 Proposed solution	17
SA238 – IT corporate applications	31
1.1 Project approvals	31
1.2 Project overview	31
1.3 Background	35
1.4 Risk assessment	38
1.5 Options considered	40
1.6 Summary of options assessment	51
1.7 Proposed solution	51
SA239 – IT sustaining infrastructure	77
1.1 Project approvals	77
1.2 Project overview	77
1.3 Background	81
1.4 Risk assessment	87
1.5 Options considered	90
1.6 Proposed solution	107
SA240 – Cyber security (SOC1 Act PROTECTED)	118
1.1 Project approvals	118
1.2 Project overview	118
1.3 Background	121
1.4 Risk assessment	125
1.5 Options considered	127
1.6 Summary of options assessment	136
1.7 Estimating the efficient costs	137
SA241 – AGN transition	143
1.1 Project approvals	143

1.2 Project overview	143
1.3 Background	145
1.4 Risk assessment	148
1.5 Options considered	150
1.6 Summary of options assessment	158
1.7 Proposed solution	158

SA217 - IT operational applications

1.1 Project approvals

Table 0.1: SA217 IT operational applications – Project approvals

Prepared by	Simon Petherick, Manager, Asset Management Systems
Reviewed by	Brooke Palmer, Head of IT Business Engagement
Approved by	Brett Miller, Chief Information Officer

1.2 Project overview

Table 0.2: SA217 IT operational applications – Project overview

Description of problem /opportunity	<p>A suite of IT critical applications are used to operate the AGN South Australian network. These include our enterprise asset management system (Maximo), our metering & billing system (Oracle CC&B), the FRC Gateway (webMethods) and our Geographic Information System (GE Smallworld). Like all applications, these are subject to periodic upgrade to ensure they are functional, cyber-secure, and supported by the vendor.</p> <p>Upgrades are generally recurrent in nature and are driven by vendor releases, mapped against business need. We adopt an N-1 approach (i.e. one level of redundancy) to managing the operational applications suite. This means we typically maintain application versions that are one version older than the latest vendor offering. This allows us to fully assess the value and benefit of an upgrade before we decide whether to adopt it. We identify the optimal time to apply minor and major version upgrades, rather than relying solely on the vendor-driven upgrading/patching schedule.</p> <p>The operational apps covered by this business case are currently owned by our delivery partner APA, who operate the AGN SA network under a longstanding contractual arrangement. Note these operational apps are distinct from our AGIG-owned corporate apps, which are discussed in business case SA238.</p> <p>Under normal circumstances, the operational app upgrades would continue as per the usual n-1 upgrade cycle, with a new version typically becoming available every 3 to 5 years (depending on the app). However, the contractual arrangement with APA to operate our network is coming to an end in 2027, after which AGIG will commence operating the network itself. As part of this transition, the suite of operational apps required to run the network must transition from APA's IT environment to AGIG's IT environment.</p> <p>The AGN transition period is scheduled to commence from 1 July 2027 and is expected to take around 18 months. Given the scale of the work involved and criticality of these operational apps, this business case considers how the AGN transition affects the upgrade cycle of operational applications and what upgrades could be brought forward or deferred.</p>
Untreated risk	As per risk matrix = High
Options considered	<ul style="list-style-type: none"> Option 1 – Deliver operational app upgrade cycle in parallel with the AGN transition (\$18.1 million capex and \$0.6 million opex) Option 2 – Pause the upgrade cycle for critical apps during the transition window (\$18.8 million capex, \$1.5 million opex)

	<ul style="list-style-type: none">• Option 3 – Uplift resources and bring forward upgrade of core applications before the transition (\$20.4 million capex, \$0.6 million opex)																								
Proposed solution	<p>Option 2 is recommended as it is vital that critical apps such as Maximo and the metering & billing system are in a steady state, with vendor support, during the transition. These apps are fundamental to operating our business and the risk and effort required to upgrade these apps during the transition is too great.</p> <p>Option 1 and 3 may be more appealing if the upgrades and transition go smoothly, however, both these options carry a higher risk of complications during the app upgrades and a risk of materially impacting the ~\$300 million AGN transition. Option 2 therefore is the most prudent option.</p>																								
Estimated cost	<p>The forecast direct capital and operating cost during the next AA period is shown below.</p> <table><tr><th>\$'000</th><th>Jan 2025</th><th>26/27</th><th>27/28</th><th>28/29</th><th>29/30</th><th>30/31</th><th>Total</th></tr><tr><td>Total capex</td><td></td><td>4,404</td><td>1,743</td><td>2,717</td><td>4,331</td><td>5,560</td><td>18,755</td></tr><tr><td>Total opex</td><td></td><td>269</td><td>326</td><td>383</td><td>300</td><td>192</td><td>1,469</td></tr></table> <p>The opex cost is primarily for extended support for core applications while they remain in their current version.</p>	\$'000	Jan 2025	26/27	27/28	28/29	29/30	30/31	Total	Total capex		4,404	1,743	2,717	4,331	5,560	18,755	Total opex		269	326	383	300	192	1,469
\$'000	Jan 2025	26/27	27/28	28/29	29/30	30/31	Total																		
Total capex		4,404	1,743	2,717	4,331	5,560	18,755																		
Total opex		269	326	383	300	192	1,469																		
Basis of costs	All costs in this business case are expressed in real unescalated dollars of January 2025 unless otherwise stated.																								
Treated risk	As per risk matrix = Moderate																								
Alignment to our vision	<p>This project aligns with the <i>Customer Focussed</i> aspect of our vision by ensuring technology systems supporting operations, billing and the call centre are adequately maintained and available to meet customers’ needs.</p> <p>This project aligns with our vision objective of being <i>A Leading Employer</i>, as it aims to provide reliable, accurate and fit-for-purpose technology solutions that allow employees and contractors to do their jobs effectively.</p>																								
Consistency with the National Gas Rules (NGR)	<p>NGR 79(1)/91 – Maintaining a stable set of Information Technology (IT) applications is critical to our business. Critical apps such as Maximo, GIS, and Oracle CC&B inform our business decisions and helps us to efficiently manage our business processes. Mitigating the risk of application outages by pausing the upgrade program during the AGN transition and deferring upgrades to critical applications until the transition is complete is the most prudent course of action. Further, if there is a likelihood any pre-transition upgrades cannot be completed in time, it may impact the AGN transition delivery and complexity, which is a significant risk. The preferred option will ensure business continuity during the transition and also provides opportunity to re-evaluate the application upgrade cycle once the software is in AGIG’s IT environment.</p> <p>NGR 79(2)/91 – The proposed expenditure is required to maintain integrity of services by ensuring applications are supported and fit for purpose throughout the AGN transition. Expenditure on upgrades – or extended support where upgrades are postponed – is vital to ensure our operational apps continue to function, allowing us to avoid material outages that might impact business continuity.</p> <p>NGR 74 – The forecast costs are based on the latest market rate testing, and project options consider the requirements of our application environment. Application upgrades are scheduled and costed as per the software providers’ recommendations. Cost assessments have been conducted for each option based on the best information available at the time of developing this business case. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.</p>																								
Stakeholder engagement	Customers consistently ranked price and affordability as their top priority. They also told us that they place a great deal of importance on safety and reliability of supply. Customers were clear they expect good communication and simple service that is																								

Other relevant documents	<p>resolution-focused. Customers agreed that supplying cleaner energy was important, but that affordability is a key consideration for them.</p> <p>Investment in our operational applications is fundamental to maintaining the safe and reliable operation of our gas distribution network in South Australia. Core applications such as Maximo and Oracle CC&B are central to our daily operations. Therefore, it is critical that we transition these applications to the AGIG IT environment and then continue to invest in these applications through timely recurrent upgrades.</p> <p>Our risk-based approach to managing these applications involves assessing business needs to determine the optimal timing for recurrent upgrades and the implementation of non-recurrent application implementations and targeted application improvements. By adopting an N-1 approach to version management, we ensure a thorough evaluation of the value and benefits before adoption whilst mitigating risks associated with outdated and unsupported systems through timely recurrent upgrades. This approach to IT investment helps us maintain sustainable costs and mitigate potential impacts on customers' gas bills, aligning with their key priority of affordability while upholding safety and reliability.</p>
	<p>This business case should be read in conjunction with:</p> <ul style="list-style-type: none"> • IT Investment Plan • Risk Management Policy and Operational Risk Model (together our Risk Management Framework) • Capitalisation Policy • Other technology Business Cases: IT Corporate Apps, IT Sustaining Infrastructure, IT Cybersecurity and AGN Transition

1.3 Background

A suite of IT critical applications are used to operate the AGN South Australian network. Like all software, our operational applications are subject to periodic upgrade to ensure they are functional, cyber-secure, and supported by the vendor.

Upgrades are generally recurrent in nature and are driven by vendor releases, mapped against business need. We adopt an N-1 approach (i.e. one level of redundancy) to managing the operational applications suite. This means we typically maintain application versions that are one version older than the latest vendor offering. This allows us to fully assess the value and benefit of an upgrade/enhancement before we decide whether to adopt it.

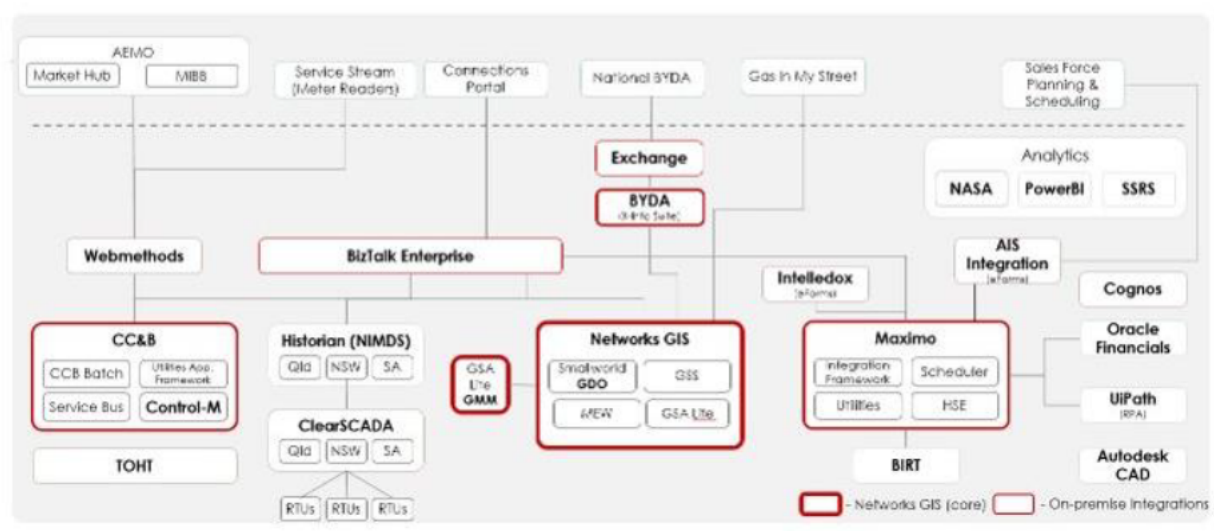
During the next regulatory period (2026/27 to 2030/31), upgrades fall due for our:

- Enterprise asset management system (Maximo)
- FRC gateway with AEMO (webMethods)
- Geographical information system (GE Smallworld)
- Metering & billing system (Oracle CC&B)
- Work and resource scheduling system (Workday)
- Middleware
- Mobility applications (Salesforce Lightning)
- Business intelligence system (Microsoft Power BI)

- Call centre telephony (NICE CXOne)
- Historian data storage software (OSISoft PI and changes to higher heating zones)
- UiPath automation software
- Meter data management software

Figure 0.1 shows how some of these key systems fit into the broader IT architecture that supports the SA networks.

Figure 0.1: AGN SA networks high-level IT architecture



These operational apps covered are currently owned by our delivery partner APA, who operate the AGN SA network under a longstanding contractual arrangement. Note these operational apps are distinct from our AGIG-owned corporate apps, which are discussed in business case SA238.

Under normal circumstances, the operational app upgrades would continue as per the usual n-1 upgrade cycle, with a new software version becoming available every 3 to 5 years (depending on each vendor's release cycle). However, the contractual arrangement with APA to operate our network is coming to an end in 2027, after which AGIG will transition to operating the network itself. This transition will see personnel, property, processes, assets, IT software, hardware and a range of new responsibilities shifting to AGIG. It is a large and extremely complex exercise, with the IT transition alone estimated at ~\$300 million over the next five years.

The AGN transition planning is progressing and timeframes have been set. As part of this transition, the suite of operational apps required to run the South Australian network must transition from APA's IT environment to AGIG's environment. These operational apps are the focus of this business case.

The AGN transition period is scheduled to commence from 1 July 2027 and is expected to take around 18 months. It will be a period of intensive work and considerable risk. The transition features migration of around 50 applications (including those due for upgrade listed in this business case) from APA's IT environment to AGIG's IT environment. Ideally, all apps being transitioned from APA to AGIG will be in a steady state and supported by the vendor throughout the transition, as this helps reduce complexity and the risk that an unsupported or incorrect version of an application has been migrated across to AGIG's IT environment. This is particularly

important for business-critical apps like Maximo, which is our enterprise asset management system, and Oracle CC&B, which is our metering and billing system.

Based on the recurrent upgrade cycle, Maximo is due for a major upgrade in 2026/27 and Oracle CC&B is due for upgrades in 2026/27 and 2030/31. If we were to go ahead with these upgrades, we would need to complete the 2026/27 upgrades prior to the transition period commencing 1 July 2027, so we can lift and shift them to AGIG in a steady state. If there is a likelihood the 2026/27 upgrades cannot be completed in time, it may impact the AGN transition delivery and complexity, which is a significant risk.

Table 0.3 summarises the upgrade requirements for the operational apps falling due during the next regulatory period.

Table 0.3: Summary of scheduled upgrades under normal circumstances (no AGN transition)

Application	Business criticality	Scheduled update	Transition delivery risk	Comments
Enterprise asset management (Maximo)	High	26/27	High	Maximo is our most important asset management solution and is core to ongoing network asset management, planning and investment. Major upgrade required from version 7.6.1.3 to version MA9. The current version will not be supported after Sep 2025.
FRC gateway (webMethods)	High	Annual	Medium	Provides access to AEMO's full retail contestability hub. Essential for customer transfers, billing and market notifications. Subject to annual updates to maintain currency.
GIS (GE Smallworld)	High	26/27, 28/29, 30/31	High	Used for network mapping and asset management. GE is ceasing support for the current version in Jun 2027.
Metering & billing (Oracle CC&B)	High	26/27 & 29/30	High	Provides transaction workflows, meter readings and delivery point billing. Support for current version ends in Apr 2027.
Workday	Medium	26/27 – 28/29	Low	Workday is provided as software as a service, version releases are automated and low effort.
Middleware	High	2026/27	Low	One-off project. Replace BizTalk with AIS (Azure Integration Services).
Mobility apps (Salesforce Lightning)	Medium	Annual	Low	Salesforce Lightning is provided as software as a service; version releases are automated and low effort.
Business intelligence (Power BI)	Medium	Annual	Low	Power BI is provided as software as a service; version releases are automated and low effort.
Call centre telephony (Nice CXOne)	High	27/28	Medium	Nice CXOne is provided as software as a service; version releases are automated and low effort.
Historian (OSISoft PI)	Medium	27/28 & 30/31	Medium	This is our storage repository for network and operational data. Upgrading during the transition would be of medium complexity but is unnecessary and we can operate on the current version for an additional year with minimal risk. All versions are supported by vendor.
UiPath	Low	26/27 & 29/30	Low	UiPath is used to automate processes in AGN SA operations only. It is relatively low cost and simple to update. The level of customisation and integrations with other operational systems is very low, which means the transition to the AGIG IT environment should be low risk. We therefore propose UiPath upgrades continue as per the scheduled business-as-usual upgrade program.

Heating value zone	Low	Annual	Low	Modifications in our historian software to enable new ways of allocating heating values to customers across different areas of the network. This will allow more accurate billing when accommodating different blends of renewable gas entering the network. This investment is low complexity and can be delivered in parallel with the AGN transition.
MDM	Low	26/27	Low	New functionality to be added to our metering and billing system to integrate with digital metering infrastructure and data. There will be an initial capital investment to add functionality, and an uplift in recurrent opex as digital meter volumes increase. The functionality enhancement is low risk and should be completed before the AGN transition.

As shown in the above table, several of these operational applications have a high or medium transition delivery risk. This means the potential for the AGN transition to impact delivery of these upgrades, or vice versa, is significant.

We must therefore consider which operational applications can be upgraded as per the above schedule, and which app upgrades could be brought forward or deferred.

It is also important to highlight that the operational app upgrades is an AGN-wide initiative. APA operates the AGN Victoria, AGN SA and AGN Queensland network, and most of these operational apps are shared between the three network businesses. Costs per application are generally allocated to AGN SA, Victoria and Queensland based on the number of customers serviced by each network, which for AGN SA is 35.2%. The exceptions to this allocation method are Historian and UiPath, which are primarily used by AGN SA and have an 81.4% and 100% allocation to AGN SA respectively.

This business case only covers the AGN SA allocation of the operational app upgrade costs.

1.4 Risk assessment

Risk management is a constant cycle of analysis, treatment, monitoring, reporting and then identifying once again, with a commitment to balance outcomes sought with delivery and cost implications considered and assessed.

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.

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 and activities required to ensure safety and compliance are not compromised, while delivery of this outcome is done as efficiently and effectively as possible.

The risk rating assesses the consequence and likelihood of the risk. The risk of an event associated with failure of an asset is rated based on the combined effect of the consequence

Figure 0.2: Risk management principles



and likelihood rating to provide an overall risk rating. This risk rating guides the risk management and mitigation activities and facilitates prioritisation.

Our Operational Risk Framework is based on AS/NZS 2885 and requires all identified risks ranked as intermediate or above to be addressed. For risks ranked as high we must *'Modify the threat, the frequency or the consequence to reduce the risk rank to intermediate or lower'*.

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 moderate or higher, we will undertake investment to reduce the risk.

Seven consequence categories are considered for each type of risk:

- **Health & safety** – injuries or illness of a temporary or permanent nature, or death, to employees and contractors or members of the public
- **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
- **Operational capability** – disruption in the daily operations and/or the provision of services/supply, impacting customers
- **People** – impact on engagement, capability or size of our workforce
- **Compliance** – the impact from non-compliance with operating licences, legal, regulatory, contractual obligations, debt financing covenants or reporting / disclosure requirements
- **Reputation & customer** – impact on stakeholders' opinion of AGN, including personnel, customers, investors, security holders, regulators and the community
- **Financial** – financial impact on AGN, measured on a cumulative basis

The primary risk event being assessed for our IT operational applications program is that one or more critical applications are not in a steady state during the AGN transition, leading to application outages and extended timeframes for completing the AGN transition.

For example, Maximo is a critical app. It is our enterprise asset management system used for asset tracking, maintenance and work order management. It is central to our network operations and any extended outage to it would severely impact our ability to operate the network, leading to compliance, operational and reputational risks. If Maximo was not in a steady state when we come to transfer it from the APA to the AGIG environment, we may experience compatibility issues, data loss and security vulnerabilities during its transition. To mitigate this risk, we would either have to run two instances of Maximo – one in each IT environment – or extend the AGN transition timeframes to allow sufficient time to resolve the problems. Neither outcome is desirable. The overall risk rating associated with IT operational applications is presented in the following table.

Figure 0.3: Untreated risk rating – IT operational apps

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

1.5 Options considered

The options considered are:

- **Option 1** – Deliver operational app upgrade cycle in a parallel with the AGN transition.
- **Option 2** – Pause the upgrade cycle for critical apps during the transition window.
- **Option 3** – Uplift resources and bring forward upgrade of core applications before the transition.

These options are discussed in the following sections. Note that all options assume the AGN transition is happening from 1 July 2027 and will take approximately 18 months. However, Option 1 is essentially a baseline of upgrade requirements and reflects the program that would be undertaken even if there was no transition.

1.5.1 Option 1 – Deliver operational app upgrade cycle in parallel with the AGN transition

Under this option, we would progress the application upgrades as per the business-as-usual cycle, delivering upgrades to all applications while the AGN transition is ongoing. This includes upgrades to critical operational applications such as our enterprise asset management system, our metering & billing system, our GIS and the FRC gateway.

1.5.1.1 Advantages and disadvantages

The advantage of this option is that the applications will remain current and supported by the vendor. This mitigates the risk of apps failing or experiencing extended outages.

However, the pending AGN transition means the disadvantages to this option are substantial. When the APA-owned apps are migrated over to the AGIG IT environment, it is important they are in a steady state. This means they must in an easily identifiable version, data is current and fully backed up, and all app functionality is stable.

Upgrading an application while simultaneously migrating it to a new IT environment can introduce multiple risks, including:

- **Compatibility issues** – The new version may not be fully compatible with the new environment, causing unexpected errors or degraded performance
- **Increased complexity** – Performing two major changes at once makes troubleshooting difficult; if issues arise, it is hard to determine whether the upgrade or the migration is the cause
- **Data loss or corruption** – If migration processes aren't handled properly, data could be lost or corrupted during the transition
- **Configuration conflicts** – The new environment may have different settings, dependencies, or security protocols that don't align with the upgraded application
- **User disruption** – If not planned carefully, downtime or unexpected failures could impact business operations and end users

- Security vulnerabilities – New environments often require updated security settings. If overlooked, the migration could expose the application to new risks
- Rollback challenges – If the upgrade or migration fails, rolling back may be difficult, especially if critical data has already been transferred or modified

While there are no guarantees that any or all the above issues will arise, the criticality of apps such as Maximo or our billing system means there will be a significant impact on business operations if problems do occur. There is also the issue that upgrading during the AGN transition may mean the transition takes longer or requires two instances of the same application in two different environments. This is less of a problem with applications such as Workday, which are provided as software as a service and subject to vendor-delivered upgrades on an automated basis. However, our enterprise asset management and metering & billing systems carry significantly more risk. A safer approach is to upgrade the app in the existing environment first or migrate it as-is before upgrading, reducing the number of variables involved.

1.5.1.2 Cost assessment

The estimated capital expenditure for Option 1 is around \$18.1 million (see Table 0.4). This estimate assumes application upgrades can be delivered as per the periodic upgrade schedule and will not be materially impacted by the transition.

Table 0.4: IT operational apps capex program 2026-31, \$'000 January 2025 – Option 1

Option 1 – Operational apps capex	2026/27	Transition		2029/30	2030/31	Total
		2027/28	2028/29			
Enterprise asset management	176	440	2,114	176	176	3,083
FRC gateway	35	35	264	264	264	863
GIS	-	529	529	-	176	1,233
Metering & billing	35	687	687	-	1,374	2,784
Workday	35	35	35	-	-	107
Middleware	881	-	-	-	-	889
Mobility apps	747	747	747	747	747	3,735
Business intelligence	218	218	218	218	218	1,092
Call centre telephony	-	35	-	-	-	35
Historian update	-	407	-	-	1,221	1,628
Automation software	25	-	25	-	25	75
Higher heating zone	300	300	300	300	300	1,500
MDM	1,105	-	-	-	-	-
Total capex	3,558	3,434	4,920	1,706	4,503	18,121

The operational apps program also includes an uplift in recurrent opex for ongoing data and storage costs (Meter Data Management) associated with digital metering data. As we roll out digital metering across the network, our metering & billing system needs to be able to collect, validate and store data from digital gas meters. There will be a \$1.1 million capital investment during 2026/27 to install additional functionality for meter data management and for our metering & billing system (Oracle CC&B) to utilise the information it needs for customer billing.

Once the digital metering functionality has been added, there will be an ongoing operating cost for data and support. Costs are based on the number of customers with digital meters and data volume and are therefore expected to increase year on year as the volume of installed digital meters increases (see Table 0.5).

Table 0.5: IT operational apps opex 2026-31, \$'000 January 2025 – Option 1

Option 1 – Opex	Transition					Total
	2026/27	2027/28	2028/29	2029/30	2030/31	
Digital metering data and cloud costs	22	79	136	177	192	606

Cost estimates are based on current market rate testing, considering the requirements of our application environment, using the best information available at the time of developing this business case.

1.5.1.3 Risk assessment

This option does not address the risk sufficiently. Upgrading applications while conducting the AGN transition would, in theory, reduce the likelihood of critical apps failing. However, this would only happen if the upgrades and transition went smoothly, with minimal issues. As discussed in section 1.5.1.1, simultaneously upgrading and migrating apps to another environment is fraught with risk. Given the scale of the AGN transition and the resourcing effort required to deliver it, we consider the potential for a critical app upgrade to experience complications during the transition is high. At the very least, we expect the simultaneous upgrade and migration would elongate and complicate the AGN Transition, leading to higher costs.

We therefore do not consider Option 1 would reduce the current risk rating any lower than high.

Table 0.6: Risk rating - Option 1

Option 1	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

1.5.1.4 Achievement of objectives

Table 0.7 outlines how Option 1 will support achievement of our vision objectives.

Table 0.7: Achieving objectives – Option 1

Vision objective	Alignment
Customer Focussed - Public Safety	-
Customer Focussed – Customer Experience	N
Customer Focussed – Cost Efficient	N
A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	N
A Leading Employer – Skills Development	-

Operational Excellence – Profitable Growth	-
Operational Excellence – Benchmark Performance	-
Operational Excellence – Reliability	-
Sustainable Communities – Enabling Net Zero	Y
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

Option 1 would not align with our strategic pillars of being *Customer Focussed* and or *A Leading Employer*, as the potential for outages to critical apps would remain high. This would disrupt service to customers (e.g. billing, meter reading, data transfer) while also causing significant disruption to our employees' ability to do their jobs.

Option 1 would also not be cost efficient. Simultaneous upgrade and transition may result in two instances of the same app being required, as well as carrying the potential for elongating the AGN transition. Either outcome would not represent efficient expenditure.

1.5.2 Option 2 – Pause the upgrade cycle for critical apps during the transition window

Under this option we would postpone major upgrade of critical applications such as Maximo, webMethods, and Oracle CC&B until after the AGN transition, picking up the upgrade cycle thereafter. Non-critical apps or applications that are relatively simple to upgrade and have a low risk of being impacted by (or impacting) the transition, such as Workday, mobility applications, and business intelligence software, will continue on their usual upgrade cycle.

Maximo, Oracle CC&B, and the webMethods will continue to operate in their current versions. These current versions fall out of vendor support during the first two years of the regulatory period. To mitigate the risk of outages while these apps remain in their current state, we will need to pay for extended support (see Table 0.8).

Table 0.8: Extended support for critical apps

Application	Current version	Current support agreement	Extended support available?	Extended support cost
Maximo	7.6.1.3	Ends Sep-2025	Y	~\$500,000 per year
Oracle CC&B	2.9	Ends Apr-2027	Y	~\$100,000 per year
FRC Gateway (Webmethods)	10.7	Ends Apr-2025	Y	~\$100,000 per year
GE Smallworld	5.3	Ends Jun-2027	N	n/a

GE Smallworld, our GIS application, is another critical application that we need to ensure is in a steady state during transition. Unfortunately, the vendor of our GIS application does not offer an extended support option for the current version. This means that if the current version of the GIS app fails, experiences data loss, or cyber-attack, the software is at risk of extended outage, leaving us with limited ability to map, trace and schedule works on our network.

To mitigate this risk, we will prioritise the GIS upgrade for 2026/27, ensuring it is completed prior to the AGN Transition. Bringing forward the GIS upgrade can be delivered with the current level of resourcing.

1.5.2.1 Advantages and disadvantages

The advantage of this approach is that it minimises the risk of the application upgrade being impacted by the transition. By postponing the upgrade, we can be certain our critical apps remain functional and reduce the likelihood of operational impacts. Pausing the upgrade cycle also eliminates the risk of the application upgrades impacting the AGN transition process.

The disadvantage of this approach is the cost of extended support. Running unsupported apps is not ideal, and while having an old version of an does not automatically mean we will experience problems, it does mean we would pay a premium for support if and when problems do occur. In ordinary circumstances we would maintain our n-1 approach and upgrade apps to ensure they remain within standard support agreements, but the AGN transition inhibits this approach. We will, however, seek to upgrade to the newest version of each application as soon as practicable once the AGN transition is complete. In the event the AGN transition takes longer than anticipated, we will review our extended support costs, risk and current transition status, and may seek to bring forward upgrades on a case-by-case basis where safe and prudent to do so.

1.5.2.2 Cost assessment

The estimated capital expenditure for Option 2 is around \$18.8 million (see Table 0.9). This estimate assumes no upgrades to critical applications occurs during the transition window (2027/28 and the first half of 2028/29).

Table 0.9: IT operational apps capex program 2026-31, \$'000 January 2025 – Option 2

Option 2 – Operational apps capex	2026/27	Transition		2029/30	2030/31	Total
		2027/28	2028/29			
Enterprise asset management	-	-	440	2,114	352	2,907
FRC gateway	-	-	264	264	264	793
GIS	1,057	-	-	-	1,057	2,114
Metering & billing	35	-	687	687	1,374	2,784
Workday	35	35	35	-	-	107
Middleware	881	-	-	-	-	889
Mobility apps	747	747	747	747	747	3,735
Business intelligence	218	218	218	218	218	1,092
Call centre telephony	-	35	-	-	-	35
Historian update	-	407	-	-	1,221	1,628
Automation software	25	-	25	-	25	75
Higher heating zone	300	300	300	300	300	1,500
MDM	1,105	-	-	-	-	1,105
Total capex	4,404	1,743	2,717	4,331	5,560	18,755

Costs in 28/29 are assumed to be incurred during the second half of the year, post AGN Transition

This option would also include operating expenditure (opex) for extended support until the applications can be upgraded post-transition. The forecast opex is shown in the following table.

Table 0.10: IT operational apps opex 2026-31, \$'000 January 2025 – Option 2

Option 2 – Opex	Transition		2028/29	2029/30	2030/31	Total
	2026/27	2027/28				
Digital metering data and cloud costs	22	79	136	177	192	606
Extended support for critical apps						
Enterprise asset management	176	176	176	88	-	617
FRC gateway	35	35	35	-	-	106
Metering & billing	35	35	35	18	-	123
Total opex	269	326	383	300	192	1,469

Cost estimates are based on current market rate testing, considering the requirements of our application environment, using the best information available at the time of developing this business case.

1.5.2.3 Risk assessment

This option has the greatest risk reduction of the three options presented, reducing the risk to a moderate rating. By postponing the upgrade of critical applications we are eliminating the risk that the application upgrade will be impacted by the transition or will cause the transition itself to be extended. However, as we will be operating older versions of the applications, we are more exposed to cyber security breaches and/or data loss, as the applications will not have the latest security patches and functionality. We therefore consider the risk of the applications experiencing an outage and affecting operations remains a moderate risk, and that this risk is as low as reasonably practicable in the circumstances.

Table 0.11: Risk rating - Option 2

Option 2	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Negligible	Low	

1.5.2.4 Achieving objectives

The following table outlines how Option 2 will support achievement of our vision objectives.

Table 0.12: Achieving objectives – Option 2

Vision objective	Alignment
Customer Focussed - Public Safety	-
Customer Focussed – Customer Experience	Y
Customer Focussed – Cost Efficient	Y
A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	Y
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	-

Vision objective	Alignment
Operational Excellence – Benchmark Performance	-
Operational Excellence – Reliability	-
Sustainable Communities – Enabling Net Zero	Y
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

Option 2 would align in our strategic pillars of being *Customer Focussed and A Leading Employer*, as it would ensure our critical applications (such as our billing system) remain functional, and our staff continue to have the tools to do their jobs.

While incurring costs for extended support is not ideal, it is a critical cost to manage risk and is a more efficient use of expenditure than potentially running two instances of the same app (Option 1).

1.5.3 Option 3 – Uplift resources and bring forward upgrade of core applications before the transition

Under this option we would ramp up resources to deliver the upgrades to Maximo, webMethods, and Oracle CC&B prior to the transition. As per our application management strategy, we would upgrade to the n-1 version, which will be fully supported by the vendor.

1.5.3.1 Advantages and disadvantages

The advantage of this option is that all critical applications would be stable and fully supported before, during and after the AGN Transition. Assuming the upgrades can be completed on time, this option would not impact on the AGN transition and would avoid the need for extended support.

However, Option 3 is a risky strategy. It is imperative that the Maximo, webMethods and Oracle CC&B upgrades are completed before the transition commences on 1 July 2027. This gives us a small window of time to implement and test the upgrades. If the upgrades are delayed, it will have flow-on effects for the transition, extending delivery timeframes and leading to transition costs beyond the ~\$300 million already estimated.

To avoid delays, we would need to ramp up our resources to deliver the upgrades on time. This means the capital cost of Option 3 would be higher than Options 1 or 2. While a resourcing uplift is feasible, there are no guarantees it can be achieved. Skilled IT resources are in high demand and difficult to secure in the Australian market. It may be particularly challenging to secure IT resources if we are only offering a short-term contract that runs until the transition commences. Our current IT resource pool will be focused on the transition and will not have the capacity to deliver the upgrades too. Option 3 therefore carries a significant delivery risk.

1.5.3.2 Cost assessment

The estimated capital expenditure for Option 3 is around \$20.5 million (see Table 0.13). This assumes the upgrades to Maximo, webMethods, and Oracle CC&B can be delivered in full prior

to the AGN transition and will therefore be migrated to the AGIG environment in a fully supported and up-to-date (n-1) version.

Table 0.13: IT operational apps capex program 2026-31, \$'000 January 2025 – Option 3

Option 3 – Operational apps capex	2026/27	Transition		2029/30	2030/31	Total
		2027/28	2028/29			
Enterprise asset management	3,070	-	176	352	352	3,951
FRC gateway	116	-	264	264	264	909
GIS	1,057	-	-	-	1,057	2,114
Metering & billing	1,946	-	-	-	1,374	2,784
Workday	35	35	35	-	-	107
Middleware	881	-	-	-	-	889
Mobility apps	747	747	747	747	747	3,735
Business intelligence	218	218	218	218	218	1,092
Call centre telephony	-	35	-	-	-	35
Historian update	-	407	-	-	1,221	1,628
Automation software	25	-	25	-	25	75
Higher heating zone	300	300	300	300	300	1,500
MDM	1,105	-	-	-	-	-
Total capex	9,500	1,743	1,766	1,882	5,560	20,451

This option would also include recurrent operating expenditure (opex) for digital metering data costs.

Table 0.14: IT operational apps extended support opex 2026-31, \$'000 January 2025 – Option 3

Option 3 – Opex	2026/27	Transition		2029/30	2030/31	Total
		2027/28	2028/29			
Digital metering data and cloud costs	22	79	136	177	192	606

Cost estimates are based on current market rate testing, considering the requirements of our application environment, using the best information available at the time of developing this business case.

1.5.3.3 Risk assessment

This option does not address the risk sufficiently. Upgrading the critical apps prior to transition could offer the greatest risk reduction in terms of preventing app outages and avoiding extended support costs. However, this would depend on the upgrades being delivered on time and in full. Given resource scarcity, the complexity of the upgrades, and the tight timeframes, the risk of the upgrade work taking longer than expended is high. This will elongate and complicate the AGN Transition, leading to higher costs.

We therefore do not consider Option 3 would reduce the current risk any lower than high.

Table 0.15: Risk rating - Option 3

Option 3	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

1.5.3.4 Achieving objectives

The following table outlines how Option 3 will support achievement of our vision objectives.

Table 0.16: Achieving objectives – Option 3

Vision objective	Alignment
Customer Focussed - Public Safety	-
Customer Focussed – Customer Experience	Y
Customer Focussed – Cost Efficient	Y
A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	Y
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	-
Operational Excellence – Benchmark Performance	-
Operational Excellence – Reliability	-
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

Option 3 would align with our strategic pillars of being *Customer Focussed* and *A Leading Employer*, as it would ensure our critical applications (such as our billing system) remain functional, and our staff continue to have the tools to do their jobs. The additional cost of bringing in additional resources is necessary to manage risk and is a more efficient use of expenditure than potentially running two instances of the same app (Option 1).

1.6 Summary of options assessment

Table 0.17 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 0.17: Comparison of options

Option	Objectives	Capex	Opex	Risks
1. Deliver operational app upgrade cycle in a parallel with the AGN Transition.	Does not align with being Customer Focussed or being A Leading Employer	\$18.1 million	\$0.6 million	This option mitigates some risk, but presents a significant risk to the AGN transition and therefore the overall risk rating remains high.
2. Pause the upgrade cycle for critical apps during	This option achieves our objectives of being	\$18.8 million	\$1.5 million	This option moderates all high and intermediate risks to ALARP.

the transition window	Customer Focussed and being A Leading Employer			
3. Uplift resources and bring forward upgrade of core applications before the transition	This option achieves our objectives of being Customer Focussed and being A Leading Employer	\$20.5 million	\$0.6 million	This option mitigates some risk, but presents a significant risk to the AGN transition and therefore the overall risk rating remains high.

1.7 Proposed solution

Our proposed solution is Option 2, pausing the upgrade cycle for our critical applications until after the transition.

1.7.1 Why is the recommended option prudent?

The operational apps covered in this business case need to be upgraded, and the AGN transition is taking place. These are constants in all options and there is no consideration that either will not occur. The key question is therefore when to conduct the upgrades: before, during, or after the transition. On this basis, we consider Option 2 represents the most prudent approach as it provides the best balance between cost and risk.

Based on the information available today, the difference in cost between the three options is relatively small, the variance being the additional opex required to pay for extended support or the additional capex for the additional resources required to accelerate the upgrades. If the approach under all three options went perfectly, Option 1 or potentially even Option 3 would represent a more efficient process, as it would avoid need for extended support. However, the risk of Option 1 or Option 3 experiencing complications is greater than the risk in Option 2.

Option 2 is a conservative approach, which ensures the critical applications will be fully functional and supported throughout the transition. Customer service and business continuity are among AGIG's highest priorities; therefore it is imperative our billing system, GIS, asset management software and FRC Gateway are functional at all times.

Option 1 carries a high risk that application upgrades are complicated by the transition and increases the potential for critical apps to be offline. Option 3, while mitigating the risk of app outages, poses a high delivery risk and has a high potential of encroaching into the AGN transition period. Neither outcome is tolerable for AGIG or our customers.

Option 2 has the advantages of completely separating the upgrade cycle from the AGN transition work, eliminating the risk of one activity complicating the other. Of course, this means we will carry some risk associated with running outdated apps, and there is also an underlying risk that other factors cause the AGN transition to take longer than expected. However, Option 2 allows sufficient control and flexibility to be able to manage these risks, should they occur.

1.7.1.1 Governance & implementation of IT initiatives

The implementation of IT initiatives outlined in this business case will be governed by AGIG's established two-tier framework, which ensures appropriate oversight and decision-making

based on the scope and impact of each undertaking. This framework encompasses both larger, more complex projects and smaller, incremental improvements.

Larger initiatives, typically involving significant capital expenditure, strategic impact, or cross-functional dependencies, will be managed as formal projects following our project management methodology. The specific requirements of this methodology, including governance, risk management, and reporting, will be tailored to the individual project's characteristics, such as risk, complexity, and cost. Where these projects involve system acquisition or outsourced services, all procurement activities will adhere to our Procurement Policy and Purchasing Procedure to ensure optimal value and efficient outcomes. Detailed business requirements will be defined closer to the implementation timeframe, considering current market capabilities and specific business needs. Furthermore, the project management processes will incorporate appropriate and comprehensive organisational change management plans aligned with the final solution and implementation approach.

Smaller, more tactical improvements will follow a streamlined, agile delivery cycle. This process ensures quicker turnaround for lower-risk, high-value non-recurrent improvements.

Regardless of the initiative's size, the following principles will apply:

- An internal business case and justification, commensurate with the initiative's, cost, risk and complexity, will be developed
- Management will review and approve the business case based on the organisation's overarching priorities, risks and benefits
- IT Management will oversee the delivery of the initiative and any associated organisational change management according to the agreed timelines and outcomes
- Business user involvement will be strategically managed to maximise their input whilst minimising disruption to their operational activities
- Organisational change management strategies will be designed to mitigate the risks associated with the change, proportionate to the initiative's benefits and organisational priorities

1.7.2 Estimating the efficient costs

The cost estimates for the IT operational applications program are based on a combination of internal and external resourcing (particularly for specialised expertise or to manage workloads), software licenses, and potential hardware, as applicable. Unit rates for internal IT and business resources are based on an established internal rate card.

Recurrent upgrade activities draw upon a mix of internal IT, business resources and external resourcing for project management, technical implementation, business requirements gathering, testing, and training. Our cost estimates for recurrent upgrades are based on historical costs where available for similar projects, such as previous upgrades for the same application.

Where specialised skills or additional capacity is required, internal teams may be supplemented by outsourced IT support resources. The rates for outsourced IT support are governed by agreed contract rate cards. Our cost estimates are informed leveraging the historical costs of delivering improvements based on business requests.

For larger and more complex non-recurrent projects, including new implementations and significant upgrades, our cost estimates include indicative pricing and implementation costs obtained from vendors and our service partners, supplemented with the increasing capabilities of our internal teams, and business resources as required.

All procurement processes for IT applications will comply with our Procurement Policy and Purchasing Procedure and will follow transparent, competitive tendering processes to select the best value for money solution.

Overall, there does not appear to be many factors affecting the sensitivity of these estimations, however a small amount is costed in USD and therefore susceptible to foreign exchange fluctuations.

1.7.3 Consistency with the National Gas Rules

NGR 79(1) and NGR 91

The proposed expenditure on our IT operational applications is consistent with Rule 79(1)(a), specifically we consider the capital expenditure is:

- **Prudent** – The expenditure is necessary in order to address the identified risks associated with migrating critical applications to a new environment. Most importantly, the proposed approach mitigates the risk of operational app upgrades impacting the AGN transition and elongated what is already an extremely intensive and complex exercise. Our operational apps will remain functional throughout the transition and therefore the proposed expenditure can therefore be seen to be of a nature that would be incurred by a prudent service provider
- **Efficient** – The forecast expenditure is based on historical costs for similar work as well as estimates from vendors. Actual upgrade costs will be reassessed post the AGN transition and we will seek to amend upgrade applications to the most appropriate version at the time, in keeping with our n-1 principles.
- **Consistent with accepted and good industry practice** – The proposed initiatives will ensure that IT applications are maintained to industry standard version levels consistent with accepted and good industry practice. This will result in all critical systems being up to date, secure and supported by vendors, consistent with good industry practice
- **Achieves the lowest sustainable cost of delivering pipeline services** – Upgrading our AGN SA IT systems is the lowest sustainable cost for suitable long-term mitigation of the risks discussed. The alternative options carry significantly higher risk, and if any of the risks do arise, will likely be a higher cost than Option 2. The chosen option is therefore consistent with the objective of achieving the highest quality and lowest sustainable cost of service delivery.

NGR 79(2)(c)

The proposed expenditure on our IT sustaining applications project is required to maintain the integrity of services through current, supported and fit for purpose IT applications, managing technology risks and preventing material outages that impact the ability of the business to function (including tracking and reporting of business information to meet our regulatory

obligations and requirements). This expenditure is therefore consistent with NGR 79(2)(c)(ii) and (iii).

NGR 74

The forecast costs in this business case are based on the latest market rate testing, and project options consider the asset management requirements as per the IT Investment Plan. Cost assessments have been conducted for each option based on the best information available at the time of developing this business case. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.

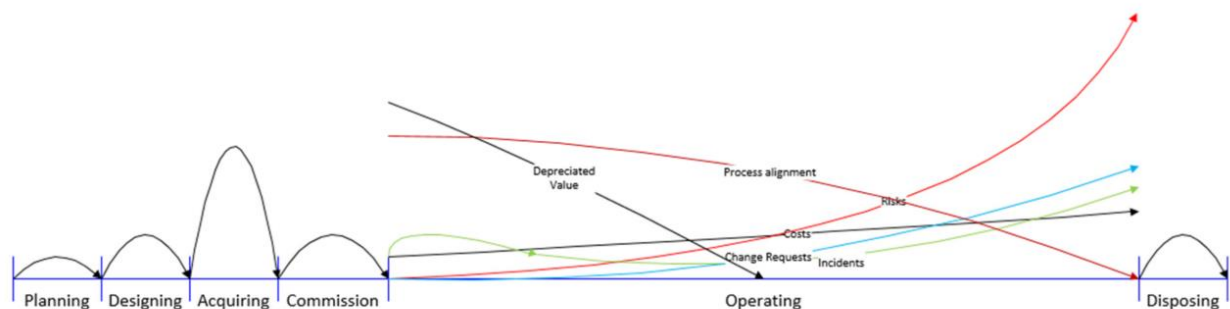
Appendix A Overview of IT operational apps activities

Like physical infrastructure assets, such as pipeline assets, IT applications operate within a lifecycle that necessitates ongoing maintenance to ensure their continued effectiveness and alignment with business needs. However, the IT landscape presents unique challenges due to the rapid pace of technological change and the intricate interdependencies between systems. As user interfaces, network infrastructure, and other IT applications evolve, older applications can experience a degradation of functionality simply due to incompatibility with the broader IT environment.

Furthermore, even the most meticulously planned and implemented IT applications may not fully address all business process requirements from their initial deployment. This gap often widens over time as business needs themselves evolve, leading to either inefficient manual workarounds or the need for modifications and upgrades to the IT applications.

The interconnected nature of these application lifecycle factors is depicted in Figure A.1 below. This model underpins our approach to determine the optimal lifespan of an application, evaluating the cost vs benefits of its continued operation, and identifying the key factors for a strategic replacement to ensure AGN's operations are supported by modern, efficient, and reliable IT applications.

Figure Appendix A.1: IT Application lifecycle concepts



The following sections describe the proposed application upgrades for the period.

A.1.1 Maximo

Maximo is our enterprise asset management solution, used to manage gas network operations. Maximo is integral to the safe and efficient operation of the AGN SA network. We use the application for:

- Asset tracking and maintenance – monitoring the condition of pipeline assets, ensuring timely maintenance and reducing downtime
- Predictive analytics – by integrating sensors and AI driven insights (for example via UiPath), we can predict potential failures and schedule proactive repairs
- Regulatory compliance – tracking inspections, incidents and compliance reports
- Workforce management – streamlining work orders, managing field crews and optimising resource allocation

- Geospatial integrations – integrating GIS technology to map and analyse the network, enhancing asset visualisation.

We currently run version 7.6.1.3 of Maximo, which is almost three years old and falls out of vendor support on 30 September 2025. After this date, IBM will no longer provide fixes, patches and support for the Maximo 7.6.1.3 release, including base Maximo and its add-on products.

While Maximo 7.6.1.3 will continue to function after September 2025, if functional issues are experienced, IBM will be unable to provide fixes unless we enter into an extended support agreement for up to five years. Other potential consequences of staying on a version of Maximo beyond its support date include:

- Security vulnerabilities – without regular security updates, Maximo can become susceptible to cyber threats, putting sensitive data and critical infrastructure at risk.
- Audit and reporting challenges – organisations must maintain up-to-date software with verifiable security measures. Running an unsupported version may lead to non-compliance with industry-specific standards such as ISO 55000, OSHA, FDA regulations, and NERC CIP.
- Reduced application reliability – as software ages without vendor support, issues may arise that impact system performance, potentially leading to operational inefficiencies and downtime.
- Integration limitations – Maximo 7.6 may face compatibility issues with AI software and other more sophisticated apps.

To avoid these issues we plan to upgrade to Maximo version MAS 9 or later. This is a major upgrade. It is unlikely we would be able to complete this upgrade prior to the start of the AGN transition on 1 July 2027, therefore our plan is to deliver the Maximo upgrade in 2028/29 and pay for extended support from September 2025 until the upgrade is done.

A.1.1.1 Maximo upgrade costs

Maximo is an enterprise-wide application, with the costs allocated between AGN SA, AGN Victoria and AGN Queensland based on customer numbers. The total cost estimate is \$10 million (capex + opex), of which AGN SA's proportion is 35.2%.

Capex includes the review of release changes, activating new features as required by the business, thoroughly testing the changes prior to release, change management, training, and coordination within IT to ensure compatibility with other systems.

Opex is the cost of extended support (~\$500,000 per year).

A.1.2 FRC Gateway (webMethods)

The AEMO FRC Gateway is part of the Full Retail Contestability (FRC) Hub, which facilitates electronic transactions between gas market participants in Australia. It enables gas retailers, distributors, and other stakeholders to exchange business-critical information securely and efficiently.

We use the FRC Gateway for:

- Customer transfers – processing customer switch requests between retailers.
- Meter data exchange – send meter readings and consumption data to retailers for accurate billing.
- Market transactions – business-to-business transactions, including service requests, disconnections, and reconnections.
- Regulatory compliance – ensures that all market participants adhere to AEMO's gas retail market procedures.
- Secure communication – using aseXML (a structured XML format) within ebXML message envelopes to transmit data over secure HTTP/S protocols.

AEMO's FRC Hub is updated periodically to accommodate system upgrades, industry changes and participant needs. The FRC Hub primarily relies on Software AG's webMethods platform. Most changes are driven by AEMO as per its FRC Hub Participant User Guide.

We are currently running version 10.7 of webMethods, which recently fell out of support. To maintain currency, we either need to upgrade the software to the latest version, and/or pay for extended support in the interim.

The FRC Gateway is a critical application, and it is imperative the software is in a steady state when it is transitioned to AGIG's IT environment and remains functional throughout the transition. To avoid the risk of an outage, our preferred approach is to maintain the current version of webMethods until the AGN transition is complete.

A.1.2.1 webMethods upgrade costs

webMethods is an enterprise-wide application, with the costs allocated between AGN SA, AGN Victoria and AGN Queensland based on customer numbers. The total cost estimate is \$2.6 million (capex + opex), of which AGN SA's proportion is 35.2%.

Capex includes the review of release changes, activating new features as required by the business, thoroughly testing the changes prior to release, change management, training, and coordination within IT to ensure compatibility with other systems.

Opex is the cost of extended support (~\$100,000 per year).

A.1.3 GIS (GE Smallworld)

GE Smallworld is a GIS system used to manage our networks. It provides a detailed digital representation of our gas infrastructure and is used for network inventory, planning, outage management and operational support. The current version of GE Smallworld is due for an upgrade and falls out of support in June 2027.

Upgrading GE Smallworld to a newer version is complex, due to the level of customisation and integration with our other applications. The GIS solution is integral to the way we operate the network therefore it is essential we ensure migration to the AGIG IT environment runs smoothly and the application remains functional throughout.

Unfortunately, GE does not offer extended support beyond June 2027, therefore we need to complete the upgrade as soon as possible, prior to the transition.

A.1.3.1 GIS upgrades costs

GE Smallworld is an enterprise-wide application, with the costs allocated between AGN SA, AGN Victoria and AGN Queensland based on customer numbers. The total cost estimate is \$6 million (capex), of which AGN SA's proportion is 35.2%.

Capex includes the review of release changes, activating new features as required by the business, thoroughly testing the changes prior to release, change management, training, and coordination within IT to ensure compatibility with other systems.

A.1.4 Metering & billing system (Oracle CC&B)

Oracle Utilities Customer Care and Billing (CC&B) is a customer information system designed for utility companies, including gas network businesses. It helps manage customer accounts, billing, service requests, and meter data efficiently. We use Oracle CC&B for:

- Billing and revenue management – issuing usage-based billing to retailers and demand customers.
- Meter data management – tracking gas consumption and issuing data to retailers for billing accuracy.
- Regulatory compliance – adherence to government regulations and industry standards for gas distribution and billing.

We currently use Oracle CC&B version 2.9, which falls out of support in April 2027. Extended support is available after this time.

The metering & billing system is integral to our operations. We cannot meet our meter data provision or billion obligations without it. The solution has a high number of integrations with other systems and very high transaction volumes. This makes upgrade and the migration to another IT environment complex and high risk. It is therefore imperative Oracle CC&B is in a steady state during the AGN Transition.

A.1.4.1 Oracle CC&B upgrade costs

Oracle CC&B is an enterprise-wide application, with the costs allocated between AGN SA, AGN Victoria and AGN Queensland based on customer numbers. The total cost estimate is \$8.25 million (capex + opex), of which AGN SA's proportion is 35.2%.

Capex includes the review of release changes, activating new features as required by the business, thoroughly testing the changes prior to release, change management, training, and coordination within IT to ensure compatibility with other systems.

Opex is the cost of extended support (~\$100,000 per year).

A.1.5 Workday

Workday is a cloud-based enterprise software platform that provides financial management, payroll, procurement and resource planning functionality. At APA it is used for budgeting, expense tracking, resource management and reporting when operating the AGN networks.

Workday upgrades are issued twice a year through automatic cloud updates, meaning we don't need to manually install new versions. These regular updates include new features, security enhancements, and bug fixes, ensuring Workday remains up to date.

As a result, the Workday upgrades carry a low risk of impacting the AGN transition and can therefore continue as per the usual schedule during the migration to the AGIG IT environment.

A.1.5.1 Workday upgrades cost assessment

Workday is an enterprise-wide application, with the costs allocated between AGN SA, AGN Victoria and AGN Queensland based on customer numbers. The total cost estimate is \$0.3 million (capex), of which AGN SA's proportion is 35.2%.

A.1.6 Middleware

Middleware is software that acts as a bridge between different applications, systems, or services, enabling them to communicate and work together efficiently. It sits between the operating system and applications, handling tasks like data exchange, authentication, and integration.

The middleware that supports the AGN SA operational apps is due for upgrade in 2026/27. It is essential this middleware is updated as soon as practicable to ensure our suite of apps maintain current performance and are protected from security vulnerabilities and compatibility issue before, during and after the AGN Transition. The proposed upgrade is a relatively straightforward one-off project, which will replace BizTalk with Azure Integration Services. We therefore consider the middleware upgrade can be delivered in full prior to the AGN Transition.

A.1.6.1 Middleware upgrades cost assessment

Our middleware solution is used enterprise-wide, with the costs allocated between AGN SA, AGN Victoria and AGN Queensland based on customer numbers. The total cost estimate of the upgrade is \$2.5 million (capex), of which AGN SA's proportion is 35.2%.

A.1.7 Mobility applications

We use the mobility functionality in Salesforce Lightning to help manage AGN network operations. It is used by field service teams for real time scheduling, data access, dispatching and remote access to asset management systems.

Salesforce Lightning updates are managed through automatic upgrades that occur three times a year. These updates include new features, enhancements, and security improvements, ensuring the application is up to date, stable, and supported, without the need for manual intervention. As a result, the updates are low risk and can be delivered in parallel with the AGN transition with minimal disruption.

A.1.7.1 Mobility upgrades cost assessment

Salesforce Lightning is an enterprise-wide application, with the costs allocated between AGN SA, AGN Victoria and AGN Queensland based on customer numbers. The total cost estimate is \$10.6 million (capex), of which AGN SA's proportion is 35.2%.

Capex includes the review of release changes, activating new features as required by the business, thoroughly testing the changes prior to release, change management, training, and coordination within IT to ensure compatibility with other systems.

A.1.8 Business intelligence

We use Microsoft's Power BI as our business intelligence software for AGN. It is used when operating the AGN SA network for:

- Real-time monitoring – Visualising gas flow, pressure, and pipeline performance
- Asset management – Tracking maintenance schedules and optimising infrastructure investments
- Regulatory reporting – Automating compliance reports for industry standards
- Operational Efficiency – Analysing historical data to improve network reliability

Power BI is provided as software as a service. Updates are automated and require little manual intervention. As a result, the Power BI upgrades carry a low risk of impacting the AGN transition and can therefore continue as per the usual schedule during the migration to the AGIG IT environment.

A.1.8.1 Power BI upgrade costs

Power BI is an enterprise-wide application, with the costs allocated between AGN SA, AGN Victoria and AGN Queensland based on customer numbers. The total cost estimate is \$3.1 million (capex), of which AGN SA's proportion is 35.2%.

A.1.9 Call centre telephony

NICE CXOne is a vital component of our call centre telephony software. NICE CXOne is a cloud-based platform that provides automation, analytics and multi-channel communication. It is used in our call centre operations to help streamline operations, scheduling and track service performance.

A minor update is required in 2027/28 to maintain version currency and install the latest patches. Updates are issued remotely via a cloud-based platform. As a result, the 2027/28 update is low risk and can be delivered in parallel with the AGN transition with minimal disruption.

A.1.9.1 NICE CXOne cost assessment

NICE CXOne is an enterprise-wide application, with the costs allocated between AGN SA, AGN Victoria and AGN Queensland based on customer numbers. The total cost estimate \$0.1 million (capex), of which AGN SA's proportion is 35.2%.

Capex includes the review of release changes, activating new features as required by the business, thoroughly testing the changes prior to release, change management, training, and coordination within IT to ensure compatibility with other systems.

A.1.10 Historian

Historian software is a specialised data management system designed to collect, store, and analyse time-series data from industrial processes, sensors, and control systems. We use

OSISoft PI as historian software for storing historical operational data for the AGN SA and AGN Queensland networks.

The historian software is due for upgrade in 2027/28, however, this coincides with the AGN Transition. Historian is not a business-critical application. While we would need to update the application once operational activities have been moved from APA to AGIG, we can operate on the current version during the transition. All versions of historian are supported by the vendor. We will therefore postpone the historian upgrade until after the transition, at minimal risk.

A.1.10.1 Historian upgrade cost

Historian costs are allocated between AGN SA, and AGN Queensland only, based on customer numbers. A different historian solution is in place for the AGN Victorian network. The total cost estimate is \$2 million (capex), of which AGN SA's proportion is 81.4%.

A.1.11 UiPath

UiPath is a robotic process automation platform that allows businesses to automate repetitive tasks using AI-powered software. It is used to track pipeline maintenance and inspections, reduce manual data entry and improve workflow automation.

UiPath is relatively low cost and simple to update. The level of customisation and integrations with other operational systems is very low, which means the transition to the AGIG IT environment should be low risk. We therefore propose UiPath upgrades continue as per the scheduled business-as-usual upgrade program.

A.1.11.1 UiPath upgrade cost

UiPath is used by AGN SA only. The total cost estimate of the upgrade is \$75,000 (capex), 100% allocated to AGN SA.

A.1.12 Higher heating zones

We need to add functionality to our historian software so that it can record different higher heating values in different parts of the network. This change will allow more accurate billing and will ensure our back-end systems can accommodate blends of renewable gas entering the network. The proposed investment is relatively straightforward and low complexity, therefore this change can be delivered along with the historian upgrade (section A.1.10) and the AGN transition at minimal risk.

A.1.12.1 Higher heating zones costs

The update in higher heating value data is for AGN SA only. The total cost estimate is \$1.5 million (capex), 100% allocated to AGN SA.

A.1.13 MDM

As we roll out digital meters across the network, we need to ensure our meter data management system can accommodate the data. Oracle and similar systems offer meter data management functionality that allows consumption data to be synchronised with billing processes. It helps automate billing, detect anomalies in gas usage, and provides customers with accurate consumption insights.

There will be an initial capital investment to add the MDM functionality for AGN SA, and an uplift in recurrent opex as the digital data volumes increase. The functionality enhancement is low risk and should be completed before the AGN Transition.

A.1.13.1 MDM

The upgrade to MDM to accommodate digital meter data is for AGN SA only. The total cost estimate is \$1.71 million (capex + opex), 100% allocated to AGN SA.

Appendix B Comparison of risk assessments

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

Option 1	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

Option 2	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Negligible	Low	

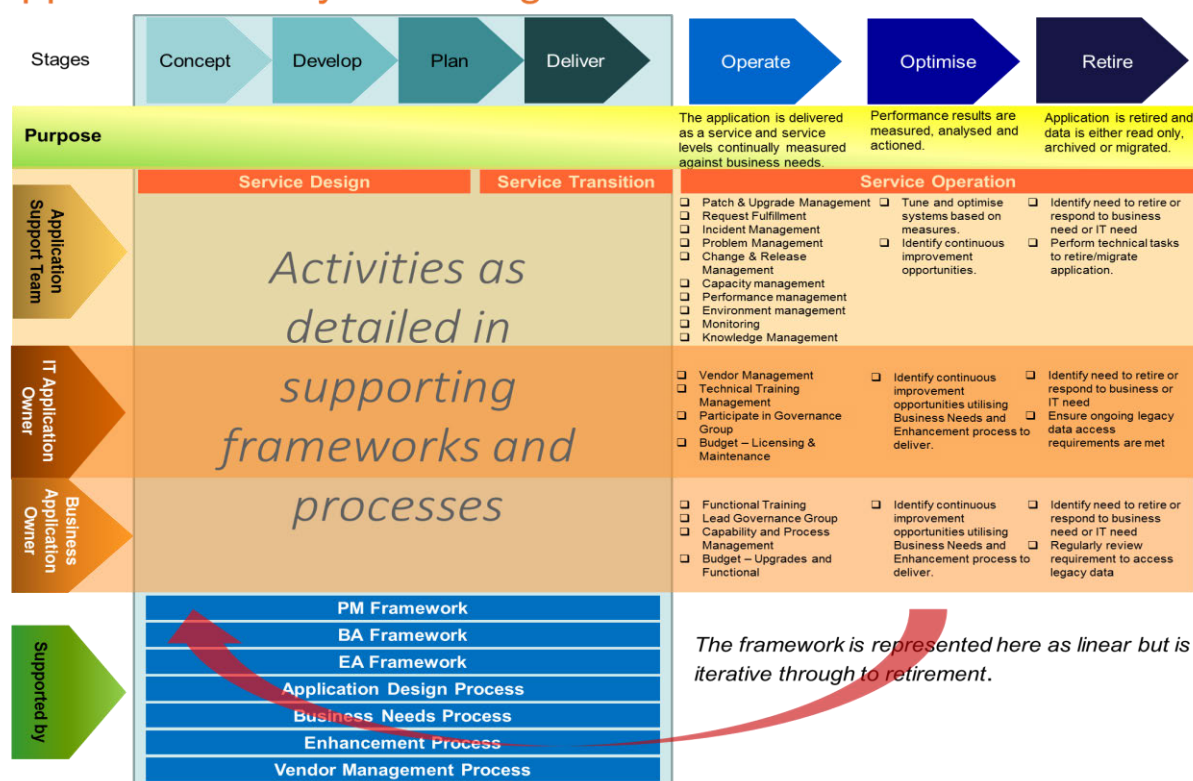
Option 3	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

Appendix C Application lifecycle management

We follow an industry standard application lifecycle framework to manage applications through the implementation, operations, optimisation and retirement phases of their lifecycle to determine upgrade timelines and priorities. This framework provides an efficient and effective approach to maintaining the security and stability of our applications while optimising lifecycle stages. This framework includes the project management methodologies to implement the applications, and ongoing lifecycle activities to operate and optimise the applications - including upgrade cycles.

The diagram below outlines the key aspects of this framework.

Application Lifecycle Management Framework



SA238 – IT corporate applications

1.1 Project approvals

Table 0.1: SA238 – Project approvals

Prepared by	Kalpna Shukla – Head of Architecture & Applications Simon Burke – Head of OneERP
Reviewed by	Brooke Palmer – Head of IT Business Engagement
Approved by	Brett Miller – Chief Information Officer

1.2 Project overview

Table 0.2: SA238 – Project overview

Description of problem /opportunity	<p>The efficient and reliable operation of AGIG's South Australian gas network business (AGN SA) is underpinned by a number of corporate and operational information technology (IT) applications. This business case covers our corporate applications. It is distinct from our operational applications which are discussed in business case SA217: IT operational applications.</p> <p>At AGIG we have a suite of corporate IT applications that are used across our businesses. These applications provide business critical functions from HR, finance and payroll, through to asset management and works planning. Over the past five years, we have sought to find common IT applications across our businesses where it makes sense to align our systems and processes through the 'One-AGIG' IT program. Where these applications are shared across businesses, we allocate costs based on the contribution to, and use of the application for each business.</p> <p>There are still business-specific applications in most of our businesses, including AGN SA (e.g. GTreasury), as we either have not yet found a global solution, or have not yet had the time to adopt one. Where applications are business-specific, the costs are directly allocated.</p> <p>We have two categories of IT applications expenditures required over the next AA period:</p> <ul style="list-style-type: none"> • Recurrent maintenance and currency activities: These are business as usual activities required to ensure our suite of applications is operationally functional, secure and kept 'in-support' by the service provider. Service providers release regular, cyclical major and minor upgrades, that we have to implement within our business. For most of our applications, we have some flexibility as to when we upgrade our instance. This provides us with the ability to develop a reasonably steady maintenance program overall. These major and minor releases often include minor application enhancements which we are able to adopt as part of the cyclical update process.
--	--

- **Non-recurrent new/replacement application projects:** As our businesses evolves, so does our suite of applications. We regularly review whether our applications remain fit-for-purpose and the most effective and efficient way of providing our services. This includes through feedback from users across the organisation, and external developments in the technology environment. This process often results in the adoption of new applications, adoption of additional significant uplifts in the capability/functionality in existing applications, or the wholesale replacement of an application.

Both categories of work are required to support the ongoing integrity of our data and services and compliance with our regulatory obligations in an environment where there is an ever-increasing reliance on our IT applications.

The identified program for the next five years reflects an increasing need for reliable, secure, compliant and efficient business processes and systems that is flexible enough to continue to meet our evolving business needs. We have carefully assessed our options in relation to the frequency of recurrent maintenance activities and non-recurrent projects to prioritise our program of work based on the strategic importance of each and their contribution to AGIG's objectives, and have adopted the following approaches:

- This business case reflects the continuation of our risk-based approach to the maintenance of our applications through a prudent and timely upgrade and refresh regime. We adopt an N-1 approach (i.e. one level of redundancy) to managing our applications suite. This means we typically maintain application versions that are one version older than the latest vendor offering. This allows us to fully assess the value and benefit of an upgrade/enhancement before we decide whether to adopt it. We identify the optimal time to apply minor and major version upgrades, rather than relying solely on the vendor-driven upgrading/patching schedule.
- This business case includes a number of non-recurrent projects that will need to be undertaken to provide additional functionality either through significant enhancements to existing applications, or introducing a new or replacement application. These projects are aimed at improving our corporate functions including health safety and environment, financial and contract management and project management for AGN SA. These programs will ensure AGN SA is able to operate within the AGIG environment.

As a result of these technology investments, the evolving business needs are met with a mature and modern IT landscape.

It should be highlighted that the transition of the operational IT assets related to our South Australian network to AGIG is not included in this business case (see business case: SA217). This program of work will not be impacted by the proposed works associated with the transition.

Untreated risk

As per risk matrix = High

Options considered

- **Option 1** – Vendor-driven recurrent maintenance and currency activities and non-recurrent new/replacement application projects (\$5.0 million capex, \$2.2 million opex)
- **Option 2** – Risk-based approach to recurrent maintenance and currency activities and non-recurrent new/replacement application projects (\$4.6 million capex, \$2.2 million opex)
- **Option 3** – Risk-based approach to recurrent maintenance and currency activities, no non-recurrent new/replacement application projects (\$3.0 million capex, \$1.6 million opex)

Proposed solution	<p>Option 2 is recommended as the most prudent and cost-effective approach to ensuring the ongoing reliability and effectiveness of AGIG's corporate IT applications supporting its South Australian operations. This strategy balances the need to mitigate risks associated with outdated and unsupported systems through timely recurrent upgrades with a strategic focus on implementing non-recurrent enhancement projects that address evolving business and customer needs. This approach aligns with good industry practice and manufacturer recommendations for maintaining a stable and secure IT environment.</p> <p>Option 1 is not recommended due to the increased frequency of upgrades and accelerated implementation of new functionalities, leading to potentially imprudent expenditure without a clear demonstration of commensurate business value for our South Australian customers. While it would address all application security, compatibility, and obsolescence risks, the cost may outweigh the demonstrated need.</p> <p>Option 3 is not recommended as it solely addresses the risk of application obsolescence. It fails to provide the necessary investment in non-recurrent application enhancement projects required to adapt to evolving business needs and foster more efficient ways of working within AGIG's South Australian operations.</p>																												
Estimated cost	<p>The forecast direct capital and operating cost during the next AA period (July 2025 to June 2031) is \$6.8 million.</p> <table><tr><th>\$'000 Jan 25</th><th>2026/27</th><th>2027/28</th><th>2028/29</th><th>2029/30</th><th>2030/31</th><th>Total</th></tr><tr><td>Capex</td><td>1,526</td><td>718</td><td>1,001</td><td>814</td><td>555</td><td>4,614</td></tr><tr><td>Opex</td><td>403</td><td>416</td><td>430</td><td>461</td><td>493</td><td>2,203</td></tr><tr><td>Total</td><td>1,929</td><td>1,133</td><td>1,432</td><td>1,275</td><td>1,048</td><td>6,817</td></tr></table> <p>The \$2.2 million increase in opex across the period is required as several apps are being replaced by newer/alternative applications, which are being hosted on the SAP RISE cloud platform and/or offered on a software as a service (SaaS) basis and therefore result in a new recurrent opex cost.</p>	\$'000 Jan 25	2026/27	2027/28	2028/29	2029/30	2030/31	Total	Capex	1,526	718	1,001	814	555	4,614	Opex	403	416	430	461	493	2,203	Total	1,929	1,133	1,432	1,275	1,048	6,817
\$'000 Jan 25	2026/27	2027/28	2028/29	2029/30	2030/31	Total																							
Capex	1,526	718	1,001	814	555	4,614																							
Opex	403	416	430	461	493	2,203																							
Total	1,929	1,133	1,432	1,275	1,048	6,817																							
Basis of costs	All costs in this business case are expressed in real unescalated dollars of January 2025 unless otherwise stated.																												
Treated risk	As per risk matrix = Intermediate																												
Alignment to our vision	<p>This project aligns with the <i>Customer Focussed</i> aspect of our vision by ensuring technology systems supporting our operations and ultimately customer services are adequately maintained and available to meet their needs.</p> <p>This project aligns with our vision objective of being <i>A Leading Employer</i>, as it aims to provide employees and third-party users of our systems with current, reliable, accurate and fit-for-purpose technology solutions that allow the business and its contractors to operate effectively.</p> <p>This project aligns to our vision of achieving <i>Operational Excellence</i> as the project will execute a lifecycle management plan that follows good industry practice and manufacturer's recommendations, mitigates risks, optimise capital and operational expenditure and minimise application support costs.</p>																												
Consistency with the National Gas Rules (NGR)	<p>NGR 79(1)/91 – Maintaining a stable set of corporate IT applications that is current and fit-for-purpose is critical to our business (they inform business decisions and helps us to efficiently manage our business processes). The proposed program of work is consistent with accepted good industry practice, several alternative options have been considered and unit rates and timing of refreshes have been tested to achieve the lowest sustainable cost of delivering pipeline services.</p>																												

	<p>NGR 79(2) – The proposed expenditure on our corporate IT applications is required to maintain the integrity of services through current, supported and fit-for-purpose IT applications, managing technology risks and preventing material outages that impact the ability of the business to function (including tracking and reporting of business information to meet our regulatory obligations and requirements).</p> <p>NGR 74 – The forecast costs are based on the latest market rate testing, and project options consider the requirements of our application environment. Application maintenance and currency activities are scheduled based on risk and costed by third-party software providers. Cost assessments have been conducted for each option based on the best information available at the time of developing this business case. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.</p>
<p>Stakeholder engagement</p>	<p>Customers consistently ranked price and affordability as their top priority. They also told us that they place a great deal of importance on safety and reliability of supply. Customers were clear they expect good communication and simple service that is resolution-focused. Customers agreed that supplying cleaner energy was important, but that affordability is a key consideration for them.</p> <p>The ongoing investment in our IT corporate applications program is fundamental to maintaining the safe and reliable operation of our gas distribution network in South Australia. Core corporate applications such as S/4HANA, GTreasury and SuccessFactors are central to our daily operations. Therefore, it is critical that we continue to invest in these applications through timely recurrent upgrades to ensure their continued operational effectiveness. Our non-recurrent projects are designed to strategically implement prioritised enhancement to existing applications and introduce new capabilities that can enhance the quality and efficiency of our service delivery.</p> <p>Our risk-based approach to managing these applications involves assessing business needs to determine the optimal timing for recurrent upgrades and the implementation of non-recurrent application implementations and targeted application improvements. By adopting an N-1 approach to version management, we ensure a thorough evaluation of the value and benefits before adoption whilst mitigating risks associated with outdated and unsupported systems through timely recurrent upgrades. This prudent approach to IT investment helps us maintain sustainable costs and mitigate potential impacts on customers' gas bills, aligning with their key priority of affordability while upholding safety and reliability.</p>
<p>Other relevant documents</p>	<p>This business case should be read in conjunction with:</p> <ul style="list-style-type: none"> • Attachment 9.3: Asset Management Plan • Attachment 9.6: Procurement Policy and Procedure • Attachment 9.7: IT Investment Plan • Attachment 9.11: Risk Management Framework • AGIG 'One IT' Strategy & Roadmap • Capitalisation Policy • Business case SA217: IT operational applications • Business case SA239: IT sustaining infrastructure • Business case SA240: Cyber security

1.3 Background

Our business processes and customer services rely on reliable access to information. That information is stored, accessed and analysed through our IT corporate applications. These IT applications help sustain our businesses by enabling a range of activities including (but not limited to):

- Finance and accounting
- Project management systems
- Procurement and contract management
- Customer relationship management and the digital customer experience
- Data archiving and document management
- Data analytics and visualisation
- Payroll and HR

1.3.1 Our corporate IT asset management approach

AGIG employs a well-established and proven application management regime, governed by our IT Investment Plan, to ensure the ongoing availability, security and optimal performance of our business-critical systems for both our staff and our customers in South Australia. Our approach involves a considered evaluation of business value, system criticality, and vendor recommendations when planning recurrent and non-recurrent capital works.

An important part of our IT asset management approach is timing and priority. Software patches and version upgrades are provided by software vendors, who recommend their technology be upgraded to ensure continued provision of support and that any potential security vulnerabilities can be addressed. These upgrades enable transition to improved versions of the technology, correct defects in the technology (which includes how a technology type interacts with other technology types), and offer additional functionality.

Software vendors provide patches and version upgrades to maintain support and address potential security vulnerabilities, often including functional changes. These upgrades typically involve the application itself and associated technology platform components, requiring assessment, design, configuration, customisation, integration, and comprehensive testing of impacted processes.

While vendor timelines are a key input, AGIG strategically applies an application lifecycle management methodology to determine the timing and priority of recurrent upgrades. This approach balances vendor recommendations with a careful consideration of business needs and risk tolerance, ensuring appropriate levels of operation, data integrity, and interoperability across our technology environment. A core principle of our methodology is maintaining a minimum of N-1 for application upgrades, which aligns with industry best practice, ensures ongoing vendor support, and mitigates risks of security breaches, system outages, and potential regulatory non-compliance. As AGIG IT is a national function, AGN SA corporate applications adhere to the AGIG application lifecycle management methodology detailed in Appendix C.

1.3.2 Overview of our IT corporate applications program for 2026-31

Our IT corporate applications program for the upcoming AA period is structured around two key categories of activities:

- **Recurrent maintenance and currency activities:** These are business as usual activities required to ensure our suite of applications is operationally functional, secure and kept 'in-support' by the service provider. Service providers release regular, cyclical major and minor upgrades, that we have to implement within our business. For most of our applications, we have some flexibility as to when we upgrade our instance. This provides us with the ability to develop a reasonably steady maintenance program overall. It also includes minor enhancements where this is delivered as part of an application update/upgrade project, noting significant and stand-alone application enhancements are undertaken as a separately scoped and implemented projects.
- **Non-recurrent new/replacement application projects:** As our businesses evolves, so does our suite of applications. We regularly review whether our applications remain fit-for-purpose and the most effective and efficient way of providing our services. This includes through feedback from users across the organisation, and external developments in the technology environment. This process often results in the adoption of new applications, adoption of significant new additional capability/functionality in existing applications, or the wholesale replacement of an application. These projects are scoped separately and implemented outside of the regular upgrade program.

Combined, these two workstreams ensure our applications are maintained appropriately, mitigate the risk of obsolescence or downtime, and provide opportunity to improve work practices and respond to changing requirements. The scale of this ongoing program may vary across regulatory periods based on application upgrade cycles and changing business needs.

AGIG relies on a well-established suite of core applications embedded across our operations. Critical corporate applications include our enterprise resource planning system (SAP S/4HANA), our HR system (SuccessFactors), and our customer relationship management (SAP C4C) system. The recent implementation of SAP S/4HANA in 2023, as part of the AGIG-wide OneERP program replacing AGN's SAP Business One, represents a strategic upgrade to our integrated business system capabilities. The transition has delivered consolidated and streamlined business processes across critical functions such as Finance and Procurement, and has enhanced integration with other key AGIG business processes. It is one of our most critical business applications, building the foundation for a range of new functionality to our business, going beyond new functionalities like mobility, user management and security groups.

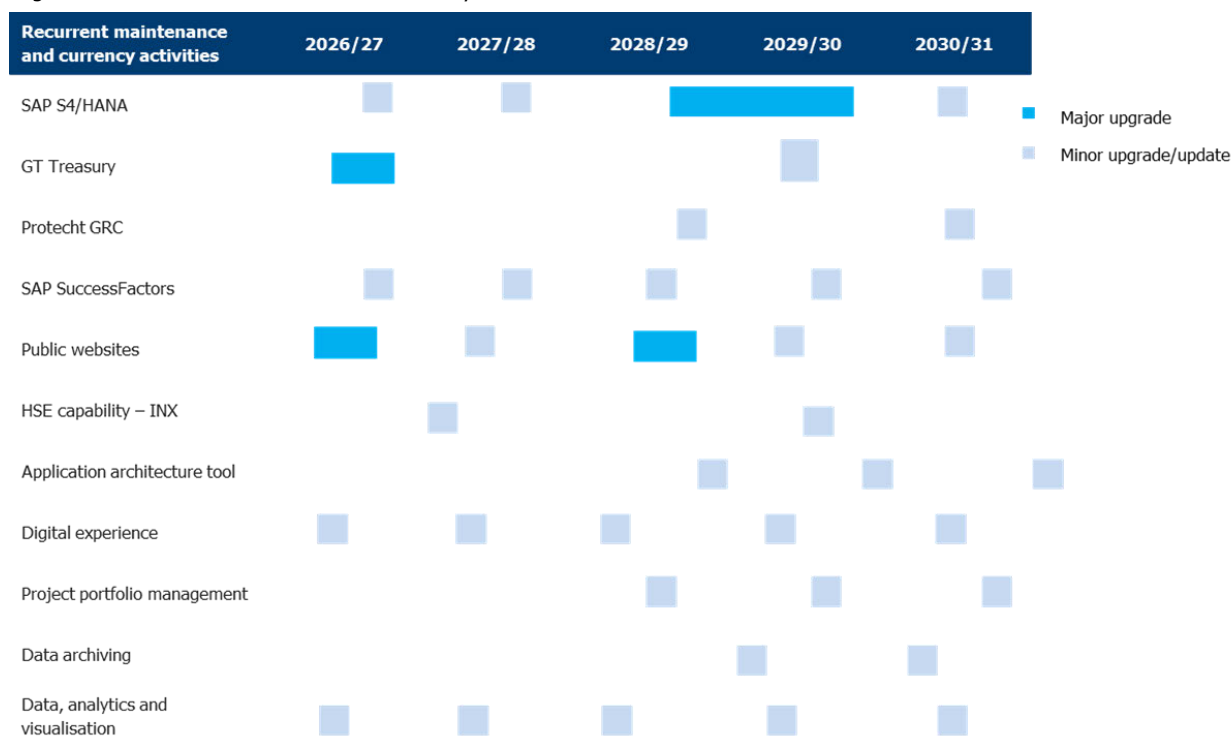
Following the completion of the OneERP project, the anticipated expenditure on corporate applications for the 2026-31 AA period (approximately \$6.8 million in total) is considerably lower than the previous period. While ongoing investment in SAP S/4HANA is necessary to maintain the system and facilitate a range of functionality non-recurrent

improvements, this is now integrated into our regular upgrade program and is significantly below the initial implementation cost.

1.3.2.1 Recurrent maintenance and currency activities

Our proposed schedule for recurrent maintenance and currency activities (see Figure 1.1) is strategically staggered throughout the period. This schedule includes major and minor application upgrades thereby ensuring currency and reliability of our corporate applications.

Figure 0.1: Recurrent maintenance and currency schedule



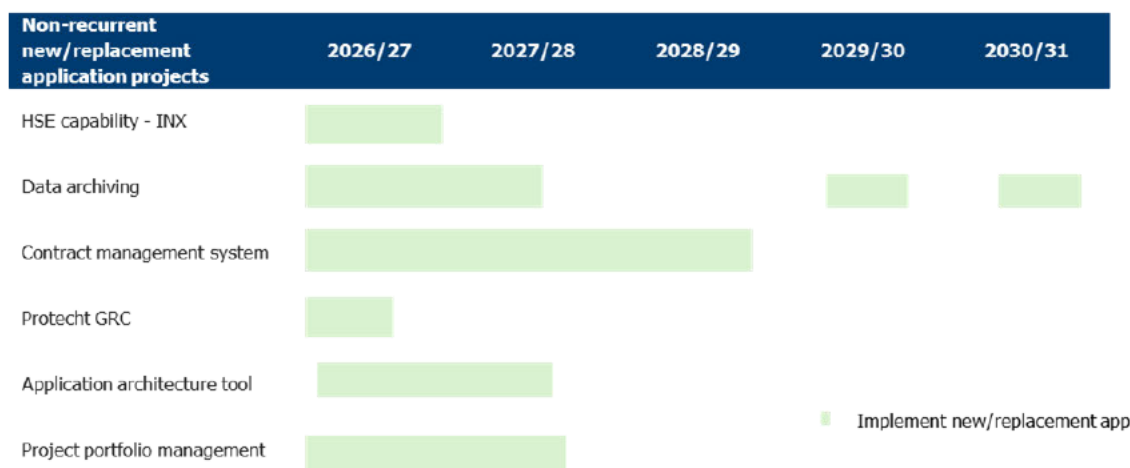
This phased approach is designed so that work is spread over the period, allowing us to deploy resources efficiently. Minor upgrades, such as the annual SuccessFactors releases, delivered via a software as a service (SaaS) model, have a shorter timeframe than major version upgrades such as S/4HANA. However, they both still require careful assessment and selective activation of features.

1.3.2.2 Non-recurrent new/replacement application projects

Similar to our recurrent expenditure schedule, our non-recurrent new/replacement application projects are staggered across the period to help optimise deliverability (see Figure 0.2). These are more strategic in nature and support the organisation delivering business strategies through technology solutions. There are two types of application implementation projects:

- The first is the introduction of a new application or significant new functionality to improve to support the business. These projects often lead to an improvement in the way we do business. For example, we propose to implement a contract management system to replace our current fragmented and highly manual contract management processes.
- The second is where a new application replaces one or more existing applications that are redundant, lacking in functionality, or no longer fit for purpose. For example, we propose to replace Protecht GRC with a new system to better manage our governance risk and compliance functions.

Figure 0.2: Non-recurrent new/replacement application project schedule



Our forecast assumes a consistent level of investment in these application improvements throughout the period. However, actual expenditure will be driven by the volume and assessed cost-benefit of business requests on a case-by-case basis governed by our two-tier improvement management process (see Appendix D).

1.4 Risk assessment

Risk management is a constant cycle of analysis, treatment, monitoring, reporting and then identifying once again, with a commitment to balance outcomes sought with delivery and cost implications considered and assessed.

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.

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.

Figure 0.3: Risk management principles



Based on these two key inputs, the risk assessment and derived risk rating then guides the actions and activities required to ensure safety and compliance are not compromised, while delivery of this outcome is done as efficiently and effectively as possible.

The risk rating assesses the consequence and likelihood of the risk. The risk of an event associated with failure of an asset is rated based on the combined effect of the consequence and likelihood rating to provide an overall risk rating. This risk rating guides the risk management and mitigation activities and facilitates prioritisation.

Our Operational Risk Framework is based on AS/NZS 2885 and requires all identified risks ranked as intermediate or above to be addressed. For risks ranked as high we must *'Modify the threat, the frequency or the consequence to reduce the risk rank to intermediate or lower'*.

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 moderate or higher, we will undertake investment to reduce the risk.

Seven consequence categories are considered for each type of risk:

1. **Health & safety** – 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. **Operational capability** – Disruption in the daily operations and/or the provision of services/supply, impacting customers.
4. **People** – Impact on engagement, capability or size of our workforce.
5. **Compliance** – Impact from non-compliance with operating licences, legal, regulatory, contractual obligations, debt financing covenants or reporting / disclosure requirements.
6. **Reputation & customer** – Impact on stakeholders' opinion of AGN, including personnel, customers, investors, security holders, regulators and the community.
7. **Financial** – Financial impact on AGN, measured on a cumulative basis.

The primary risk event being assessed for our IT corporate applications is that as IT applications versions become outdated, 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.

The untreated risk¹ rating associated with IT corporate applications is presented in Table 0.3.

Table 0.3: Untreated risk rating

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

Security breaches, and unavailability of operational and corporate systems gives rise to safety, operations, customer/reputational, compliance and financial consequences, as described below.

- *Operations* – Uncorrected deficiencies or 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. This can result in lengthy supply outages, with the potential to impact >10,000 customers or at least one major demand customer (using >10 TJ per annum).
- *Compliance* – Unsupported and poorly integrated systems and compromised customer information may result in AGN not complying with a range of legal and regulatory obligations, for example the financial reporting requirements.
- *Reputation and customer* – Poorly performing IT systems and inaccurate data may result in breaches of the service standards, set out in the South Australian Gas Distribution Code⁸⁰. In addition, security breaches may result in confidential customer data being compromised. This in turn can impact AGN's reputation.
- *Finance* – Non-compliance with our obligations relating to data management can result in financial penalties. There is also the risk of having to pay a premium to resolve compatibility issues with unsupported/obsolete applications if the necessary upgrades are not installed.

1.5 Options considered

The options considered are:

- **Option 1** – Vendor-driven recurrent maintenance and currency activities and non-recurrent new/replacement application projects
- **Option 2** – Risk-based approach to recurrent maintenance and currency activities and non-recurrent new/replacement application projects
- **Option 3** – Risk-based approach to recurrent maintenance and currency activities, no non-recurrent new/replacement application projects

These options are discussed in the following sections.

¹ Untreated risk is the risk level assuming there are no risk controls currently in place. Also known as the 'absolute risk'.

An option to not upgrade or implement improvements in our application suite, only replacing applications on failure was dismissed due to the criticality of our application suite for our operations and business continuity. For example, it is not practicable to run applications such as SAP S/4HANA or SuccessFactors to failure or to update regularly (e.g. patches), as too many of our business functions depend on these applications working correctly. A run to fail or 'do nothing' option has therefore not been explored further in this business case.

1.5.1 Option 1 – Vendor-driven recurrent maintenance and currency activities and non-recurrent new/replacement application projects

This option provides a state where all systems would be patched, upgraded and supported according to the release schedules provided by vendors, irrespective of business criticality. Under this option, all maintenance and currency activities are undertaken promptly when these become available from vendors.

This option assumes AGN implements all vendor-recommended upgrades across our application suite at the vendor's estimated costs and timeline. For S/4HANA for example, this would entail the implementation of Feature Pack Stacks (FPS) every six months (considered minor upgrades) and a major version every two years. This option also includes adhering to additional SuccessFactors minor releases, and additional public website platform releases.

In addition, this option provides an allowance for new/replacement application projects based on an identified business need.

1.5.1.1 Advantages and disadvantages

An advantage of this approach is that it provides greater certainty that all AGN's systems are fully supported, operational, and are subject to the latest cyber security patches/measures (updates). It would reduce the likelihood of application downtime, and by continually adopting the latest versions, it would help ensure compatibility with emerging hardware and device technologies. Adopting upgrades and patches immediately also means our applications will remain fully supported by the vendors' maintenance teams.

Under this option we would also utilise an allowance for business-driven application enhancements to existing systems. This would allow us to make planned (and ad-hoc) investments in applications to maximise new capabilities based on business need and cost benefit analysis, as well as getting the optimum value out of our investment.

The major disadvantage of the vendor-driven maintenance and currency approach is the cost. Vendors typically release major upgrades every 2-5 years, often with several minor updates in between. The cost of an update varies by application, but each update can cost anywhere from \$50,000 to \$5,000,000. Further, the frequency of update would likely affect deliverability, requiring an uplift in internal or external resources to keep on top of the rolling upgrade program.

A key concern with adopting all vendor-driven upgrades is the potential for increased complexity and unnecessary effort. While application upgrades often include new functionalities or 'add-ons', not all of these are essential or aligned with AGIG's specific business needs. Implementing every vendor-recommended update or upgrade could lead to a more complex application landscape, requiring resources to manage and test features that may never be fully utilised. This approach may divert valuable IT resources away from more strategic initiatives and could increase the risk of introducing instability without a clear and demonstrable business benefit. Furthermore, adhering strictly to vendor cycles may necessitate upgrades even when the current system adequately meets AGIG's requirements, potentially leading to premature investment and inefficient resource allocation.

Our preference is to only invest in applications where the upgrade is either essential (for example for cyber security or business continuity reasons) or we can see value in the new functionality (the functionality will be used and will improve our business operations).

1.5.1.2 Achievement of objectives

Table 0.7 outlines how Option 1 will support achievement of our vision objectives.

Table 0.4: Achieving objectives – Option 1

Vision objective	Alignment
Customer Focussed – Public Safety	-
Customer Focussed – Customer Experience	Y
Customer Focussed – Cost Efficient	Y
A Leading Employer – Health and Safety	Y
A Leading Employer – Employee Experience	-
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	N
Operational Excellence – Benchmark Performance	N
Operational Excellence – Reliability	Y
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

Option 1 would align with our strategic objective of being *Customer Focussed* and being *A Leading Employer*, as it would help ensure our application suite is fully functional, meaning we can provide a high quality and reliable service to customers, as well as ensuring our employees have the applications they need to be able to do their jobs.

However, Option 1 would not align with our objective of achieving *Operational Excellence*. Adopting all vendor-driven upgrades may result in over-investment in our application suite, which does not represent efficient expenditure. Option 1 does not allow for a more strategic approach to investing in IT applications, whereby we would make sure our application suite grows and changes in line with our business growth and changes to work practices.

1.5.1.3 Cost assessment

The estimated direct capital cost of this option is \$5.0 million (see Table 0.4).

This cost estimate is based on the projected expenses for upgrading and maintaining the existing application suite, along with anticipated changes dictated solely by vendor roadmaps. It's important to note, this approach does not allow for any synergies or coordinated upgrade efforts in similar or shared applications across the AGIG businesses.

This option also includes a range of non-recurrent new/replacement application projects based on identified requirements and new product availability (see Appendix A.2 for a description of each and the options considered).

Table 0.5: IT corporate applications capex program 2026-31 – Option 1, \$'000 January 2025

Capex – Option 1	2026/2 7	2027/2 8	2028/2 9	2029/3 0	2030/3 1	Total
Application maintenance and currency						
SAP S/4HANA	108	108	216	216	-	649
GTreasury	177	-	-	71	-	248
SAP SuccessFactors	17	17	17	17	17	87
Public websites	83	27	113	27	27	278
SAP S/4HANA incremental functionality	87	87	87	87	87	433
Digital customer experience	248	192	213	232	225	1,110
Data, analytics and visualisation	61	115	101	92	93	462
Application architecture tool	-	-	28	24	21	74
HSE capability - INX	-	33	-	33	-	66
Protect GRC	-	-	57	-	27	84
Data archiving	-	-	-	40	59	99
Total application maintenance and currency	782	579	832	842	556	3,590
Enhancement projects						
HSE capability - INX	73	-	-	-	-	73
Data archiving	147	-	-	40	59	246
Protect GRC	120	-	-	-	-	120
Application architecture tool	26	28	-	-	-	55
Project portfolio management	63	59	-	-	-	122
Contract management system	423	186	169	-	-	778
Total enhancement projects	853	274	169	40	59	1,395
Total capex	1,634	853	1,001	882	615	4,985

This option would also require a \$2.2 million increase in opex across the period associated. This increase is primarily attributed to:

- Software subscriptions and support contracts
- Increase training requirements for staff to adapt to frequent changes and new functionalities introduced with each upgrade

- Potentially higher maintenance costs associated with frequently updated and potentially more complex systems
- The transition of SAP S/4HANA and SuccessFactors to the SAP RISE platform and the associated SaaS subscription models, driven by vendor upgrade paths

The uplift in opex is shown in Table 0.6.

Table 0.6: IT corporate apps opex program - Option 1, \$'000 January 2025

Opex – Option 1	2026/2 7	2027/2 8	2028/2 9	2029/3 0	2030/3 1	Total
Application maintenance and currency						
SAP S/4HANA	116	118	118	118	118	590
GTreasury	81	81	81	88	88	419
SAP SuccessFactors	30	30	30	30	30	152
Digital customer experience	46	48	52	57	74	277
Data, analytics and visualisation	21	24	24	35	42	147
Total application maintenance and currency	295	302	306	329	353	1,585
Enhancement projects						
HSE capability - INX	17	20	20	27	30	115
Data archiving	13	13	13	13	13	63
Protect GRC	34	34	37	37	41	183
Application architecture tool	10	13	19	21	22	85
Project portfolio management	9	9	9	9	9	45
Contract management system	25	25	25	25	25	127
Total enhancement projects	108	114	124	133	140	619
Total opex	403	416	430	461	493	2,203

The estimated impact on opex resulting from the relevant application upgrades is discussed further in Appendix A.

1.5.1.4 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. This is consistent with our operational risk framework, as it reduces the residual risk outcome from high to moderate or lower.

Table 0.7: Risk assessment - Option 1

Option 1	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Low	Low	

1.5.2 Option 2 – Risk-based approach to recurrent maintenance and currency activities and non-recurrent new/replacement application projects

As a prudent operator, AGN has conducted thorough risk assessments to determine the criticality of its IT systems supporting its operations. Consistent with these assessments and good industry practice, we have determined that maintaining our systems at the current version with a level of redundancy (N-1) is the most efficient and effective strategy for ensuring continued compliance, data integrity and operational reliability.

This option involves a plan to systematically implement recurrent upgrades to our applications in alignment with this N-1 approach and our technology lifecycle management plan. This strategy ensures software currency, vendor support, security risk mitigation, and maintenance of essential features and functionality for business users.

Our approach to recurrent maintenance and currency activities is pragmatic, prioritising those that deliver clear business value or address risks of not upgrading exceeding our established tolerances.

Unlike the vendor-driven approach outlined in Option 1, Option 2 does not include the immediate application of all released patches, except in cases of identified cyber security vulnerabilities requiring immediate action.

Option 2 also incorporates provisions for non-recurrent new/replacement application projects based on a clearly identified business need and positive cost benefit.

1.5.2.1 Advantages and disadvantages

This risk-based approach offers several key advantages. Firstly, it allows AGN to proactively manage cybersecurity risks by implementing necessary recurrent upgrades in a timely manner, but strategically aligned with our assessment of the threat landscape related to our environment, potentially will resulting in a lower overall cost compared to a purely vendor-driven approach. Secondly, it enables a systematic alignment of recurrent upgrades with enterprise-wide requirements and our technology lifecycle management plan, ensuring maximum benefit across the organisation.

The disadvantage of this option is the potential for a temporary increase in risk related to vendor support or compatibility issues. By strategically delaying some recurrent upgrades, there may be a period where maintenance costs in the event of an issue are potentially higher. However, we will consider this risk on a case-by-case basis, assessing the specific application, the criticality of the upgrade, and the potential business impact of delaying it. Furthermore, a thorough assessment will be undertaken to understand any potential compatibility issues arising from the N-1 approach before a decision to delay an update or upgrade is made.

1.5.2.2 Achieving objectives

The following table outlines how Option 2 will support achievement of our vision objectives.

Table 0.8: Achieving objectives – Option 2

Vision objective	Alignment
Customer Focussed – Public Safety	-
Customer Focussed – Customer Experience	Y
Customer Focussed – Cost Efficient	Y
A Leading Employer – Health and Safety	Y
A Leading Employer – Employee Experience	-
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	Y
Operational Excellence – Benchmark Performance	Y
Operational Excellence – Reliability	Y
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

This option delivers against all of our vision objectives of being *Customer Focussed*, being *A Leading Employer* and displaying *Operational Excellence* as it proactively maintains a stable IT applications environment to support business processes, in line with good industry practice at a sustainable cost over the medium to longer term.

Option 2 aligns with our objective of being *Customer Focussed*, as it would deliver the appropriate risk mitigation to ensure availability and reliability of core 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 Leading 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 aligns with our objective to achieve *Operational Excellence*.

1.5.2.3 Cost assessment

The estimated direct capital cost of Option 2 is \$4.6 million as shown in the following table. This estimate encompasses the projected costs for strategically upgrading and maintaining our existing application suite, as well as the investments in targeted non-recurrent initiatives to address evolving business requirements and compliance to the overall application landscape.

Table 0.9: IT corporate applications capex program 2026-31– Option 2, \$'000 January 2025

Capex – Option 2	2026/27	2027/28	2028/29	2029/30	2030/31	Total
	7	8	9	0	1	
Application maintenance and currency						

Capex – Option 2	2026/27	2027/28	2028/29	2029/30	2030/31	Total
SAP S/4HANA	-	-	216	216	-	433
GTreasury	177	-	-	71	-	248
SAP SuccessFactors	17	17	17	17	17	87
Public websites	83	-	113	-	-	196
SAP S/4HANA incremental functionality	87	87	87	87	87	433
Digital customer experience	248	192	213	232	225	1,110
Data, analytics and visualisation	61	115	101	92	93	462
Application architecture tool	-	28	28	24	21	102
HSE capability - INX	-	33	-	33	-	66
Protect GRC	-	-	57	-	54	111
Data archiving	-	-	-	40	59	99
Total application maintenance and currency	673	472	832	814	555	3,347
Enhancement projects						
HSE capability - INX	73	-	-	-	-	73
Data archiving	147	-	-	-	-	147
Protect GRC	120	-	-	-	-	120
Application architecture tool	26	-	-	-	-	26
Project portfolio management	63	59	-	-	-	122
Contract management system	423	186	169	-	-	778
Total enhancement projects	853	245	169	-	-	1,267
Total capex	1,526	718	1,001	814	555	4,614

This option would also require a \$2.2 million increase in opex across the period, consistent with Option 1.

1.5.2.4 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. This is consistent with our operational risk framework, as it reduces the residual risk outcome from high to intermediate or lower.

Table 0.10: Risk assessment - Option 2

Option 2	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Low	Low	

This option appropriately addresses the identified risks, achieving a similar risk outcome as Option 1, but it does so at a lower overall cost.

1.5.3 Option 3 – Deliver the upgrades program only, with no non-recurrent new/replacement application projects

Option 3 proposes a program focused solely on delivering the necessary recurrent application upgrades, following the same risk-based assessment and N-1 approach outlined in Option 2. However, this option explicitly excludes any investment in non-recurrent new/replacement application projects.

1.5.3.1 Advantages and disadvantages

The primary advantage of this approach is the potential for lower overall expenditure during the period as it limits investment to only the necessary recurrent upgrades required to maintain application currency and vendor support of applications.

A significant disadvantage of this approach is the failure to address evolving business needs and optimise our existing suite of applications through targeted non-recurrent enhancement projects including increased functionality of existing applications and the implementation of new and replacement applications. Whilst recurrent upgrades maintain the technical currency of our applications, they often do not provide the specific new functionalities, nor the customisation, required to fully leverage their potential and address evolving business needs. For example, the ongoing incremental improvements to our recently implemented SAP S/4HANA, which are crucial for optimising user experience and unlocking new capabilities, like advanced analytics or automation, would cease. Similarly, opportunities to enhance our digital experience and to address our fragmented contract management system would be foregone. This process of incremental improvement should continue throughout the life of the application to ensure we are maximising the value of the solution to our business and ultimately customers.

If we were to stop investing in application enhancements and relied on recurrent upgrades only, we would be foregoing the opportunity to improve and standardise our business processes.

1.5.3.2 Achieving objectives

The following table outlines how Option 3 will support achievement of our vision objectives.

Table 0.11: Achieving objectives – Option 3

Vision objective	Alignment
Customer Focussed – Public Safety	-
Customer Focussed – Customer Experience	N
Customer Focussed – Cost Efficient	Y
A Leading Employer – Health and Safety	N
A Leading Employer – Employee Experience	-
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	Y

Operational Excellence – Benchmark Performance	N
Operational Excellence – Reliability	N
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

Investing in new versions of applications but failing to then build on that through incremental improvement does not reflect the actions of *A Leading Employer*. While this option would be relatively low cost, it would not meet our objective of *Operational Excellence*, it may result in applications becoming less reliable or unsuited to business needs, leading to manual workarounds and potential for information inaccuracy. Essentially, we would not be giving our employees the tools they need, leading to dissatisfaction, inefficiency and increased risk of not having accurate information on which to base important business decisions.

1.5.3.3 Cost assessment

The estimated direct capital cost of Option 3 is \$3.0 million. As detailed in Table 0.12, this estimate covers the project expenses for the periodic upgrades to maintain our existing application suite and ensure ongoing vendor support, but it explicitly excludes any proactive investment in application improvements or new functionalities to address evolving business needs with operations.

Table 0.12: IT corporate applications capex program 2026-31– Option 3, \$'000 January 2025

Capex – Option 3	2026/2 7	2027/2 8	2028/2 9	2029/3 0	2030/3 1	Total
Application maintenance and currency						
SAP S/4HANA	-	-	216	216	-	433
GTreasury	177	-	-	71	-	248
SAP SuccessFactors	17	17	17	17	17	87
Public websites	83	-	113	-	-	196
SAP S/4HANA incremental functionality	87	87	87	87	87	433
Digital customer experience	248	192	213	232	225	1,110
Data, analytics and visualisation	61	115	101	92	93	462
Total application maintenance and currency	673	411	746	716	421	2,969
Total capex	673	411	746	716	421	2,969

This option would also require a \$1.5 million increase in opex across the period associated. This increase is primarily attributed to:

- Software subscriptions and support contracts
- Increase training requirements for staff to adapt to frequent changes and new functionalities introduced with each upgrade

- Potentially higher maintenance costs associated with frequently updated and potentially more complex systems
- The transition of SAP S/4HANA and SuccessFactors to the SAP RISE platform and the associated SaaS subscription models, driven by vendor upgrade paths

The uplift in opex is shown in Table 0.13.

Table 0.13: IT corporate apps opex program 2026-31– Option 3, \$'000 January 2025

Opex – Option 3	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Application maintenance and currency						
SAP S/4HANA	116	118	118	118	118	590
GTreasury	81	81	81	88	88	419
SAP SuccessFactors	30	30	30	30	30	152
Digital customer experience	46	48	52	57	74	277
Data, analytics and visualisation	21	24	24	35	42	147
Total application maintenance and currency	295	302	306	329	353	1,585
Total opex	295	302	306	329	353	1,585

Cost estimates are based on current market rate testing, considering the requirements of our application environment, using the best information available at the time of developing this business case.

1.5.3.4 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. This is consistent with our operational risk framework, as it reduces the residual risk outcome from high to moderate or lower.

Table 0.14: Risk assessment - Option 3

Option 3	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Low	Low	

Option 3 will still deliver an upgrades program, therefore it addresses the obsolescence risk associated with unsupported applications. As a result, Option 3 achieves the same overall risk rating as Options 2 and 3. However it is important to note, it does not allow for any non-recurrent improvements requested by the business, which could place business operations at risk if the improvement is required to address a material issue. Unfortunately, the risk matrix does not provide sufficient granularity to be able to discern a higher risk rating for this option.

1.6 Summary of options assessment

Table 0.17 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 0.15: Summary of options analysis

Option	Capex	Opex	Risks	Objectives
Option 1: Upgrade based on vendor recommended cycles	\$5.0 million	\$2.2 million	This option moderates all high and moderate risks to ALARP	Does not align with being <i>Customer Focussed, A Leading Employer</i> or achieving <i>Operational Excellence</i>
Option 2: Deliver upgrades and enhancements on a risk-based assessment of business needs	\$4.6 million	\$2.2 million	This option moderates all high and moderate risks to ALARP	This option achieves our objectives of being <i>Customer Focussed</i> , being <i>A Leading Employer</i> and achieving <i>Operational Excellence</i>
Option 3: Deliver the upgrades program only, with no application enhancements	\$3.0 million	\$1.6 million	This option moderates all high and moderate risks to ALARP, but may compromise our ability to address risks that emerge during the period	Does not align with being <i>Customer Focussed, A Leading Employer</i> or achieving <i>Operational Excellence</i>

1.7 Proposed solution

Our proposed solution is Option 2: a strategic approach encompassing risk-based recurrent application upgrades and prioritised non-recurrent improvements and implementations driven by identified business needs. This solution involves the execution of a defined application lifecycle management plan to systematically maintain and evolve our critical business applications. By adhering to a pragmatic upgrade schedule and selectively implementing targeted improvements, this approach ensures the ongoing reliability, security, functionality and interoperability of our services, while preserving their long-term integrity and supporting operational efficiency of AGN's suite of applications.

1.7.1 Why is the recommended option prudent?

Option 2 represents the most prudent approach for AGN as it provides the optimal balance between effectively mitigating the risks associated with outdated and unsupported applications and ensuring cost-effectiveness. This strategy aligns with established good industry practices for managing critical IT assets within regulated utilities.

Our proposed solution proactively addresses risks by maintaining software currency, ensuring ongoing vendor support, strengthening security, and preserving the integrity of our technology environment through a well-defined and risk-based cycle of application upgrades. The increased potential for system failures and the associated impacts inherent in Options 1 and 3 are deemed unacceptable for AGN's commitment to reliable service.

Option 2 not only ensures AGN meets its minimum expected legislative and regulatory obligations but also minimises business disruptions arising from unplanned system

outages, under-performing applications, or inadequate vendor support. Furthermore, by incorporating targeted and prioritised non-recurrent improvements and implementations, this option allows us to meet evolving business needs by ensuring appropriate and fit-for-purpose application functionality exists.

Option 2 is consistent with our vision of being *A Leading Employer*, by providing our teams with reliable and effective tools, and it supports our commitment to *Operational Excellence* by enabling lower overall costs of service delivery in the long term, ultimately benefiting our customers.

Maintaining our IT applications effectively throughout the period and the application lifecycle is a fundamental aspect of responsible management, particularly given their integral role in the management and long-term decision-making processes our business. Choosing a less proactive approach would be significant oversight.

1.7.1.1 Governance and implementation of IT initiatives

The implementation of IT initiatives outlined in this business case will be governed by AGIG's established two-tier framework (Appendix D), which ensures appropriate oversight and decision-making based on the scope and impact of each undertaking. This framework encompasses both larger, more complex projects and smaller, incremental improvements.

Larger initiatives, typically involving significant capital expenditure, strategic impact, or cross-functional dependencies, will be managed as formal projects following our project management methodology. The specific requirements of this methodology, including governance, risk management, and reporting, will be tailored to the individual project's characteristics, such as risk, complexity, and cost. Where these projects involve system acquisition or outsourced services, all procurement activities will adhere to our Procurement Policy and Purchasing Procedure to ensure optimal value and efficient outcomes. Detailed business requirements will be defined closer to the implementation timeframe, considering current market capabilities and specific business needs. Furthermore, the project management processes will incorporate appropriate and comprehensive organisational change management plans aligned with the final solution and implementation approach.

Smaller, more tactical improvements will follow a streamlined, agile delivery cycle (sprint cycle). This process ensures quicker turnaround for lower-risk, high-value non-recurrent improvements.

Regardless of the initiative's size, the following principles will apply:

- An internal business case and justification, commensurate with the initiative's, cost, risk and complexity, will be developed
- Management will review and approve the business case based on the organisation's overarching priorities, risks and benefits
- IT Management will oversee the delivery of the initiative and any associated organisational change management according to the agreed timelines and outcomes

- Business user involvement will be strategically managed to maximise their input whilst minimising disruption to their operational activities
- Organisational change management strategies will be designed to mitigate the risks associated with the change, proportionate to the initiative's benefits and organisational priorities

1.7.2 Estimating the efficient costs

The cost estimates for this program are based on a combination of internal and external resourcing (particularly for specialised expertise or to manage workloads), software licenses, and potential hardware, as applicable. Unit rates for internal IT and business resources are based on an established internal rate card.

Recurrent upgrade activities draw upon a mix of internal IT, business resources and external resourcing for project management, technical implementation, business requirements gathering, testing, and training. Our cost estimates for recurrent upgrades are based on historical costs where available for similar projects, such as previous upgrades for the same application.

Smaller improvements, particularly within systems like SAP S/4HANA, are primarily delivered utilising AGIG's internal IT support teams, leveraging their growing expertise. Where specialised skills or additional capacity is required, these internal teams may be supplemented by outsourced IT support resources. The rates for outsourced IT support are governed by agreed contract rate cards. Our cost estimates are informed leveraging the historical costs of delivering improvements based on business requests.

For larger and more complex non-recurrent projects, including new implementations and significant upgrades, our cost estimates include indicative pricing and implementation costs obtained from vendors and our service partners, supplemented with the increasing capabilities of our internal teams, and business resources as required.

All procurement processes for IT applications will comply with our Procurement Policy and Purchasing Procedure and will follow transparent, competitive tendering processes to select the best value for money solution.

Overall, there does not appear to be many factors affecting the sensitivity of these estimations, however a small amount is costed in USD and therefore susceptible to foreign exchange fluctuations.

1.7.3 Consistency with the National Gas Rules

NGR 79(1)/91

The proposed expenditure on our corporate applications is also consistent with NGR 79(1)(a) and NGR 91, specifically we consider the capital and operating expenditure is:

- **Prudent** – The expenditure is necessary in order to address the identified risks. The proposed initiatives also ensure that our corporate application assets are maintained and replaced before they arrive at the end of their useful economic life. The proposed expenditure can therefore be seen to be of a nature that would be incurred by a prudent service provider.
- **Efficient** – The forecast expenditure is based on historic costs for similar work as well as estimates from relevant vendors of likely solutions. A formal procurement process will be undertaken once the project enters its delivery phase to ensure efficient prices are achieved through a competitive tender process.
- **Consistent with accepted and good industry practice** – The proposed initiatives will ensure that our corporate applications are maintained to industry standard version levels consistent with accepted and good industry practice. This will result in all critical systems being up to date, secure and supported by vendors, consistent with good industry practice.
- Achieves the **lowest sustainable cost of delivering pipeline services** – Upgrading our corporate 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)(c)

The proposed expenditure on our corporate applications program is required to maintain the integrity of services through current, supported and fit-for-purpose IT applications, managing technology risks and preventing material outages that impact the ability of the business to function (including tracking and reporting of business information to meet our regulatory obligations and requirements). This expenditure is therefore consistent with NGR 79(2)(c)(ii) and (iii).

NGR 74

The forecast costs in this business case are based on the latest market rate testing, and project options consider the asset management requirements as per the IT Investment Plan. Cost assessments have been conducted for each option based on the best information available at the time of developing 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 Detail of IT corporate applications requirements and options considered

A.1.1 SAP S/4HANA

AGIG has recently implemented SAP S/4HANA as its enterprise-wide enterprise resource planning (ERP) system. AGN and DBP commenced use of SAP S/4HANA in October 2023, with MGN to follow suit by end of 2026. The 'OneERP' program is an enterprise-wide initiative, with costs allocated to the three AGIG entities based on the number full time equivalent (FTE) employees.

As with all applications, SAP S/4HANA is subject to periodic major (new S/4HANA version) and minor (new feature pack stack) upgrades. These upgrades are specified by the vendor (SAP) and roll out the latest version and functionality each time. Traditionally, every S/4HANA version was released annually with mainstream maintenance support from SAP for five years. Once the period of mainstream maintenance has elapsed, the version falls out of support, potentially incurring higher maintenance costs if something was to go wrong. With S/4HANA version 2023, SAP has changed its support model to provide seven years of mainstream maintenance and a new S/4HANA version every two years, with regular releases of new functionality for the latest version delivered by regular feature pack stacks (FPS). While there is no requirement to adopt every major (new version) and minor (FPS) upgrade available, it is prudent to maintain an up-to-date version of the ERP system where practicable.

The version of SAP S/4HANA that went live at AGN was S/4HANA 2021, which will be out of support in 2026. A later version, S/4HANA 2023, is now available. Phase 2 of the OneERP program, which will implement the new ERP at MGN, will upgrade OneERP S/4HANA to version 2023 in conjunction with a move to SAP's RISE cloud platform. This upgrade will be completed in the current AA period.

Rather than incur the cost of minor upgrades earlier (approximately \$243,000), we have chosen to defer the next S/4HANA upgrade until 2029, when a new version will be available. By the end of 2026, all three AGIG entities (AGN, DBP and MGN) will be operating on the same version of S/4HANA. The 2023 version falls out of support in 2030 after which all three businesses will share the costs of the major upgrade in 2028/2029. AGN is comfortable carrying the maintenance risk on the 2023 version of SAP S/4HANA until then.

A.1.1.1 SAP S/4HANA upgrades cost assessment

SAP S/4HANA is an enterprise-wide application, with the costs allocated between the three business entities. Costs for SAP S/4HANA are split based on FTE. The current allocation is:

- AGN = 24.57% (AGN SA is 8.66%)
- DBP = 58.86%
- MGN = 16.57%

The cost estimate provided by SAP for the 2029 major upgrade is \$5.0 million. AGN SA allocation based on FTE is 8.66%, or \$0.433 million.

The following tables show the proposed capex and opex uplift over the period.

Table A.1: SAP S/4HANA upgrades, \$'000 January 2025

SAP S/4 HANA	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	-	-	216	216	-	433
Opex (software and services)	116	118	118	118	118	590

Capex includes the review of release changes, activating new features as required by the business, thoroughly testing the changes prior to release, change management, training, and coordination within IT to ensure compatibility with other systems.

There will be an ongoing operating cost associated with maintaining SAP S/4HANA. Historically, our ERP solution (SAP Business One) was hosted on Microsoft Azure services. When the new version of SAP S/4 HANA is implemented, it will shift to the SAP RISE PaaS solution.

The overall subscription cost for SAP RISE, which will host S/4 HANA (among other applications) is \$1,973,846 in 2026 and another \$43,077 on top of that in 2027 repeated in forward years. However, this is offset by a \$650,769 reduction in annual Microsoft Azure costs for hosting S/4 HANA. AGN SA's allocation of the net SAP RISE costs is \$116,000 in 2026/27, increasing to \$118,000 per year for the remainder of the AA period.

A.1.1.2 SAP S/4HANA application enhancements

Building upon the recent successful implementation of SAP S/4HANA in October 2023, AGIG has already recognised the value of ongoing, targeted non-recurrent improvements to further optimise this critical enterprise-wide platform. Consistent with our proactive approach to maximising the benefits of our IT investments, AGIG incurred approximately \$1.5 million across 2024 to implement targeted improvements to SAP S/4HANA, addressing minor post go-live refinements, reflecting an updated procurement policy and unlocking initial opportunities to enhance the user experience and streamline workflows.

Leveraging this initial investment and our commitment to a best-practice SAP lifecycle management approach, we are now actively keeping abreast of the latest SAP roadmaps, versions, releases and features. This proactive engagement ensures that we are well-informed about SAP's future direction and can strategically align potential S/4HANA functionalities with evolving business needs identified. As business stakeholders come to IT with their requirements, we will have a clear understanding of the available SAP capabilities to address them effectively.

Moving forward, we expect the level of required non-recurrent improvements to reduce to a more sustainable level and have therefore budgeted \$1 million per annum across AGIG to strategically unlock future S/4HANA functionalities, such as mobility for an enhanced user experience.

As SAP S/4HANA is an enterprise-wide application, the costs of these non-recurrent improvements are shared across the AGIG entities. Based on FTE allocation, AGN SA's share of this budgeted \$1 million per annum is 8.66% of costs, equating to approximately \$86,600 per annum for targeted S/4HANA improvements that will enhance our South Australian operations. Each potential for S/4HANA functionality to meet a business need as a non-recurrent improvement will be evaluated on a case-by-case basis governed by our two-tier improvement management process outlined in Appendix D to ensure each need is delivered cost-effectively.

A.1.2 SAP SuccessFactors

SuccessFactors is a strategic HR tool that supports AGIG's human capital management needs. Regular maintenance and upgrades are crucial to ensure its effectiveness and compliance with evolving HR regulations.

SuccessFactors, as a SaaS solution, operates on a regular release cycle. This model ensures that customers benefit from continuous innovation, enhanced security, and improved functionality. Failure to adopt timely updates can lead to several negative consequences:

- Security risks: Outdated systems, including SuccessFactors, are more vulnerable to cyber threats
- Compliance issues: Regular Updates include regulatory changes. Not adhering to regulatory changes can result in legal and possible financial penalties
- Functional limitations: Missing out on new features and enhancements can hinder operational efficiency and strategic initiatives
- Vendor support: Delayed upgrades may impact vendor support

SuccessFactors typically releases two updates per year. These updates introduce new features, enhancements, and bug fixes. The release cycle is designed to balance the need for innovation with the stability and reliability of the platform.

Each release includes a mix of mandatory and optional changes:

- Mandatory changes: These changes are essential for maintaining the security and compliance of the platform. They are automatically applied to all customer instances
- Optional changes: These changes offer additional features and functionalities that can be selectively implemented based on specific AGIG needs

By proactively managing SuccessFactors updates, AGIG can ensure optimal performance, security, and compliance, while reaping the benefits of continuous innovation.

A.1.2.1 SAP SuccessFactors - options

The following options have been considered for the SuccessFactors upgrades

- Option 1: Do not upgrade
- Option 2: Proactive half yearly release management

Option 1 is not preferred because the half yearly releases, under a SaaS model, are automatically applied to the AGIG SuccessFactors environments. Mandatory changes will be applied during the SAP SuccessFactors release schedule and not proactively managing these releases is likely to have adverse impact to AGIG employees and HR processes, as well as the risks associated with outdated software.

The preferred approach is Option 2, which is to proactively manage the half yearly releases to ensure they are managed without adverse impact to AGIG and that new features and enhancements are adopted to streamline processes and improve user experience.

A.1.2.2 SAP SuccessFactors – cost assessment

SuccessFactors is an enterprise-wide application, with the costs allocated between the three business entities. Costs for SuccessFactors are split based on FTE. The current allocation is:

- AGN = 24.57% (AGN SA is 8.66%)
- DBP = 58.86%
- MGN = 16.57%

The project costs of proactively managing SuccessFactors half yearly release is a capital cost. Capex includes the review of release changes, activating new features as required by the business, thoroughly testing the changes prior to release, change management, training, and coordination within IT to ensure compatibility with other systems.

The estimate from similar practices at other companies is \$100,000 per release, or \$200,000 each year. AGN SA allocation based on FTEs is 8.66%, or \$17,316 each year.

There will also be an ongoing opex cost associated with maintaining SAP SuccessFactors. Opex includes the software subscription, support contracts, training and maintenance, minus the software subscription costs for retired systems.

The following table shows the proposed expenditure over the period.

Table A.2: SuccessFactors upgrades, \$'000 January 2025

SuccessFactors	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	17	17	17	17	17	87
Opex (software and services)	30	30	30	30	30	152

A.1.3 Public websites

Our high-level Digital Customer Experience Strategy, identifies seven key areas for improvement. The first of these is AGIG website uplift, and it is an immediate priority. Customers make 1/3 of decisions based on Google search, and AGIG has ~0% market share on informational content. It is therefore vital we upgrade/re-platform our website and improve content and accessibility.

We have started the like-for-like upgrade/re-platform of our website this year, and work to improve content and accessibility will continue into the 2026/27 financial year at an estimated cost of \$492,857 for AGIG. We have also planned for a subsequent upgrade in 2028/29 at an estimated cost of \$665,714 for AGIG. AGN SA allocation based on revenue is 16.91%, totalling \$ 195,947 over the next AA period. We are not forecasting additional operating expenditure in relation to our Public Websites.

The following table shows the proposed expenditure over the period.

Table A.3: Public websites upgrades, \$'000 January 2025

Public websites	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	83	-	113	-	-	196

The other six key areas for improvement under our Digital CX Strategy are covered under Digital Experience below.

A.1.4 HSE capability – INX InControl upgrade

AGIG's HSE teams collaborate across the business to support the safe planning and implementation of all AGIG work. Their focus is on occupational health and safety, which includes mental and physical health both in the office and on site, and well as environment issues such as waste minimisation, spill response and emissions reduction.

Currently, the HSE teams at the three businesses, AGN, MGN and DBP, all use different systems to gather and record HSE data.

MGN and AGN use spreadsheets to keep record of incidents. MGN and AGN currently operate in an outsourced business model and the OH&S component is the responsibility of their service provider partners.

The DBP team uses INX InControl, an application that helps organisations record incidents, manage risks, and assign corrective actions. The INX tool has been adequate for DBP until now, but the software is old and implemented on-prem.

In 2027, AGN will insource its business operations from the APA. APA has been using Maximo HSE specific modules, developed a SafeGuard system to front-end Maximo and has also been using Power BI for related reporting.

In summary, across AGIG and including APA, we currently have several isolated solutions that don't share data and don't provide consolidated reporting capabilities. Processes for maintaining spreadsheets is manual and time consuming. Onboarding the APA's Maximo OH&S system will significantly add to the complexities of this landscape.

We therefore need to uplift and standardise our HSE management practices, and make the shift to a single enterprise-wide solution.

A.1.4.1 HSE capability – options

The proposed expenditure during the 2026-31 period is to conduct the detailed analysis of AGIG's requirements and then fully scope **and implement** a suitable HSE application.

The process of technology selection will include a comprehensive assessment of the business needs, vendor solutions and AGIG's relevant existing systems including the APA systems. The study would assess the options for migrating to a latest version of INX (Option 1 outlined below), adoption of the incoming APA solution (Option 2), and implementing a new, fit-for-purpose vendor solution (Option 3). Key considerations will also include assessing if a single enterprise solution could be achievable and if not what alternative combination would work.

We are considering several options to upgrade our HSE systems:

- Option 1 – Continue using existing HSE solutions
- Option 2 – Adopt incoming APA's solution
- Option 3 – Implement a fit-for-purpose HSE solution

Current thinking is that Option 3 is the most likely solution, however, this will be further refined once we have completed our system analysis. Discussion on the proposed options is provided below.

Option 1

While continuing to use spreadsheets is permissible in the short term, these fragmented practices will become increasingly inefficient and difficult to manage once APA operations are integrated into the AGIG businesses. It is not practicable for AGN or MGN to adopt DBP's INX solution, as the application is highly tailored to DBP's transmission pipeline businesses and not suited to a distribution business that carries a significantly different suite of operational risks. We consider there are better applications more suited to distribution and transmission operations that could be implemented enterprise-wide at a comparable cost.

Option 2

Adopting the Maximo-SafeGuard HSE solution from APA might potentially be a pragmatic option considering the size of the APA business operations being insourced in 2027. The AGN SA network is already managed using a Maximo solution, but it is too early to determine whether or not it could also offer any consolidation opportunities, hence the reason for the analysis component of this project.

Adopting a solution without sufficient understanding poses significant risks, including misalignment with business needs, inefficiencies, and unmet objectives. Unknown technical constraints issues could lead to delays, increased costs, or project failure, and non-compliance.

Without a thorough evaluation, we would risk wasting resources and introducing more delays to solving the bigger picture of AGIG HSE needs. A viable alternative would be to adopt a new, fit-for-purpose HSE solution, as per Option 3.

Option 3

Option 3 is currently considered the most prudent option. We would assess the existing INX capability against a few others in the market and adopt a fit for purpose HSE tool. There are several potential tools that would suite our usability, performance, integration, data management, and compliance requirements. These include the likes of Cority and Enablon (both are comprehensive environmental health and safety management software), SAP EHS (part of the SAP suite), Intelex and Sphera (both cloud-based HSE platforms). Each alternative provides enhanced user interfaces, improved data handling, better integration options, and strong compliance features, making them well-suited for modern enterprise needs.

This project will involve costs for conducting a comprehensive assessment of AGIG's broader enterprise needs, developing a HSE tool strategy, and then carrying out a tool evaluation process guided by that strategy and the identified needs. Key steps include defining requirements, evaluating products & vendors, configuring the tool to support business processes, migrating data, and training users. The project will also include system integration and testing to ensure it meets regulatory and operational needs.

We expect to commence this project in 2026, with the aim of implementing an upgraded HSE tool during 2027/28 and migrating data from all three businesses over the remainder of the period.

A.1.4.2 HSE capability – cost assessment

The HSE tool is an enterprise-wide project, with /the costs allocated between the three business entities. Costs are split based on proportion of revenue. The current revenue-based allocation is:

- AGN = 48% (AGN SA is 16.91%)

- DBP = 35%
- MGN = 17%

The total costs (capex and opex) over the 2026-31 AA period across the three entities is estimated at \$1.5 million. Estimated costs of the HSE solution allocated to AGN SA are provided in the table below.

Table A.4: HSE capability tool estimate, \$'000 January 2025

HSE capability	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	73				-	73
Capex (periodic refresh)	-	33	-	33	-	66
Opex (software and services)	17	20	20	27	30	115

Capex includes infrastructure, customisation and labour costs to implement the new system. Cost estimates have been developed based on historical precedent and advice from potential vendors. We have identified a lower and upper estimate for the following project elements:

- Initial assessment and requirements gathering
- Software selection
- Implementation and customisation
- Testing and QA
- Data migration
- Training and change management
- Go-live and support
- Software licensing & potential Infrastructure costs
- Ongoing maintenance and compliance updates

Operating costs include software subscriptions and support contracts, and maintenance.

For the purposes of this forecast, we have used the mid-point for each project element. These costs will be refined further as we commence the assessment and software selection process.

Cost estimates are based on quotes provided by the vendor.

A.1.5 Data archiving

AGIG is currently undergoing a digital transformation to modernise and consolidate its IT systems to better support business needs. As a result of this process, certain business systems are being phased out to reduce technical debt. However, these systems still house important business data that must remain accessible to the business, regulators and customers. Appropriate data archiving is crucial for AGIG to meet data retention requirements and ability to access or report on historical data as/when required. While retention of historical data is a significant Usecase, there is also an emerging need to strategically manage the growing volumes of data across the enterprise through archiving.

AGIG currently does not have data archiving capability in place to meet these requirements. The aim of this project is to establish this capability within AGIG. Data archiving will be leveraged by downstream projects to securely archive data from business systems in preparation for their

decommissioning. The goal is to implement a fit for purpose secure, compliant, and cost-effective data archiving strategy that will enable AGIG to decommission multiple business systems scheduled for retirement between 2026 and 2031, as well as manage the growing data across the Organization.

Data archiving is a critical enabler for decommissioning, as it ensures the preservation of essential data, allowing systems to be retired safely. Data archiving also enables effective management of exponential data growth from digitisation that often leads to unpredictable live data storage costs.

Decommissioning obsolete systems will relieve AGIG from the burden of maintaining outdated, potentially vulnerable legacy systems, which are susceptible to cybersecurity and compliance risks.

If the phased-out systems cannot be decommissioned several key issues of concern arise:

- Security risk – unsupported databases and O/S, inability to apply security patches
- Compliance risk – difficult to meet regulatory requirements, protect data integrity over mandate periods, and respond effectively to audits or legal inquiries
- Financial risk – need to support and maintain licensing and infrastructure, retain organisational resources, training and knowledge transfer to provide support
- Operational risk – solutions no longer supported by vendors, loss of knowledge and capability of supporting applications, obsolete hardware that can no longer be maintained
- Business access risk – data is inaccessible from other production systems, complicates data retention management, uncertainty if application can be recovered from outages

Establishing this data archiving capability is crucial for maintaining regulatory compliance, reducing costs, and ensuring the security and integrity of long-term data. The successful delivery of this project will also lay the foundation for a robust data archiving strategy that supports AGIG's ongoing operational, regulatory, and business needs.

A.1.5.1 Data archiving - options

We considered several options for implementing a data archiving capability across AGIG. In summary, the credible options are:

- Option 1 – Develop custom DIY data archiving solution
- Option 2 – Implement an off-the-shelf data archiving product
- Option 3 – No change to existing situation (do not decommission the redundant applications)

Option 3 is not preferred as it will not address the technical debt issue. Redundant systems maintained as "Read-Only" incur costs on dead assets where supportability may already be an issue posing security and operational risks. It is important that we can decommission the redundant applications and ensure continuity and security of required data.

Option 1 is viable for organisations where specific needs cannot be fully addressed by off-the-shelf products, however a custom solution requires specialist in-house expertise, which AGIG does not currently have. We consider there are off-the-shelf solutions that can fully address AGIG's requirements and would not require substantial in-house customisations. We therefore propose to pursue Option 2.

An off-the-shelf product is considered as the best option by AGIG for several reasons:

- Focus on core business – AGIG can focus the resources on strategic initiatives rather than dedicating significant time and effort to developing and maintaining a custom solution
- Speed of implementation – off-the-shelf products are ready to deploy with minimal customisation, allowing organisations to start archiving data much faster
- Lower risk – off-the-shelf solutions reduce project risks related to scope creep, delays, and unforeseen technical challenges that are common in custom development projects. The predictable nature of these products leads to more successful outcomes
- Lower total cost – off-the-shelf products typically have lower overall costs when considering long-term maintenance, updates, and the need for specialised resources
- Built-in compliance and security – these solutions are designed with industry standards and regulations in mind, offering built-in compliance features and security measures
- Currency – vendors enhance their products, providing updates, new features, and security patches, evolving the systems with changing technology and regulatory landscapes
- Proven reliability – these products are tried and tested in the market, ensuring a high level of reliability and performance. They come with established best practices
- Vendor support – they come with support, including troubleshooting, training, and regular updates, ensuring that your system remains up-to-date and secure
- Scalability and flexibility – off-the-shelf solutions are built to scale and can handle growing data volumes and offer flexible options for expansion
- Ease of integration – they are often equipped with pre-built connectors and APIs for seamless integration with existing systems, saving time and reducing complexity

In summary, an off-the-shelf data archiving product is better because it offers quick deployment, proven reliability, and lower total costs.

A.1.5.2 Data archiving cost estimate

The data archiving project is an enterprise-wide project, with costs allocated between the three business entities. Costs are split based on proportion of revenue. The current revenue-based allocation is:

- AGN = 48% (AGN SA is 16.91%)
- DBP = 35%
- MGN = 17%

The total project capex across the three entities is estimated at \$1.46 million. The AGN SA allocation is provided in the table below.

Table A.5: Data archiving solution estimate, \$'000 January 2025

Data archiving	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	147	-	-			147
Capex (periodic refresh)	-	-	-	40	59	99
Opex (software and services)	13	13	13	13	13	63

Capex includes infrastructure, licencing fees, customisation and labour costs to implement the new system. Costs are derived from advice from potential vendors, and includes consideration of cloud vs on premises costs, with an on-premises solution currently the preferred option.

Operating costs include software subscriptions and support contracts, training and maintenance.

A.1.6 Digital experience

During the current AA period, AGN implemented a customer relationship management (CRM) solution across its gas distribution network businesses (AGN and MGN). As per the business case SA137 - Digital Customer Experience, we have implemented a flexible CRM with foundational functionality. The project was a success and we can now offer our customers a contemporary experience that is comparable with other gas distribution businesses.

Now the CRM has been established, the application has entered the maintenance and enhancements phase. We must invest in our CRM to ensure it remains current (and secure) while implementing enhancements to improve the solution and ensure it is providing our customers the service they expect. Our strategy for the next AA period is to make relatively small investments in incremental improvements to our CRM. Our aim is not to establish a best in-class CRM in line with those offered by electricity networks, rather we want to keep our online offering in line with other Australian gas network businesses.

For example, Jemena Gas Networks currently offers a self-service portal whereby customers can see the status of bills, payments, connections and disconnection services. This ability to self-serve and have visibility of connection status is a feature our customers have said would be valuable to them and is a basic level of service they expect from their utility provider. We believe this is particularly important in the current environment where customers are both switching to and away from gas.

While the specific detail of CRM enhancements is not yet defined, we have developed a high level Digital CX Strategy, which identifies seven key areas for improvement:

1. AGIG website uplift
2. Digital marketing / engagement
3. Appliance sales website
4. Customer portal
5. Calculators / comparison tools
6. Trades market place
7. Trade hub

The first is outlined above under Public Websites.

The remaining six initiatives form part of our ongoing CRM enhancement strategy, and are currently in the discovery stage. Current focus is on building bill comparison and appliance selector tools, improving customers' self-serve capabilities, and making business-to-business communications easier. These enhancements are relatively low cost and can be delivered via customisation and/or additional module provided by the vendor.

Our plan over the coming AA period is to test these initiatives with customers and make incremental improvements to our current digital offering across AGN and MGN. As such, at the

time of developing this business case there is no detailed specification or schedule for improvements. We therefore propose to include an allocation for ongoing enhancements to the CRM and broader digital customer experience throughout the period, driven by business need and customers' communication preferences.

We estimate total capital investment of approximately \$4.8 million over the next five years, to be allocated between the AGN and MGN businesses based on the number of customers on each network. AGN SA's share on this basis is 23.06%.

We also expect there will be an associated operating cost uplift for cloud subscriptions, support and training.

Table A.6: Digital customer experience estimate, \$'000 January 2025

Digital customer experience	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	248	192	213	232	225	1,110
Opex (software and services)	46	48	52	57	74	277

A.1.7 Contract management system

AGIG's Contracts and Procurements business unit currently manage contracts using email, Excel spreadsheets, Adobe Sign, and network drives. This fragmented approach is inefficient, increases risk of errors and does not provide centralised oversight of all contracts. A 2023 internal audit identified weaknesses in controls over procurement and contractor/vendor management, and flagged the lack of a robust contract management system to be a significant risk. The audit found that controls on procurement for operating expenditure are acceptable, but with major improvements required in the following areas:

- Compliances with procurement procedures
- Performance of formal price comparison before renewal of contracts
- Review of dollar threshold on the requirements of tender process and request for proposal
- Inspection of insurance policies from contractors
- Maintenance of document execution checklists
- Managing existing vendors and new vendor registration process
- Reconciliation of unit costs in purchase order against the schedule of rates in contracts

A key recommendation resulting from the audit is to implement an end-to-end digitised contract management system, for use across the AGIG entities. Such a system is expected to provide the following benefits:

- Reduce risk by digitising the contract management process
- Provide end-to-end visibility of all contracts in a single system
- Strengthen controls and governance over procurement and vendor management
- Improve the effectiveness of the review and approval processes
- Effective management through ability to monitor vendor and contract performance
- Improved decision making through improved data and reporting

A range of off-the-shelf contract management applications are available, such as SAP Ariba, Coupa, Oracle, Zycus and several others. Many of these applications offer similar core features, with a range of functionalities that can be tailored to suite an organisations' needs. This can make it challenging to identify the most appropriate solution, particularly for a large multi-faceted business such as AGIG.

A key consideration for AGIG is integration with SAP S/4HANA. The enterprise is currently in the process of moving all its business entities onto this single ERP application, with MGN, AGN and DBP all expected to be operating on the same platform by the end of 2026. To ensure any new contract management system is optimised for AGIG's requirements and can be integrated with SAP S/4HANA, we propose to undertake a detailed analysis of our IT environment, technical requirements and business needs before committing to a contract management solution.

We therefore propose to commence design and implementation of an enterprise contract management solution from 2026/27 onwards, once the business has fully transitioned to SAP S/4HANA. Our plan is to implement a new system across all three entities by the end of 2028.

Detailed scoping and costing of the new contract management system has not yet been conducted. The discovery and design phase is expected to commence during 2026 and will include:

- Analysis of the market landscape for a best-fit solution by defining and prioritising use cases
- Prioritising organisational must-haves over nice-to-haves, formalising scope such as contract digitisation, storage, AI and data handling
- Reviewing organisational application and infrastructure architecture to identify opportunities for efficiencies, as well as potential barriers
- Ensuring AGIG's contract management processes can evolve by reviewing vendors' future roadmaps
- Workflow mapping and maturity assessment of departments that will use the new system
- Change management requirements and decommissioning effort
- Cost comparison and high level benefits analysis

This analysis will then directly inform the application design and implementation of the new contract management asset.

For the purpose of this forecast, we have conducted an initial desktop study of the potential costs of a new contract management system, supported by preliminary conversations with potential vendors. Current thinking leans towards SAP integrated platforms such as Ariba, we have therefore developed an estimate based on the potential cost of implementing SAP Ariba.

Discovery and design, implementation, delivery and migration of data is estimated at \$4.6 million. This includes three years of licensing costs.

We expect the new solution would be provided as a SaaS solution. Ongoing licencing costs from 2026/27 onwards would be expensed and are estimated at \$150,000 per annum.

These costs will be allocated between the three entities based on revenue, of which AGN SA's allocation is 16.91%.

Table A.7: Contract management system cost estimate, \$'000 January 2025

Contract management system	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	423	186	169	-	-	778
Opex (software and services)	25	25	25	25	25	127

A.1.8 Data, analytics and visualisation

Background

In 2024, AGIG implemented a new data analytic and visualisation (DAV) tool, as part of an enterprise-wide data architecture, reporting and governance program. DAV tools are software applications that help in analysing and interpreting complex datasets to extract meaningful insights. These tools also enable users to create visual representations of data, such as graphs, charts, and dashboards, to make the data easier to understand and communicate. Until recently, AGIG had an abundance of data, but scarce information and analysis. The DAV tool has been rolled out to the businesses and has begun to be used by AGN SA.

The value of the AGIG DAV platform is to drive a common language for data (as well as the understanding of data flows) across AGIG. Centrally accessible, secure, and reliable data sets can be for:

- Compliance and business critical reporting – fragmented, disparate and inconsistent reporting due to unreliable information and manual manipulation, making it difficult to be transparent with our regulators, customers and internal business stakeholders
- Better decision making – ensuring simple access to quality information in a timely manner (i.e. the right information in the right format at the right time to the right person) supports good decision making
- Efficiency through streamlining business processes – standardising and centralising analytics from systems (i.e. OneERP) and improving and automating more of our reporting and analytics, will create synergies across AGIG. It will reduce duplication of effort and allow less time to be spent collecting, collating and manually calculating information to support business decisions, and enable more time undertaking value-add analysis activities
- Cyber risk management – cyber controls, such as identity and access controls, are only effective when the controlled data is appropriately governed and managed

The DAV offers user the ability to connect various data sources, customise visualisations, create dashboards and stories, and share analysis in a meaningful way. Its uses are versatile, and it can be applied to a range of data such as regulatory information notice (RIN) reporting, asset condition information, and financial reporting.

Opportunity for enhancements

Given the system is relatively new to our business, there is scope for significant enhancements as the business gets used to using the tool and identifies where it can be applied. Within the year of operation, the IT department has received a large number of requests from users to enhance the DAV tool and enquiries on alternative use cases.

While we will not necessarily adopt every enhancement requested by the business, there are opportunities to incorporate additional functionality into the DAV tool such as artificial

intelligence and machine learning. As a minimum, we plan to expand the breadth of on-prem and cloud apps based reporting and to introduce a data governance tool and an infographic utility. We will also allocate funding for continuous delivery and improvements of data management practices over the period.

We therefore estimate total capex of \$2.7 million on DAV enhancements over the 2026-31 AA period. These costs will be allocated across the three entities based on revenue split. AGN SA's allocation is therefore 16.91%.

Table A.8: DAV system enhancements, \$'000 January 2025

DAV enhancements	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	61	115	101	92	93	462
Opex (software and service)	21	24	24	35	42	147

The DAV cost estimate is based on historical actuals for enhancements, early assessment of the DAV user requests already received, and high level estimates from the vendor on the data governance and infographic enhancements.

Capex includes project delivery, implementation of the data governance and infographic tools, and initial subscription costs. Opex covers ongoing Microsoft Azure subscription and support.

A.1.9 Protecht GRC application

Currently at AGIG, several teams use Protecht, a legacy web-based governance, risk and compliance (GRC) tool. Our Assurance and Risk teams find the tool not fit for purpose and difficult to use, while some teams, such as IT Commercial and IT Service Desk, have already stopped using it for related reasons.

Over time, the tool has been heavily customised and AGIG has lost the internal technical expertise needed to maintain it effectively. While the vendor provides stop-gap technical support, this arrangement does not allow for functionality enhancements and additional use cases. The business is increasingly concerned about the risk of the tool becoming inoperable.

AGIG pays approximately \$100,000 annually in licensing and technical support for about 70 users. The aim of this project is to implement a suitable upgrade or replacement to the current Protecht GRC tool that can be used across AGIG.

A.1.9.1 Protecht GRC – options

We considered several options to for addressing the issues with our GRC system, including maintaining Protecht as is, or upgrading to a newer version of the same application. However, it is clear there is limited value in maintaining use of a system that our users have made clear is no longer fit for purpose.

We therefore consider the most prudent option is to upgrade to a new, fit for purpose GRC tool from a different software provider. There are several options on the market, which we are currently looking into. The application will most likely be cloud-based, as there are very few on-premises solutions offered by vendors.

A.1.9.2 Protecht GRC – cost assessment

The new GRC tool will be an enterprise-wide application, with the costs allocated between the three business entities. Costs are split based on proportion of revenue. The current revenue-based allocation is:

- AGN = 48% (AGN SA is 16.91%)
- DBP = 35%
- MGN = 17%

The estimated total cost of the new GRC solution is \$1.8 million. The AGN SA allocation is provided in the following table.

Table A.9: GRC tool estimate, \$'000 January 2025

Protecht	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	120	-				120
Capex (periodic refresh)			57	-	54	111
Opex (software and services)	34	34	37	37	41	183

Capital costs include implementation, project management, initial licencing for the additional module, customisation, and integration. Opex includes ongoing software subscriptions, support and training.

Opex includes the software subscription, support contracts, training and maintenance.

Cost estimates have been developed based on historical precedent and advice from potential vendors.

A.1.10 Application architecture management system

The objective of this project is to upgrade our enterprise application management practices by implementing an application architecture management system within AGIG. This strategic initiative aims to align our IT infrastructure with business goals, optimise operational efficiency, strengthen our compliance and IT security posture, and enhance our ability to quickly adapt to market changes and regulatory demands.

The current AGIG IT landscape is characterised by fragmented systems and a need for more cohesive alignment with our business strategies. This leads to inefficiencies and missed opportunities for innovation and improvement. Implementing an application architecture tool will enable us to construct a single-source-of-truth blueprint of our IT architecture, ensuring that it supports and drives our business objectives efficiently.

AGIG, as a utility organisation, faces a unique set of IT challenges due to the critical nature of its services, regulatory demands, and the need for constant availability and reliability. Key IT challenges include:

- Cyber security threats – Utilities are high-value targets for cyberattacks due to the critical infrastructure they control, which includes transmission and distribution systems. Ensuring the security of IT and operational technology (OT) systems against threats is a paramount concern. This involves protecting against both external attacks and internal vulnerabilities

- Regulatory compliance – Utility companies are among the heavily regulated industries. They must comply with regulations concerning data protection, operational security, and reporting standards. Managing compliance, particularly across different states with varying requirements, adds complexity to IT management
- Customer service and engagement – Modern customers expect digital, seamless, and personalised service interactions. Utilities must provide reliable online services for billing, outage reporting, and real-time customer support, which demands high IT system availability and integration
- Ageing IT (and other) infrastructure – Utilities must manage outdated IT systems and infrastructure that are vulnerable to failures and security breaches. Upgrading these systems while maintaining continuous service availability presents a significant challenge
- Integration of renewable energy sources – As the energy sector moves towards renewable sources, like increasing use of hydrogen, utilities need to integrate these new technologies into their grids. This integration requires advanced IT solutions to manage variable factors like flows and pressure and maintain grid stability
- Smart grid technologies – Implementing smart grid technologies involves the deployment of advanced metering infrastructure, smart sensors, and IoT devices. Managing the data from these devices, ensuring their security, and integrating them into existing systems poses significant IT challenges
- Data management and analytics – Utilities generate vast amounts of data from sensors, meters, and customers. Effectively managing, storing, and analysing this data to improve operational efficiency and customer service requires robust IT infrastructure and advanced analytics capabilities
- Operational efficiency – There is a constant pressure to improve operational efficiency and reduce costs. IT systems must support process optimisation, resource management, and automation, all while minimising downtime and service disruptions
- Disaster recovery and business continuity – Given their critical role in infrastructure, utility companies must have strong disaster recovery and business continuity plans. This involves maintaining IT systems that can withstand or quickly recover from disruptions caused by natural disasters, system failures, or cyberattacks
- Talent acquisition and retention – The rapid pace of technological advancements requires skilled IT professionals, and partners who are proficient in the latest technologies and security practices. Finding and retaining this talent is an ongoing challenge

Addressing these challenges requires a strategic approach to IT management, investment in modern technology solutions, and continuous improvement of cyber security practices.

Implementing better application architecture management would offer a number of benefits for AGIG including support for APA transition, enhancing cyber security risk and compliance management, IT decision-making, and alignment IT with business objectives. Application architecture can also provide continuous insights into how IT architectures can adapt to changing business needs. A summary of benefits for AGIG is provided below:

- Enhanced decision-making – By providing comprehensive insights into the IT environment, application architecture tools enable better decision-making at both strategic and operational levels. Stakeholders can assess the impact of proposed changes, evaluate alternatives, and prioritise initiatives based on their alignment with business goals
- Risk management and compliance – Application architecture tools provide a framework for assessing and managing risks associated with IT systems and processes, including Cyber Security and regulatory compliance. By identifying vulnerabilities, ensuring compliance with regulations and standards, and implementing robust governance practices, organisations can mitigate risks and enhance security posture
- Improved visibility and transparency – Application architecture tools provide a centralised platform for documenting and visualising the entire IT landscape, including applications, infrastructure, data, and processes. This enhanced visibility allows stakeholders to understand the relationships between different components and make informed decisions
- Support for digital transformation – As AGIG is driving ERP, CRM and other digital transformation, application architecture tools will play a crucial role in modernising IT infrastructure, integrating new technologies, and aligning IT with business strategy. EAM tools provide the visibility and governance needed to drive successful digital initiatives
- Efficient use of IT resources – Application architecture tools help identify redundant systems, overlaps, and opportunities for consolidation. This can lead to cost savings and more efficient use of IT resources
- Facilitated communication and collaboration – Application architecture tools promote collaboration among different stakeholders, including IT teams, business units, and external partners. By providing a common platform for architecture communication, surveys and documentation, these tools foster cross-functional collaboration and engagement
- Restructuring and expansion – Application architecture tools can offer scalability and flexibility to support AGIG's growth and restructuring, including the upcoming AGN transition and its complexities

A.1.10.1 Application architecture management system - options

We considered several options for implementing an application architecture solution. In summary, the credible options are:

- Option 1 – Develop custom in-house solution
- Option 2 – Implement a commercial tool
- Option 3 – No change to existing manual processes

We eliminated Option 3, as it is clear that the existing manual processes should not continue, particularly given the ongoing AGIG-wide implementation of a single enterprise resource planning application (SAP S/4HANA). The SAP S/4HANA implementation offers a window of opportunity to standardise other applications across AGIG, therefore it makes sense to implement an enterprise-wide application architecture tool that is compatible with SAP S/4HANA.

With this in mind, we have selected Option 2 as the most viable solution. There are a number of 'off-the-shelf' tools that could be adopted at a lower cost than developing a custom in-house solution. Products such as SAP's LeanIX can be tailored to meet DBP, AGN and MGN's

requirements, offering a single application architecture management solution across all three organisations that can also integrate with SAP S/4HANA.

A.1.10.2 Application architecture management system – cost assessment

The Application architecture tool is an enterprise-wide project, with the costs allocated between the three business entities AGN, DBP and MGN. Costs are split based on proportion of revenue. The current revenue-based allocation is:

- AGN = 48% (AGN SA is 16.91%)
- DBP = 35%
- MGN = 17%

The total cost across the three entities is estimated at \$0.2 million. AGN SA's allocation is shown in the table below

Table A.10: Application architecture estimate, \$'000 January 2025

Application architecture	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	26					26
Capex (periodic refresh)		28	28	24	21	102
Opex (software and services)	10	13	19	21	22	85

Costs are derived from quotes provided by the potential vendors. The most likely solution to be implemented is SAP's LeanIX. The preferred solution will be implemented by a third-party contractor, who has provided cost estimates for onboarding, development and support costs for a LeanIX solution.

Operating costs include software subscriptions and support contracts, training and maintenance.

A.1.11 Project portfolio management software

AGIG's project management needs are diverse. Across our three business entities projects range from construction and engineering to IT implementation and real estate management. While our project management capabilities have been adequate to date, there is no unified approach or IT solution to support project and portfolio management across the group. This means project delivery, reporting, close out and analysis can vary across AGN, DBP, and MGN.

Project portfolio management (PPM) software offers a range of benefits, including improved project scheduling, enhanced collaboration, more transparent cost tracking and the opportunity for more efficient deployment of resources. By providing the AGIG businesses a consistent and shared suite of tools, we can improve our portfolio management and make data-driven decisions, which will ultimately allow better cost management and more accurate forecasting.

We therefore propose to introduce enterprise-wide portfolio and project management software. Given the variety of projects and depth of our portfolio, we are looking to implement two PPM tools: Primavera and Altus.

Both Primavera and Altus are powerful project management applications, which offer different yet complementary PPM tools. Primavera is more specialised for construction and engineering, and is suited to operational projects across our transmission and distribution businesses. Altus

is more suited to property and general project management, and will be used for managing our property portfolio and IT/commercial projects. Both solutions integrate well with SAP products.

A.1.11.1 PPM – cost assessment

We plan to implement Primavera and Altus during 2026/27, at a capital cost of approximately \$1.6 million. Annual ongoing subscription fees for the software services will be incurred from 2027/28 onwards, at an estimate \$10,000 per year.

The PPM tools will be used by approximately 100 users across DBP, AGN and MGN. Costs will therefore be split based on user count, of which AGN's allocation is 7.53%.

The AGN SA allocation provided in the following table.

Table A.11: PPM software estimate, \$'000 January 2025

PPM software	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	63	59	-	-	-	122
Opex (software and services)	9	9	9	9	9	45

Capex includes software, licencing fees, customisation and labour costs to implement the new PPM tools.

Opex includes the software subscription, support contracts, training and maintenance.

Cost estimates have been developed based on historical precedent and advice from vendors.

A.1.12 GTreasury

GTreasury is a cloud-based treasury management system used by our AGIG finance teams to manage cash, risk and payments. It includes several key tools used to manage our cash positions, forecasting, debt management and investment portfolios. GTreasury is used exclusively by our finance/treasury teams, and is an AGN-owned application.

GTreasury is due for upgrade in 2026/27. The upgrade offers an improved payments module and integration with SAP and our data, analytics and visualisation dashboard. We expect this will be a two-year implementation project, to be completed by the end of 2027/28.

A.1.12.1 GTreasury cost estimate

GTreasury is owned by AGN and used by the central finance team. Cost are therefore allocated between the AGN network businesses (Victoria, SA, QLD), with AGN SA's allocation being 35.24%.

The total project capex is estimated at \$0.7 million. The AGN SA allocation is provided in the table below.

Table A.12: GTreasury estimate, \$'000 January 2025

GTreasury	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex (project delivery)	177	-	-	71	-	248
Opex (software and services)	81	81	81	88	88	419

Appendix B Comparison of risk assessments

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

Option 1	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Low	Low	

Option 2	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Low	Low	

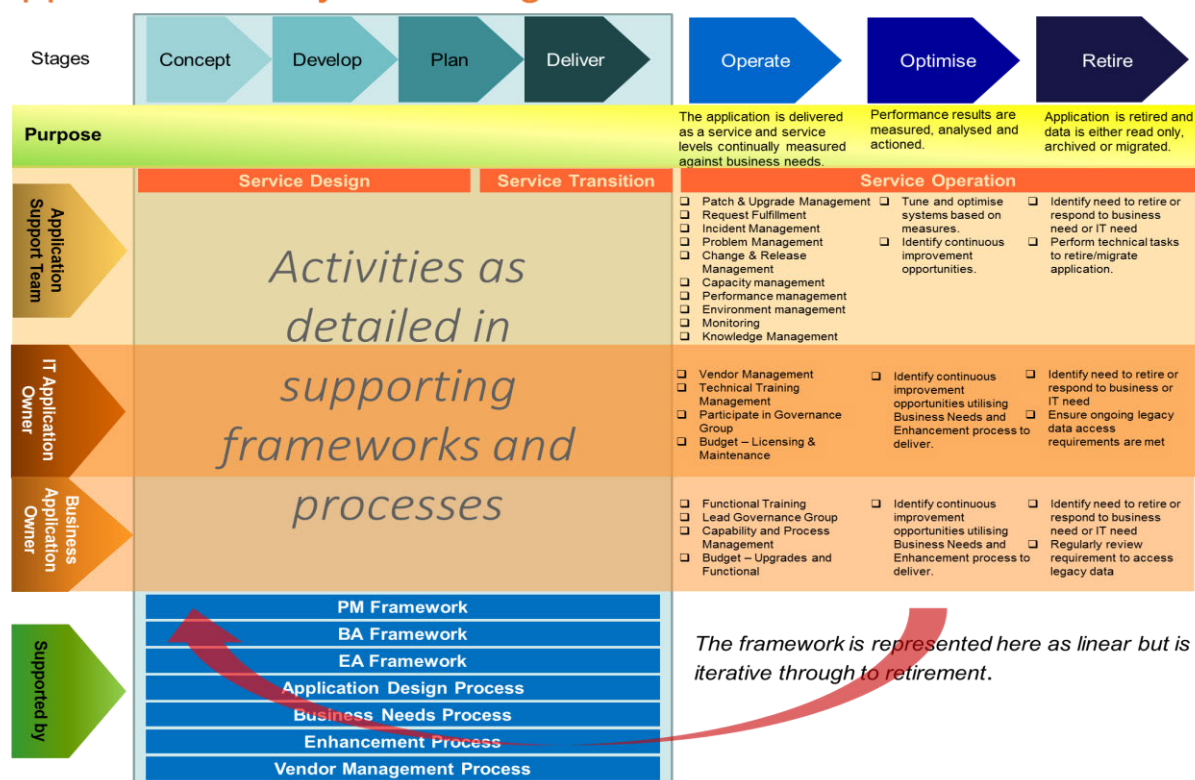
Option 3	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Low	Low	

Appendix C Application lifecycle management

We follow an industry standard application lifecycle framework to manage applications through the implementation, operations, optimisation and retirement phases of their lifecycle to determine upgrade timelines and priorities. This framework provides an efficient and effective approach to maintaining the security and stability of our applications while optimising lifecycle stages. This framework includes the project management methodologies to implement the applications, and ongoing lifecycle activities to operate and optimise the applications - including upgrade cycles.

The diagram below outlines the key aspects of this framework.

Application Lifecycle Management Framework

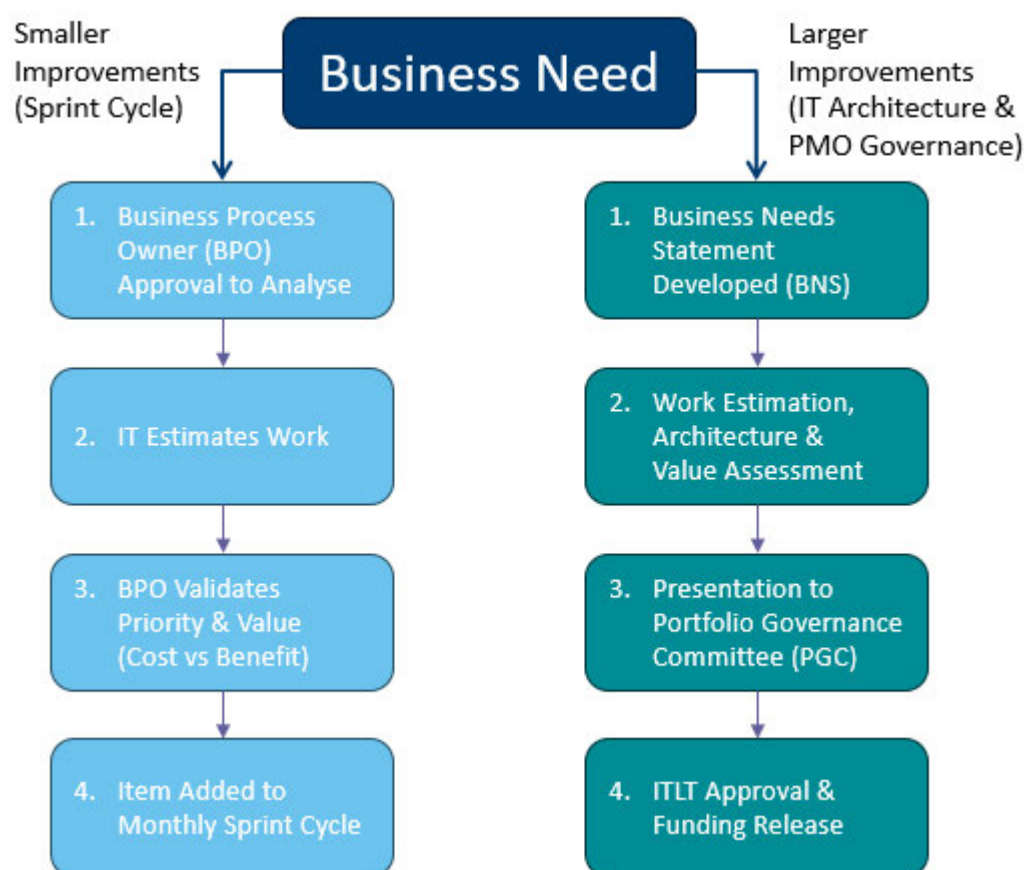


Appendix D Improvement management process

AGIG employs a dual-path improvement management process.

- Smaller items are via the AGIG Business Process Owner approval and monthly sprints, focusing on rapid delivery of business needs
- Larger, strategic implementations & improvements undergo IT PMO governance, requiring a Business Needs Statement and ITLT approval for funding

This ensures both agility and strategic alignment, prioritising improvements with clear business value, and is outlined in the following diagram.



Note: AGIG is investing in the development of SAP internal expertise to reduce reliance on external vendors to deliver minor improvements and manage increasing costs from vendors.

SA239 – IT sustaining infrastructure

1.1 Project approvals

Table 0.1: SA239 IT sustaining infrastructure – Project approvals

Prepared by	Dan Hayward – Head of Infrastructure & Support
Reviewed by	Brooke Palmer – Head of IT Business Engagement
Approved by	Brett Miller – Chief Information Officer

1.2 Project overview

Table 0.2: SA239 IT sustaining infrastructure – Project overview

Description of problem /opportunity	<p>The investment proposed in this business case is driven by the ongoing need to maintain the existing levels of service to our customers while mitigating the risks of service interruptions, cyber security breaches and degraded performance due to the use of Information Technology (IT) infrastructure beyond its useful life. Our key objective is to ensure that Australian Gas Networks (AGN) in South Australia (SA) continues to maintain reliable, secure, compliant and efficient business processes, systems and services while keeping the risk of service interruptions, cyber breaches and system performance at an acceptable level.</p> <p>Our IT infrastructure underpins the delivery of all AGN services; it enables our staff to connect to our systems, data and communication networks; it also allows us to securely store, search, and process the large volumes of data we need to service our customers and to meet a range of legal and regulatory obligations, including those prescribed in the National Gas Rules (NGR).</p> <p>Many IT infrastructure components will reach the end of their useful life during the next five-year period. This business case considers the upgrade or replacement of these components over the period as part of the end user devices, and network and currency workstreams.</p> <p>There is also a need to ensure that our infrastructure is hosted in a way that is cost efficient and fit for purpose in the long term. There is an opportunity to leverage the industry trend of moving from company-owned infrastructure to cloud-based infrastructure hosting, which is assessed in this business case against the base-case of maintaining the existing on-premise data centre solution.</p> <p>If this program of work is not completed, AGN's critical business systems will be exposed to high risks of cyber security breaches, compromised customer, employee and/or corporate data, prolonged outages and poor IT system performance. This would adversely affect the safety and integrity of our services and could result in AGN failing to fulfil its customer and regulatory obligations under the NGR and other legislative and regulatory instruments.</p>
Untreated risk	As per risk matrix = High
Options considered	<p>Options were considered separately for each workstream in the program:</p> <p>End user devices:</p>

- **Option 1: Vendor-recommended refresh** – Proactively replace end user devices in line with vendor-recommended lifecycles (\$1.2 million capex)
- **Option 2: Conservative refresh** – Refresh the end user devices on a schedule that has been extended compared to the vendor-recommended lifecycles where it is prudent to do so (\$1.0 million capex)

Network and currency:

- **Option 1: AGN-centric approach to infrastructure refresh** – Do nothing more to consolidate the AGN infrastructure into the shared AGIG environment and only upgrade those AGN infrastructure components that are running out of support in the next period (\$2.2 million capex)
- **Option 2: 'AGIG One IT' approach to infrastructure refresh** – Finalise the transition to the shared AGIG infrastructure environment and upgrade the AGN part of the shared infrastructure in accordance with the 'AGIG One IT' Strategy & Roadmap, taking advantage of the economies of scale brought about by the shared services model (\$2.1 million capex)

Data centre:

- **Option 1: BAU** – Continue to refresh data centre infrastructure assets in our on-premise data centre (\$0.4 million capex)
- **Option 2: 'Organic' transition to cloud** – Transition our data centre infrastructure to cloud in an orderly manner as our existing on-premise data centre components run out of support (\$0.1 million capex plus \$0.2 million opex uplift)
- **Option 3: 'Big Bang' transition to cloud** – Migrate all of data centre infrastructure to the cloud at once (\$0.2 million capex plus \$0.2 million opex uplift)

Proposed solution

1. **End user devices:** Option 2 is recommended as the most cost-effective way to refresh our end user devices while keeping the risks associated with outdated or unsupported devices at an acceptable level. While Option 1 would reduce these risks even further, following vendor-recommended approach without attempting to extend the life of devices via good management practices does not represent a prudent level of expenditure.
2. **Network and currency:** Option 2 is recommended as it represents the most cost-effective option of maintaining the current levels of service enabled by our networking infrastructure and software. Option 1 is more expensive than Option 2 because it does not invest into any further consolidation of the AGN infrastructure after the current period and therefore isn't able to take advantage of the consolidation, most notably the consolidation of our Active Directory (AD) that is part of the 'AGIG One IT' roadmap.
3. **Data Centre:** Option 2 is recommended as the most cost-effective long-term solution for our data centre, when assessed on the total expenditure (totex) basis.

Estimated cost

The forecast direct capex (excluding overheads) during the next five-year period (July 2026 to June 2031) is \$3.2 million.

\$'000 Jan 2025	26/27	27/28	28/29	29/30	30/31	Total
End User Devices	411	156	156	156	156	1,037
Network and currency	648	382	326	465	230	2,051
Data Centre	52	14	14	20	14	115
Total	1,112	552	497	641	400	3,203

The forecast opex uplift (excluding overheads) during the next five-year period is \$0.2 million.

\$'000 Jan 2025	26/27	27/28	28/29	29/30	30/31	Total
-----------------	-------	-------	-------	-------	-------	-------

Data Centre	33	38	49	58	62	239
All costs in this business case are expressed in real unescalated dollars at January 2025 unless otherwise stated.						
As per risk matrix = Moderate						
<p>This project aligns with the <i>Customer Focussed</i> aspect of our vision by ensuring that our technology platforms and office equipment are adequately maintained and available to maintain our services in a manner that meets the needs of our customers.</p> <p>This project aligns with our vision objective of being <i>A Leading Employer</i>, as it aims to provide employees with current, reliable, high performing and fit-for-purpose technology solutions that allow the business to operate effectively.</p> <p>This project aligns with our vision to of <i>Operational Excellence</i> as it is driven by a lifecycle management framework that follows good industry practice, mitigates risks, optimises capital and operational expenditure, and minimises infrastructure support costs.</p>						
<p>NGR 79(1)/91 – The proposed proactive IT sustaining infrastructure initiatives are consistent with accepted good industry practice in terms of the timing of asset renewals, several alternative options have been considered and unit rates and timing of refreshes have been tested to achieve the lowest sustainable cost of delivering pipeline services.</p> <p>NGR 79(2) – The proposed expenditure on our IT sustaining infrastructure project is required to maintain the integrity of services through current, supported and fit for purpose IT infrastructure, managing technology risks and preventing material outages or deteriorating performance which can come from ageing infrastructure. The proposed capex is justifiable under NGR 79(2)(c) as it is necessary to:</p> <ul style="list-style-type: none"> • Maintain and improve the safety of services (NGR 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 (NGR 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 • Comply with a regulatory obligation or requirement (NGR 79(2)(c)(iii)) - the proactive lifecycle management of IT infrastructure mitigates the risk of a breach of regulatory obligations (<i>Security of Critical Infrastructure Act, Privacy Act</i> and gas market reporting that need timely access to information for regulatory reporting), which may eventuate if the systems residing on IT infrastructure were not available or are compromised <p>NGR 74 – The forecast costs are based on the latest market rate testing, and project options consider the requirements of our IT infrastructure environment. Cost assessments have been conducted for each option based on the best information available at the time of developing this business case. The infrastructure renewal options have been based on service provider recommendations and assessed by AGIG's IT specialists. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.</p>						
Customers consistently ranked price and affordability as their top priority. They also told us that they place a great deal of importance on safety and reliability						

**Other relevant
documents**

of supply. Customers were clear they expect good communication and simple service that is resolution-focussed. Customers agreed that supplying cleaner energy was important, but that affordability is a key consideration for them.

Our IT sustaining infrastructure program is necessary to ensure the ongoing stability, integrity and security of our technology environment at an affordable level. This is critical for the safety and reliability of our services and our ability to provide the levels of service that our customers expect and value.

This business case should be read in conjunction with:

- Attachment 9.3: Asset Management Plan
- Attachment 9.6: Procurement Policy and Procedure
- Attachment 9.7: IT Investment Plan
- Attachment 9.11: Risk Management Framework
- AGIG 'One IT' Strategy & Roadmap
- Capitalisation Policy
- Business case SA217: IT operational applications
- Business case SA238: IT corporate applications
- Business case SA240: Cyber security

1.3 Background

Information Technology (IT) infrastructure is critical to ensuring our staff can be connected to our systems, data and communication networks reliably, efficiently and securely, irrespective of whether they are working in a corporate office, from home, at one of our remote locations, or while travelling from one site to another. It also allows us to securely store, search, and process the large volumes of data we need to service our customers and to meet a range of legal and regulatory obligations, including those prescribed in the NGR.

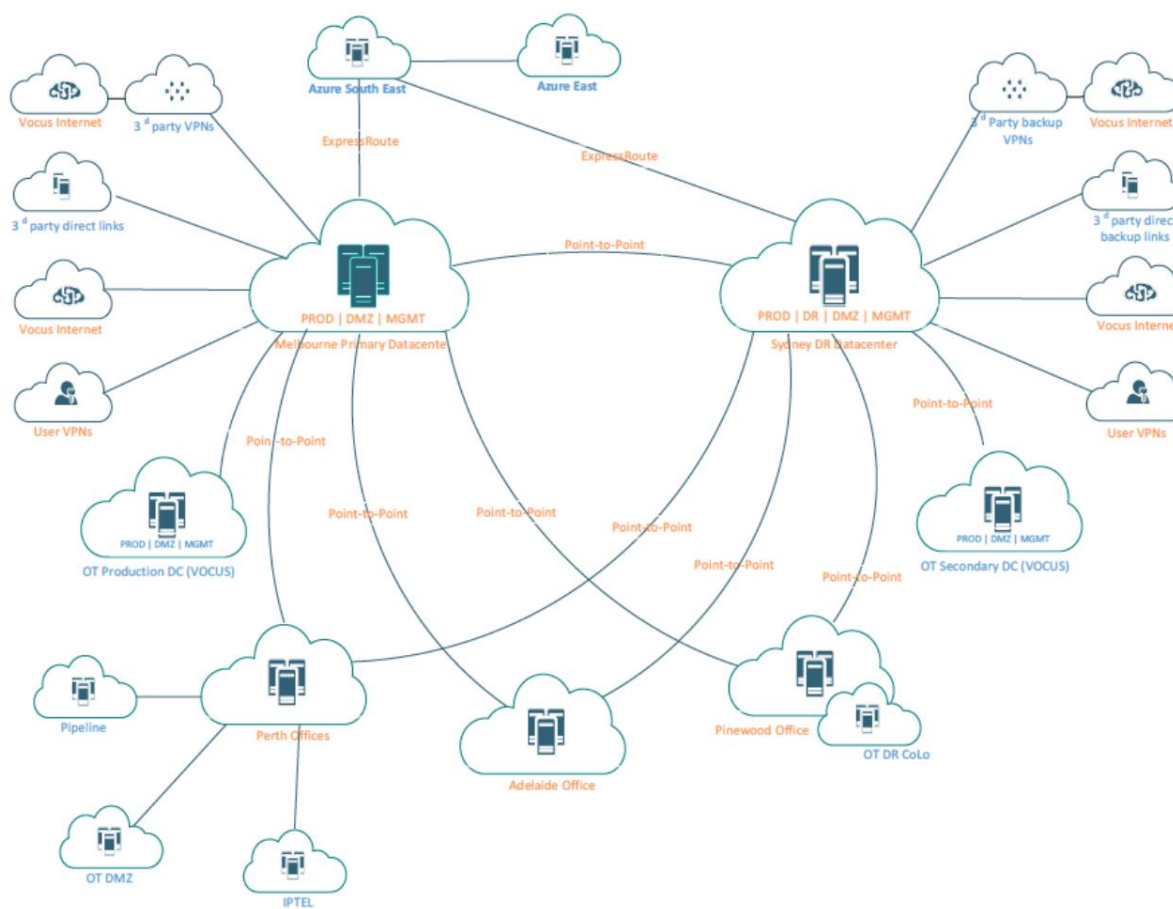
Our IT infrastructure assets include end user devices such as laptops, mobile phones and office computer equipment as well as the networking and data centre equipment that underpin all our communications, information storage and processing.

1.3.1 AGN's IT infrastructure environment

AGN is part of the Australian Gas Infrastructure Group (AGIG), which also includes the Dampier to Bunbury transmission pipeline (DBP) and Multinet Gas Networks (MGN).

Figure 0.1 shows the AGIG technology infrastructure environment and network layout that connects all AGIG offices, including the AGN locations.

Figure 0.1: AGIG Technology Infrastructure environment



1.3.1.1 Transition to shared AGIG IT infrastructure

In late 2019, AGIG launched its 'AGIG One IT' Strategy & Roadmap² with the aim of consolidating disparate technology environments and leveraging economies of scale across the group. One of the challenges of implementing a group-wide strategy for AGIG has been that its business entities operate across multiple Australian jurisdictions and have overlapping regulatory periods (see Figure 0.2), with AGN and MGN regulated by the Australian Energy Regulator (AER) and DBP regulated by the Economic Regulation Authority (ERA).

Figure 0.2: Access arrangement periods for AGIG entities

	2021		2022		2023		2024		2025		2026		2027		2028		2029		2030		2031	
	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2	H1	H2
DBP	AA5 (2021-25)										AA6 (2026-30)											
AGN SA & other	AA 2021/22-2025/2026										AA 2026/27-2030/31											
AGN Victoria & Albury	AA 2023/24-2027/28										AA 2028/29-2032/33											
MGN	AA 2023/24-2027/28										AA 2028/29-2032/33											

The 'AGIG One IT' Strategy & Roadmap served as a supporting document for the AGN South Australia AA 2021/22-2025/2026, AGN Victoria and Albury AA 2023/24-2027/28 and MGN AA 2023/24-2027/28 submissions. The AER favourably assessed the proposed program and included capex allowances in its final determinations noting that:

- *"The scope of the proposed work, and the approach of using an independent expert to develop cost estimates, supported by market and vendor quotes, industry norms and historical costing to determine project cost, is considered to be a reasonable approach."*³
- *"We consider AGIG's strategy of moving to a common enterprise-wide platform across its networks to be a prudent approach that is likely to minimise risks and enable economies of scale in operational planning as well as the costs of procuring and supporting IT."*⁴
- *"We consider AGN's approach to infrastructure renewal [as part of a broader program to deliver AGIG's single national consolidated platform] is in line with good industry practice and the scope and methodology to determine costs is considered reasonable."*⁵

The consolidation program initiated in the current AA period for AGN SA continued into AA 2023/24-2027/28 for AGN (Victoria & Albury) and MGN, as approved by the AER.

In the current AGN SA AA period, we have completed data centre consolidation and rationalisation of our IT managed service providers, while also initiating

² AGN: SA Final Plan July 2021 – June 2026, Attachment 8.8: Capex business cases – South Australia, SA138 – AGIG IT Strategy & Roadmap, July 2020

³ AER: Attachment 5: Capital expenditure | Draft decision – Australian Gas Networks (SA) Access Arrangement 2021-26, November 2020, p.32

⁴ AER: Attachment 5: Capital expenditure | Draft decision – Australian Gas Networks (VIC & Albury) Access Arrangement 2023–28, December 2022 p.13

⁵ AER: Attachment 5: Capital expenditure | Draft decision – Australian Gas Networks (VIC & Albury) Access Arrangement 2023–28, December 2022 p.12

the consolidation of our user identity management services (i.e. Active Directory) across the group.

Additionally, we conducted a detailed inventory of all shared AGIG infrastructure assets used by AGN, confirming the percentage allocation to AGN of the total maintenance or refresh costs for each asset. This ensures fair cost distribution and prevents SA customers from bearing the expenses associated with IT infrastructure used by other AGIG entities. Moreover, we engaged independent experts to confirm the costs and frequency of lifecycle upgrades of our infrastructure assets, helping us to balance costs and risks effectively. Our shared infrastructure is now maintained according to a unified roadmap, with costs allocated to each AGIG entity based on a defined allocation model.

1.3.1.2 Infrastructure asset categories

Table 0.3 summarises the categories of AGIG's IT Infrastructure assets and their approximate lifecycles. For the shared AGIG assets, the table outlines the basis for allocating costs to AGN SA, using the following methods:

- **FTE-based:** Costs are allocated based on the number of full time equivalent (FTE) users in AGN divided by the total number of FTE users across all AGIG entities
- **Server-based:** Costs are allocated based on the proportion of servers assigned to AGN compared to the total number of servers across AGIG
- **Revenue-based:** If the above methods cannot be reliably applied due to multiple cost drivers affecting each entity's total cost, costs are allocated based on AGN SA's revenue relative to the total AGIG revenue

Detailed description of each of the asset categories is provided in 1.6.4Appendix A.

Table 0.3: AGN and AGIG IT infrastructure assets and their lifecycles

IT asset category	Description	Allocation basis	Asset lifecycle
AGN-owned infrastructure			
End user devices ⁶	End user devices (e.g. laptops, desktops, tablets, mobile devices, intrinsically safe devices), office and meeting room equipment (e.g. audio video equipment, projectors, printers) and telephony devices	N/A – 100% AGN SA owned	2-5 years
Meeting room equipment	Audio visual (AV) and meeting room equipment including video conferencing, presentation and digital signage technology	N/A – 100% AGN SA owned	5 years
Shared infrastructure			
<i>Network and currency</i>			
Standard Operating Environment (SOE)	Windows operating system, preferred web browsers, embedded end-point client software such as ██████████	User count	5 years

⁶ Refer to Section 1.5.1 for detailed information on the types of devices included in this category and their lifecycles

IT asset category	Description	Allocation basis	Asset lifecycle
	██████████, file compression software, etc		
Optimisation and collaboration tools	██████████ ██████████ ██████████ ██████████	Revenue	5 years
Office networking equipment	Office based network routing and switching equipment	Revenue	2-5 years
Operating systems	██████████ based operating systems	Revenue	3-5 years
Databases	Relational databases - ██████████ ██████████	Bottom-up allocation based on database usage	3-4 years
Authentication and identity management	Active Directory, group policy, security groups, distribution lists, etc	User count	3-4 years
IT service management (ITSM)	██████████ that provides digital workflows and procedures to support standard IT processes, including: <ul style="list-style-type: none"> • Incident Management • Request Management • Change Management • Knowledge Management • IT Purchasing 	Revenue	1 year
<i>Data centre</i>			
Data centre platform	██████████ hyperconverged hardware incorporating compute, memory, storage and networking used to host corporate server workloads	Number of servers allocated to AGN	5 years
Data centre core network	Data centre-based network routing and switching hardware	Number of servers allocated to AGN	5 years
Data centre appliances	██████████ ██████████, etc	Number of servers allocated to AGN	5 years
Infrastructure management tools	Monitoring, backup, orchestration, software distribution software, etc	Number of servers allocated to AGN	3-4 years

1.3.2 Scope and structure of this business case

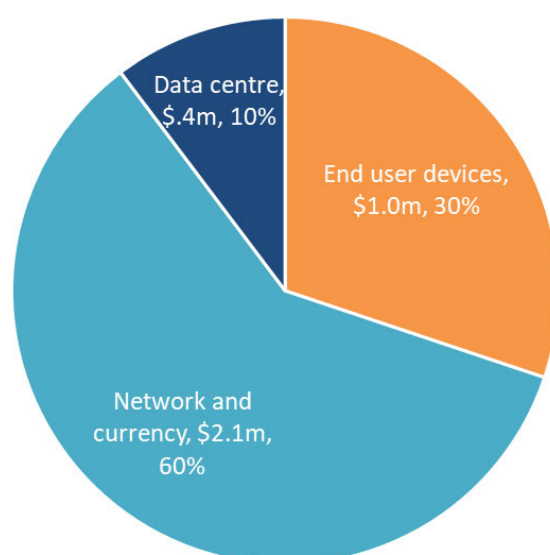
As the scope of this business case encompasses three different types of infrastructure, with different ownership structures and support arrangements, options for keeping this infrastructure current were considered separately for each of the associated recurrent workstreams:

- **End user devices:** The replacement / upgrade options for physical end user and office equipment are usually considered separately from those for the infrastructure software and services. AGN has 100% ownership of this asset category and as such the replacement of these devices is driven by the AGN-specific asset management plan and roadmap

- **Network and currency:** Due to their interconnected nature and shared support arrangements, the program of ongoing refresh for the assets in this category is driven by the AGIG-wide roadmap. AGN must take part in the roadmap initiatives, to enable economies of scale and adequate risk mitigation
- **Data centre:** In the current period, we consolidated the disparate data centres and vendor service arrangements into two AGIG-wide data centres. This brought our data centre infrastructure in line with industry practice and mitigated security risks that existed due to multiple provider arrangements. Having consolidated our data centres, we are now considering the options for refreshing the assets by evolving them in line with good industry practices, delivering the best value for money in the long term

Figure 0.3 depicts the forecast total expenditure (capex plus incremental opex) for the recommended options across each of these workstreams.

Figure 0.3: Relative share of the proposed infrastructure total expenditure (capex plus new opex) between the three workstreams



1.3.3 Description of problem /opportunity

The underlying driver for the investment described in this business case is the ongoing need to cost-efficiently maintain our existing levels of service to our customers while mitigating the risk of failure, cyber incidents or degraded performance due to the use of IT infrastructure beyond its useful life. Our IT infrastructure underpins the delivery of all IT services, which, in turn, are critical to the delivery of core AGN services and to our ability to securely store and access customer data.

As the IT infrastructure equipment approaches the end of its useful life, the risk of it failing increases and vendors no longer provide support or replacement parts for such equipment. It also becomes increasingly difficult to quickly implement the remedial actions required to resolve platform or system failures. In a worst-case scenario (which becomes increasingly probable as the infrastructure ages), the platform or system may experience a catastrophic failure and cannot be recovered, resulting in an urgent need to either upgrade or replace it to restore operations.

Aged IT infrastructure is also associated with increased cyber security risks. Vendors prescribe a regime of periodic security patches that must be applied with each upgrade. Deviating from the vendor-prescribed regime can void vendor warranty support arrangements and result in increased vulnerability to cyberattacks.

Finally, if IT infrastructure is not regularly refreshed its performance degrades due to insufficient capacity to support required storage, network bandwidth or computing resources.

Our IT infrastructure assets must therefore be renewed or replaced before they reach the end of their useful life. The useful lives of IT assets vary depending on their type, how heavily they are used and if they are used in the corporate offices, at home or in the field. Data centre, networking equipment and data centre appliances typically have a longer useful lifetime than end user devices such as laptops, mobile phones and tablets, resulting in a different frequency of upgrades or replacements as different types of equipment age and no longer perform at the standard required.

There is also an opportunity to leverage the industry trend of moving from company-owned infrastructure to cloud-based hosting. Cloud hosting technologies are becoming increasingly prevalent across all industry sectors, including utilities. The benefits of cloud hosting include greater scalability and flexibility, increased agility, and reduced operational risks. Increasingly, many vendors are offering only cloud-based versions of their products or services, which further accelerates the adoption of cloud technologies. On the other hand, cloud adoption comes with its own set of risks including vendor lock-ins, increased complexity of IT operations, and cyber security threats. This business case considers the opportunities, benefits and risks associated with cloud hosting when selecting a preferred option for our data centre roadmap.

1.4 Risk assessment

Risk management is a constant cycle of analysis, treatment, monitoring, reporting and then identifying once again, with a commitment to balance outcomes sought with delivery and cost implications considered and assessed.

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.

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 and activities required to ensure safety and compliance are not compromised, while delivery of this outcome is done as efficiently and effectively as possible.

The risk rating assesses the consequence and likelihood of the risk. The risk of an event associated with failure of an asset is rated based on the combined effect of the consequence and likelihood rating to provide an overall risk rating. This risk rating guides the risk management and mitigation activities and facilitates prioritisation.

Our Operational Risk Framework is based on AS/NZS 2885 and requires all identified risks ranked as intermediate or above to be addressed. For risks ranked as high we must *'Modify the threat, the frequency or the consequence to reduce the risk rank to intermediate or lower'*.

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 moderate or higher, we will undertake investment to reduce the risk.

Seven consequence categories are considered for each type of risk:

- 1 **Health & safety** – 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 **Operational capability** – Disruption in the daily operations and/or the provision of services/supply, impacting customers
- 4 **People** – Impact on engagement, capability or size of our workforce

Figure 0.4: Risk management principles



- 5 **Compliance** – Impact from non-compliance with operating licences, legal, regulatory, contractual obligations, debt financing covenants or reporting / disclosure requirements
- 6 **Reputation & customer** – Impact on stakeholders' opinion of AGN, including personnel, customers, investors, security holders, regulators and the community
- 7 **Financial** – Impact on AGN, measured on a cumulative basis

The primary risks of not renewing IT infrastructure include significant outages and cybersecurity breaches. As infrastructure ages and approaches the end of its useful life, its reliability decreases. Vendors may discontinue support or impose high fees for extended assistance. Additionally, security updates and patches may become unavailable, leaving the infrastructure vulnerable to cyberattacks.

The untreated risk⁷ ratings associated with IT sustaining infrastructure are presented in the following tables.

Table 0.4: Untreated risk rating – End User Devices

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	High
Consequence	Minimal	Minimal	Minor	Minimal	Significant	Significant	Significant	
Risk level	Low	Low	Intermediate	Low	High	High	High	

Table 0.5: Untreated risk rating – Network and currency

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	High
Consequence	Minor	Minor	Minor	Minor	Significant	Significant	Significant	
Risk level	Intermediate	Intermediate	Intermediate	Intermediate	High	High	High	

Table 0.6: Untreated risk rating – Data Centre

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	High
Consequence	Minor	Minor	Minor	Minor	Significant	Significant	Significant	
Risk level	Intermediate	Intermediate	Intermediate	Intermediate	High	High	High	

Failure of IT infrastructure and the resulting outages to key applications may lead to major safety incidents, for example, when technology becomes outdated (reaching end of support / end of life status), the IT infrastructure becomes more vulnerable to security incidents due to lack of security updates and vendor support. Security breaches of the infrastructure may cause outages in operational systems that would adversely affect the safety and integrity of AGN services. This may result in insufficient safety information being available in real time to field crews and a lack of visual representation of an asset, thereby increasing the likelihood of a safety incident.

⁷ Untreated risk is the risk level assuming there are no risk controls currently in place. Also known as the 'absolute risk'.

Outdated or unsupported IT infrastructure could result in unplanned production outages or degraded performance of our IT applications and network, resulting in the following supply consequences:

- Unreliable or underperforming infrastructure can result in inefficient work order processing, which may hinder the ability to make spatial and logical queries, delay timely repairs and maintenance, and increase the duration of outages
- Degraded IT infrastructure performance may result in slower, less efficient responses to customer calls
- Outdated IT infrastructure can result in inefficient processes, leading to delays in monitoring and managing the distribution network, which could impact the reliability and safety of gas delivery
- Inadequate IT infrastructure could hamper the company's ability to collect, analyse, and utilise data effectively for decision-making, leading to missed opportunities for optimisation and improvement of gas transport

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.

Catastrophic failure in underlying infrastructure may result in outages of AGN's core IT systems which, in turn, may lead to non-compliance with the AGN's regulatory and customer obligations. For example:

- A failure in infrastructure supporting the enterprise resource planning (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
- Security breaches may result in confidential customer data being compromised.
- Failure of the infrastructure supporting IT systems or data required to meet regulatory compliance requirements can lead to fines and penalties for the company, as well as damage to its reputation with regulatory bodies and customers
- Failure to renew data centre's backup and recovery solutions may put AGN at risk of losing critical data in the event of a disaster, resulting in prolonged downtime and significant compliance, reputational, financial and critical infrastructure impact

The consequences identified above may result in sizeable additional costs. Furthermore, without ongoing vendor support for upgrades or replacements to keep the infrastructure current, AGN will be forced to hire expensive consultants with detailed knowledge of outdated systems and infrastructure components.

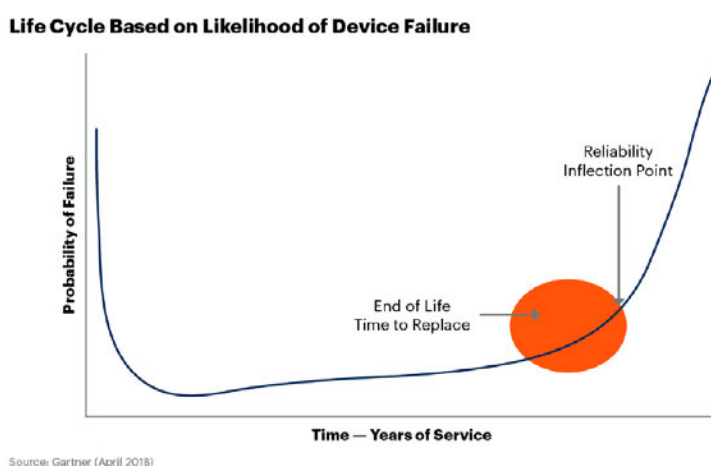
1.5 Options considered

1.5.1 End user devices

The scope of this workstream comprises the ongoing refresh or replacement of AGN's end user devices, including personal equipment such as laptops and mobile phones, office equipment, work from home (WFH) equipment, and field devices.

All devices are built with intrinsic obsolescence factors that include limited battery life, failing connector ports and declining performance. The useful life of end user devices also depends on a variety of factors related to their usage, for example, whether they are frequently moved around, or used to access high-performance and memory-intensive applications. As illustrated in a recent Gartner research paper⁸ (see Figure 0.5), while the individual lifecycles vary depending on device type and its usage patterns, the device failures follow a common pattern when the failure rates dramatically increase past a certain inflection point. Gartner recommends that "the goal should be to replace devices before the probability of failures increases significantly".

Figure 0.5: Device life cycle and optimal replacement point based on likelihood of device failure. Source: Gartner⁹



To determine the feasible refresh options to consider, we reviewed vendor recommendations and specific warranty periods for our devices, as well as compatible industry practices and benchmarks.

The options considered are:

- **Option 1: Vendor-recommended refresh** – Proactively replace the end user devices in line with vendor-recommended lifecycles
- **Option 2: Conservative refresh** – Refresh the end user devices on a schedule that has been extended compared to the vendor-recommended lifecycles where it is prudent to do so

8 Gartner, Inc.: *Recommended Life Spans to Guide PC, Mobile and Other Device Replacement Strategies*, 31 March 2021, p. 2

9 Source: Gartner, Inc.: *Recommended Life Spans to Guide PC, Mobile and Other Device Replacement Strategies*, 31 March 2021, p. 3

Table 0.7 lists the types of devices in scope, their quantities and the refresh rates for each of the options considered.

Table 0.7: Quantities of different types of end user devices and lifespans considered in each of the options

Project / device type	Quantity	Lifespan per option (years)	
		Option 1	Option 2
End user devices refresh			
Laptops	72	3	3.5
WFH hardware	20	5	5
Monitors and docks	72	5	5
Desktops	0	5	5
MFPs	2	5	5
Mobile phones	30	2	2.5
Tablets	10	3	3.5
Meeting room refresh			
AV and meeting room equipment	7	5	5

The options are discussed in the following sections.

1.5.1.1 Option 1 – Vendor-recommended refresh

Under this option, the refresh rate of our end user devices follows the vendor-recommended lifecycles.

1.5.1.1.1 Advantages and disadvantages

The advantage of this option is that critical devices (laptops, tablets and phones) are refreshed more frequently than under Option 2. This will provide a slightly lower cyber risk, a minor boost in productivity for users and a slightly lower possibility of the equipment failing in service.

The disadvantage of this option is that the additional device refreshes result in a higher cost for the program overall.

1.5.1.1.2 Achievement objectives

Table 0.8 outlines how Option 1 will support the achievement of our vision objectives.

Table 0.8: Achieving objectives – Option 1

Vision objective	Alignment
Customer Focussed – Public Safety	Y
Customer Focussed – Customer Experience	Y
Customer Focussed – Cost Efficient	N
A Leading Employer – Health and Safety	Y
A Leading Employer – Employee Experience	Y
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	N
Operational Excellence – Benchmark Performance	-

Vision objective	Alignment
Operational Excellence – Reliability	Y
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	N
Sustainable Communities – Socially Responsible	-

Refreshing the end user equipment according to vendor-recommended cycles ensures that it is safe, reliable, secure, and user-friendly. Providing our staff with the latest models of laptops, mobile phones, tablets, and other work-related equipment can enhance productivity, boost morale, and create additional learning opportunities.

However, this approach does not align with our vision of *Operational Excellence* or *Sustainable Communities*, given its higher cost and the environmental impact of replacing devices more frequently than may be necessary based on their condition.

1.5.1.1.3 Cost assessment

The estimated direct capital cost of Option 1 is \$1.2 million as shown in Table 0.9.

Table 0.9: Forecast capex – Option 1 End user devices, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
End user devices	180	180	180	180	180	899
Meeting room refresh	255	-	-	-	-	255
Total	435	180	180	180	180	1,154

1.5.1.1.4 Risk assessment

Table 0.10 summarises the risk rating for Option 1.

Table 0.10: Risk rating - Option 1 End user devices

Option 1	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Negligible
Consequence	Minimal	Minimal	Minimal	Minimal	Minor	Minor	Minor	
Risk level	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	

This option reduces the residual risk from high to negligible. This is through mitigating the reliability and performance risks associated with keeping devices past their useful life. Having reliable devices can prevent interruption to business operations for staff who perform key operational activities. Ensuring devices are updated with the latest security patches also reduces the risk of vulnerability to cyber attacks.

1.5.1.2 Option 2 – Conservative refresh

In this option, we considered extending the lifecycles of our end user device types compared to the vendor-recommended lifecycles.

1.5.1.2.1 Advantages and disadvantages

The advantage of this option is that the extension of lifecycles for some of the larger volume equipment types results in a reduction of cost overall.

The disadvantage of this option is that this means a slightly higher risk associated with cyber events, possible lower productivity and a slightly increased possibility of the equipment failing in service.

1.5.1.2.2 Achievement of objectives

Table 0.11 shows that Option 2 is fully aligned with our vision objectives.

Table 0.11: Achieving objectives – Option 2 End user devices

Vision objective	Alignment
Customer Focussed – Public Safety	Y
Customer Focussed – Customer Experience	Y
Customer Focussed – Cost Efficient	Y
A Leading Employer – Health and Safety	Y
A Leading Employer – Employee Experience	Y
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	Y
Operational Excellence – Benchmark Performance	Y
Operational Excellence – Reliability	Y
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	Y
Sustainable Communities – Socially Responsible	-

While providing slightly reduced reliability and security, prudently sweating IT assets where possible still results in a high level of staff productivity and morale, and results in a reliable asset fleet.

In addition, the cost saving realisation from sweating the assets means that this approach aligns with our vision of *Operational Excellence* and *Sustainable Communities*.

1.5.1.3 Cost assessment

The estimated direct capital cost of Option 2 is \$1.0 million as shown in Table 0.12.

Table 0.12: Forecast capex – Option 2 End user devices, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
End User Devices	156	156	156	156	156	782
Meeting Room Refresh	255	-	-	-	-	255
Total	411	156	156	156	156	1,037

1.5.1.4 Risk assessment

Table 0.13 summarises the risk rating for Option 2.

Table 0.13: Risk rating - Option 2 End user devices

Option 2	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Negligible
Consequence	Minimal	Minimal	Minimal	Minimal	Minor	Minor	Minor	
Risk level	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	

Similar to Option 1, Option 2 also reduces the residual risk from high to negligible by mitigating reliability and performance risks associated with keeping devices past their useful life, as well as vulnerability to cyber attacks.

1.5.1.5 Options assessment

Table 0.14: Comparison of options – End user devices

Option	Achievement of objectives	Capex costs	Treated risk
Option 1	This option would not be consistent with our <i>Operational Excellence</i> or <i>Sustainable Communities</i> objectives	\$1.2 million	Negligible residual risk
Option 2	This option is consistent with all our objectives	\$1.0 million	Negligible residual risk

Option 2 is recommended as the most cost-effective way to refresh our end user devices while keeping the risks associated with outdated or unsupported devices at an acceptable level. While Option 1 would reduce these risks even further, following the vendor-recommended approach without attempting to extend the life of devices via good management practices does not represent a prudent level of expenditure.

Project	Refresh freq.	% alloc. to AGN SA	Description	Included in:	
				Opt 1	Opt 2
	5 yrs	16.9%	The 2026 refresh will include both [REDACTED] which is more cost efficient than running these two projects separately.	Y	Y
	2-3 yrs	35.2%	The gap in the refresh schedule in 2026 is due to the [REDACTED] being bundled together for efficiency reasons.	Y	Y
SD-WAN	4-5 yrs	3.9%	[REDACTED] such as greater resilience options, greater bandwidth to meet business needs, reduce time and cost to deliver new sites, and more cost efficient WAN communications.	Y	Y

These options are discussed in the following sections.

1.5.2.1 Option 1 – AGN-centric approach to infrastructure refresh

This option constitutes the base case for the networking and currency workstream, against which we assess other credible options. Under this option, AGN will not participate in further consolidation of the AGIG infrastructure and will only undertake necessary refreshes to maintain currency of AGN's part of the infrastructure environment. Under this option AGN will not participate in the AD consolidation project that is scheduled for 2026/27 in the 'AGIG One IT' Strategy & Roadmap.

1.5.2.1.1 Advantages and disadvantages

The advantage of this option is that it avoids an allocation of capex associated with the AD consolidation project.

The disadvantage of this option is it fails to unlock the economies of scale and other benefits associated with AD consolidation. This includes:

- Improved security and efficiency and to align with AD best practices
- Aligned user access, authentication, and auditing controls in line with AGIG cyber security policies and standard
- Simplified user login experience for staff
- Improved efficiency of the IT management and maintenance of the AGN infrastructure environment

As a result, the other projects in this workstream become more costly.

1.5.2.1.2 Achievement of objectives

Table 0.16 shows the alignment with our vision objectives.

Table 0.16: Achieving objectives – Option 1 Network and currency

Vision objective	Alignment
Customer Focussed – Public Safety	-
Customer Focussed – Customer Experience	-
Customer Focussed – Cost Efficient	N

A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	N
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	-
Operational Excellence – Benchmark Performance	N
Operational Excellence – Reliability	-
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

This option will not meet our vision of being *Customer Focussed*, or achieving *Operational Excellence* as it does not represent the lowest overall cost for our infrastructure. It also results in AGN staff not receiving the benefits of a centralised AD, therefore not reflecting our objective to be *A Leading Employer*.

1.5.2.1.3 Cost assessment

The estimated direct capital cost of Option 1 is \$2.2 million as shown in Table 0.17.

Table 0.17: Forecast next AA period capex – Option 1 Network and currency, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/2031	Total
Office networking	48	125	-	-	295	467
AD consolidation	-	-	-	-	-	-
SOE	-	138	2	-	-	140
OS currency	161	161	161	161	161	803
SQL currency	42	45	-	3	-	90
SNOW upgrades	55	55	55	55	55	274
Collaboration	-	-	109	-	-	109
	185	-	-	-	-	185
	-	9	9	9	9	35
SD-WAN	52	-	-	-	15	67
Total	542	533	335	227	534	2,170

1.5.2.1.4 Risk assessment

Table 0.18 provides a risk assessment for Option 1.

Table 0.18: Risk rating - Option 1 Network and currency

Option 1	Health & Safety	Environ-ment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Low
Consequence	Minor	Minor	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Negligible	Negligible	Low	Low	Low	

Risks associated with aged and deteriorated infrastructure assets include reliability, performance and vulnerability to cyber security attacks. Prudently replacing end of life

assets in line with good industry practice reduces these risks from high to low under Option 1. This option is not considered ALARP.

1.5.2.2 Option 2 – ‘AGIG One IT’ approach to infrastructure refresh

In addition to refreshing our recurrent assets as proposed in Option 1, this option also includes the consolidation of the AGN AD into the shared AD that will be set up for all AGIG entities.

AGIG currently has three corporate AD domains, one for each entity, that manage user authentication and authorisation to network resources. Each AD structure is fragmented, resulting in a disjointed user experience, security risks, and inefficient maintenance and support.

Each AD has evolved separately from the others, resulting in inconsistent design and configuration. This necessitates extra effort to audit, manage and protect each of them and increases risk of compromise due to wider attack surface.

As part of the ‘AGIG One IT’ Roadmap, we plan to execute the AD migration and SOE upgrade simultaneously. This approach minimises user disruption by consolidating change management activities into a single project timeline.

1.5.2.2.1 Advantages and disadvantages

The advantages of consolidating the AGN AD into the AGIG AD are:

- Improved security and efficiency and to align with AD best practices
- Aligned user access, authentication, and auditing controls in line with AGIG cyber security policies and standard
- Simplified user login experience for staff
- Improved efficiency of the IT management and maintenance of the AGN infrastructure environment

It also results in reduced costs associated with some of the other elements in this workstream.

The only disadvantage of this option is the capital cost associated with the AD project.

1.5.2.2.2 Achievement of objectives

Table 0.19 shows alignment with our vision objectives.

Table 0.19: Achieving Objectives - Option 2 Network and currency

Vision objective	Alignment
Customer Focussed – Public Safety	-
Customer Focussed – Customer Experience	-
Customer Focussed – Cost Efficient	Y
A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	Y
A Leading Employer – Skills Development	Y
Operational Excellence – Profitable Growth	-

Operational Excellence – Benchmark Performance	Y
Operational Excellence – Reliability	-
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

This option meets our vision of being *Customer Focussed*, and achieving *Operational Excellence* as represents the lowest overall cost for our infrastructure. By undertaking the AD consolidation first, the costs of other projects in this workstream will be reduced compared to those in Option 1, and reduce support overheads.

It will improve employee access to IT resources and provide a seamless IT experience across AGIG, aligning with our objective to be *A Leading Employer*.

1.5.2.2.3 Cost assessment

The estimated direct capital cost of Option 2 is \$2.1 million as shown in the following table.

Table 0.20: Forecast capex – Option 2 Network and currency, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Office networking	173	-	-	248	-	420
AD consolidation	49	-	-	-	-	49
SOE	-	131	2	-	-	132
OS currency	152	152	152	152	152	760
SQL currency	32	35	-	2	-	69
SNOW upgrades	55	55	55	55	55	274
Collaboration	-	-	109	-	-	109
	136	-	-	-	-	136
	-	9	9	8	8	35
SD-WAN	52	-	-	-	15	66
Total	648	382	326	465	230	2,051

1.5.2.2.4 Risk assessment

Table 0.21 summarises the risk rating for Option 2.

Table 0.21: Risk rating - Option 2 Network and currency

Option 2	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Hypothetical	Negligible
Consequence	Minor	Minor	Minor	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	

Risks associated with aged and deteriorated infrastructure assets include reliability, performance and vulnerability to cyber security attacks. Prudently replacing end of life assets in line with good industry practice reduces these risks under Option 2. Compared

with Option 1, risk is further reduced under this option to Negligible through consolidating AGN into the AGIG AD.

1.5.2.3 Options assessment

Table 0.22: Comparison of options – Network and currency

Option	Achievement of objectives	Costs	Treated risk
Option 1	This option would not be consistent with our objective of being <i>A Leading Employer</i> or <i>Operational Excellence</i>	\$2.2 million	Low residual risk (not ALARP)
Option 2	This option is consistent with all our objectives	\$2.1 million	Negligible residual risk

Option 2 is recommended as it represents the most cost-effective option of maintaining the current levels of service enabled by our networking infrastructure and software. Option 1 is more expensive than Option 2 because it does not invest into any further consolidation of the AGN infrastructure after the current AA period and therefore isn't able to take advantage of the consolidation, most notably the consolidation of AGN's AD that is part of the 'AGIG One IT' Strategy & Roadmap.

1.5.3 Data centre

During the current AA period, we consolidated and rationalised our data centre platform and equipment as part of the 'AGIG One IT' roadmap, with the key objectives to¹¹:

- Support feedback from our stakeholders, regulators, and customers that they value reliable and safe delivery of energy to our customers backed by timely support when they need help
- Address specific issues and risks common to all AGIG businesses, including cyber security
- Achieve economies of scale in purchasing and support costs

As part of the data centre consolidation, AGN moved away from its previous infrastructure as a service (IAAS) arrangements and was allocated a share of the physical infrastructure in the newly established AGIG data centres. AGN has benefitted from the enhanced security, improved resource utilisation, better scalability, and stabilised and improved performance.

In considering the options for our data centre evolution in next AA period and beyond, our primary objective is to ensure that our infrastructure is both cost effective and fit for purpose in the long term. One option that is increasingly popular among our industry peers and similar size businesses is moving from the on-premises data centre infrastructure to a cloud-based infrastructure hosting.

¹¹ AGN: SA Final Plan July 2021 – June 2026, Attachment 8.8: Capex business cases – South Australia, SA138 – AGIG IT Strategy & Roadmap, July 2020, p. 444

The options for refreshing our data centre assets in the next AA period are:

- **Option 1: BAU** – Continue to refresh data centre infrastructure assets in our on-premises data centre
- **Option 2: 'Organic' transition to cloud** – Transition our data centre infrastructure to cloud in an orderly manner as our existing on-premise data centre components run out of support.
- **Option 3: 'Big Bang' transition to cloud** – Migrate all of data centre infrastructure to the cloud at once

It is assumed that under both Option 2 and Option 3, all AGN servers will move to the Azure cloud by 2030, but the move to the cloud would be more gradual under Option 2 (Table 0.23). Note that there is an assumed 30% reduction in the total number servers by 2029 due to SaaS and RISE migrations.

Table 0.23: On-premises vs cloud servers under each option

Number of servers	2024	2025	2026	2027	2028	2029	2030
Option 1 BAU (on-premises)							
BAU - AGIG total	368	346	324	302	280	258	236
BAU – AGN	27	26	24	22	21	19	17
Option 2 Organic							
% Azure Servers	-	-	20%	40%	60%	80%	100%
Total number of servers	-	-	65	121	168	206	236
AGN number of servers	-	-	5	8	12	14	17
AGN number of On-Prem Servers	27	26	19	14	9	5	-
Option 3 Big Bang							
% Azure Servers	-	-	-	-	25%	75%	100%
Total number of servers	-	-	-	-	70	193	236
AGN number of servers	-	-	-	-	4	13	17
AGN number of On-Prem Servers	27	26	24	22	17	6	-

The opex estimates for Options 2 and 3 are for the Azure server licences, backup, disaster recovery and necessary bandwidth provisions. Under all three options, there is ongoing capex for the System Center Configuration Manager (SCCM) and Mobile Device Management (MDM), the tools that are necessary for remote management of the data centre infrastructure.

The options are discussed in the following sections.

1.5.3.1 Option 1 – BAU

This option continues the BAU data centre infrastructure refreshes utilising our existing on-premises data centres.

1.5.3.1.1 Advantages and disadvantages

The key advantage of retaining and updating our infrastructure on premise is that it will avoid potential risks associated with cloud infrastructure such including vendor lock-ins, increased complexity of IT operations, and cyber security threats. This option also avoids the incremental opex associated with cloud-based solutions.

The disadvantage is that it will not allow AGN to unlock key cloud benefits such as scalability and flexibility, enhanced disaster recovery, improved reliability and performance, and access to latest technologies that both provide operational benefits and drive lower costs.

It also fails to realise the benefits of cloud, resulting in the highest cost possible alternatives.

1.5.3.1.2 Achievement of objectives

Table 0.24 shows how this option aligns to our vision objectives.

Table 0.24: Achieving Objectives – Option 1 Data centre

Vision objective	Alignment
Customer Focussed – Public Safety	-
Customer Focussed – Customer Experience	-
Customer Focussed – Cost Efficient	N
A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	-
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	N
Operational Excellence – Benchmark Performance	N
Operational Excellence – Reliability	-
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

This option does not align with our vision of being *Customer Focussed* or achieving *Operational Excellence*, because it has a higher cost than Options 2 and 3.

1.5.3.1.3 Cost assessment

The direct capital cost of this option is \$0.4 million as shown in Table 0.25.

Table 0.25: Forecast capex – Option 1 Data centre, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Data centre appliances	37	37	37	37	37	186
Data centre platform	-	103	-	103	-	207
Infrastructure tools	2	2	2	2	2	10
Total	39	143	39	143	39	403

1.5.3.1.4 Risk assessment

Table 0.26 summarises the risk rating for Option 1.

Table 0.26: Risk rating - Option 1 Data centre

Option 1	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Hypothetical	Hypothetical	Remote	Hypothetical	Remote	Hypothetical	Remote	Negligible
Consequence	Minimal	Minimal	Minor	Minimal	Minor	Minimal	Minor	
Risk level	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	

The continued refresh of our data centre infrastructure reduces the residual risk under Option 1 from high to negligible (ALARP).

1.5.3.2 Option 2 – ‘Organic’ transition to cloud

This option considers an ‘orderly’ transition to cloud that involves a gradual and planned move of IT infrastructure resources to the cloud as the existing on-premises resources approach the end of their useful life or are due for a major refresh.

1.5.3.2.1 Advantages and disadvantages

The advantages of moving to cloud-based infrastructure hosting include:

- *Scalability and flexibility:* The cloud allows for easily scalable resources to meet fluctuating demands. Businesses can quickly adjust their IT resources during peak periods or in response to changing regulatory requirements without the need for significant upfront investments
- *Enhanced disaster recovery:* Cloud providers typically offer robust disaster recovery and backup solutions, ensuring that critical data and applications are protected and can be restored rapidly in the event of a disaster
- *Improved reliability and performance:* Cloud services often come with guaranteed uptime and service-level agreements, which can offer greater reliability compared to on-premises infrastructure
- *Access to latest technologies:* Increasingly, many vendors are offering only cloud-based versions of their products or services, which further accelerates the adoption of cloud technologies

These benefits also drive lower cost, and reflects the most cost-effective option of the available alternatives.

The phased approach results in delivery risks being better managed. Each migration can be evaluated for performance and security before moving on to the next component.

The disadvantage of moving infrastructure operations to the cloud includes potential risks such as vendor lock-ins, increased complexity of IT operations, and cyber security threats.

1.5.3.2.2 Achievement of objectives

The following table outlines how Option 2 will support achievement of our vision objectives.

Table 0.27: Achieving Objectives - Option 2 Data centre

Vision objective	Alignment
Customer Focussed – Public Safety	-
Customer Focussed – Customer Experience	-
Customer Focussed – Cost Efficient	Y
A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	-
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	Y
Operational Excellence – Benchmark Performance	Y
Operational Excellence – Reliability	-
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

This option is Customer Focussed and reflects *Operational Excellence* as it spreads out investments over time rather than incurring substantial expenses all at once, lowering costs over time.

1.5.3.2.3 Cost assessment

The estimated direct costs associated with this option are \$0.4 million as shown in Table 0.28.

Table 0.28: Forecast capex and opex – Option 2 Data centre, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex	52	14	14	20	14	115
Opex	33	38	49	58	62	239
Total	85	52	63	78	76	354

A breakdown of the capex and opex is provided in Table 0.29 and Table 0.30.

Table 0.29: Forecast capex – Option 2 Data centre, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Data centre appliances	-	-	-	-	-	-
Data centre platform	50	12	12	19	12	106
Infrastructure tools	2	2	2	2	2	10
Total	52	14	14	20	14	115

Table 0.30: Forecast opex – Option 2 Data centre, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Data centre appliances	-	-	-	-	-	-
Data centre platform	33	38	49	58	62	239
Infrastructure tools	-	-	-	-	-	-
Total	33	38	49	58	62	239

1.5.3.2.4 Risk assessment

Table 0.31 summarises the risk rating for Option 2.

Table 0.31: Risk rating - Data centre Option 2 Data centre

Option 2	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Hypothetical	Hypothetical	Remote	Hypothetical	Remote	Hypothetical	Remote	Negligible
Consequence	Minimal	Minimal	Minor	Minimal	Minor	Minimal	Minor	
Risk level	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	

As with Option 1, the refresh of data infrastructure assets under Option 2 addresses the high untreated residual risk, lowering this to negligible (ALARP).

1.5.3.3 Option 3 – 'Big Bang' transition to cloud

Under this option we would migrate all of data centre infrastructure to the cloud at once.

1.5.3.3.1 Advantages and disadvantages

Option 2 results in the same outcome as Option 2, therefore the advantages and disadvantages are the same as described in section 1.5.3.2.1.

1.5.3.3.2 Achievement of objectives

The following table shows how Option 3 would achieve our vision objectives.

Table 0.32: Achieving objectives - Option 3 Data centre

Vision objective	Alignment
Customer Focussed – Public Safety	-
Customer Focussed – Customer Experience	-
Customer Focussed – Cost Efficient	N
A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	-

Vision objective	Alignment
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	N
Operational Excellence – Benchmark Performance	Y
Operational Excellence – Reliability	-
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

This option is not Customer Focussed and does not reflect *Operational Excellence* as it achieves the same overall outcomes as Option 3 but at a higher overall cost, and with more delivery and cost risk.

1.5.3.3.3 Cost assessment

The estimated direct costs associated with this option are \$0.4 million as shown in

Table 0.33: Forecast capex and opex – Option 3 Data centre, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex	2	26	75	75	26	204
Opex	-	9	34	56	62	161
Total	2	35	109	131	88	366

A breakdown of the capex and opex is provided in Table 0.34 and Table 0.35.

Table 0.34: Forecast capex – Option 3 Data centre, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Data centre appliances	-	-	-	-	-	-
Data centre platform	-	24	73	73	24	195
Infrastructure tools	2	2	2	2	2	10
Total	2	26	75	75	26	204

Table 0.35: Forecast opex – Option 3 Data centre, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Data centre appliances	-	-	-	-	-	-
Data centre platform	-	9	34	56	62	161
Infrastructure tools	-	-	-	-	-	-
Total	-	9	34	56	62	161

1.5.3.3.4 Risk assessment

'Big Bang' transition carries a higher risk of potential service interruptions and/or technical challenges, as everything is transitioning simultaneously with less time for testing individual components.

Table 0.36: Risk risk - Option 3

Option 3	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Hypothetical	Hypothetical	Unlikely	Hypothetical	Unlikely	Hypothetical	Unlikely	Low
Consequence	Minimal	Minimal	Minor	Minimal	Minor	Minimal	Minor	
Risk level	Negligible	Negligible	Low	Negligible	Low	Negligible	Low	

Similar to the other options, refreshing our data infrastructure assets under option 3 will address the high untreated residual risk, lowering this to low (not ALARP).

1.5.3.4 Options assessment

Table 0.37: Comparison of options – Data centre

Option	Achievement of objectives	Costs	Treated risk
Option 1	This option would not achieve <i>Operational Excellence</i> and would not be considered being <i>Customer Focussed</i>	\$0.4 million capex	Negligible residual risk ALARP
Option 2	This option is consistent with all our objectives	\$0.1 million capex \$0.2 million opex	Negligible residual risk ALARP
Option 3	This option deliver the program at a higher cost and delivery risk than Option 2 and could therefore be arguably not achieving <i>Operational Excellence</i> or being <i>Customer Focussed</i>	\$0.2 million capex \$0.2 million opex	Low residual risk (not ALARP)

Option 2 is recommended as the most cost-effective long-term solution for our data centre based on a total expenditure (totex) assessment. Additionally, Option 2 has a lower risk rating compared to Option 3 due to a more gradual transition to the cloud, which is associated with fewer project risks.

1.6 Proposed solution

We propose to proceed with the program of work that entails implementing the recommended options for each of the workstreams.

1.6.1 Why is the recommended option prudent?

1.6.1.1 End user devices

The recommended option proposes extending the refresh cycle for laptops, mobile phones and tablets by six months beyond the vendor-recommended term because, based on our experience and according to industry benchmarks, this can be done without a material increase of the risk of failure. For all other devices, the recommended option aligns with vendor recommendations, industry benchmarks and the practice of our industry counterparts (Table 0.38).

Table 0.38: AGN end user device refresh cycles compared with industry practice and Gartner recommendations

	AGN: recommended option	Gartner ¹²	SA Power Networks ¹³	Ausgrid ¹⁴	Essential ¹⁵
Laptops	3.5	3.5	3.5	3-4	4
WFH hardware	5	n/a	n/a	n/a	n/a
Monitors and docks	5	n/a	n/a	5	5
Desktops	5	5	5	n/a	4
MFPs	5	n/a	n/a	n/a	n/a
Mobile phones	2.5	2.5	2.5	3	2-3
Tablets	3.5	3	3.5	4	3-4
AV and meeting room equipment	5	n/a	4	5	n/a

This approach is prudent because it delivers the best value for money while maintaining risk at an acceptable level.

1.6.1.2 Network and currency

The recommended option aligns with 'AGIG-one IT' approach to infrastructure refresh, which finalises the transition to the shared AGIG infrastructure environment commenced in the current AA period.

This approach is prudent because it allows us to realise economies of scale from efficiently sharing the resources; it is more cost efficient and provides a greater risk reduction than the alternative.

1.6.1.3 Data centre

The recommended option of gradual transition to the cloud is prudent because it follows the prevailing industry trends, delivers best value for money and has lower level of risk than the 'big bang' rapid transition also considered as one of the alternatives.

1.6.2 Implementation of the initiatives

End user device refresh is a standard BAU process that is not expected to face any challenges.

The preferred option for 'Network and currency' workstream dovetails into the program of work already undertaken by other AGIG entities, which decreases the implementation complexity and risk of failure.

Transition to the cloud is the journey undertaken by many companies, and we will be following a well-established pathway. The recommended option of gradual transition will

¹² Gartner, Inc.: *Recommended Life Spans to Guide PC, Mobile and Other Device Replacement Strategies*, 31 March 2021

¹³ SA Power Networks, *2020-25-2030 Regulatory Proposal*, Supporting document 5.12.5, 15 July 2024

¹⁴ Ausgrid: Attachment 5.9.e – ICT & infrastructure program – 31 Jan 2023 – Public, Appendix 3

¹⁵ Essential Energy ICT Business Plan – January 2023, p.12

allow us to further de-risk the implementation by using a staged approach and learning along the way.

1.6.3 Estimating the efficient costs

Costs for this project have been estimated using standard 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 9.10). In particular, the planned infrastructure renewal will ensure our devices are compatible with the objectives of the AGIG IT Strategy & 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.

Table 0.39: IT sustaining infrastructure capex by project, \$'000 January 2025

Category / project	2026/27	2027/28	2028/29	2029/30	2030/31	Total
End User Devices						
End User Devices	156	156	156	156	156	782
Meeting Room Refresh	255	-	-	-	-	255
End User Devices total	411	156	156	156	156	1,037
Network and currency						
Office networking	173	-	-	248	-	420
AD consolidation	49	-	-	-	-	49
SOE	-	131	2	-	-	132
OS currency	152	152	152	152	152	760
SQL currency	32	35	-	2	-	69
SNOW upgrades	55	55	55	55	55	274
Collaboration	-	-	109	-	-	109
[REDACTED]	136	-	-	-	-	136
[REDACTED]	-	9	9	8	8	35
SD-WAN	52	-	-	-	15	66
Network and currency total	648	382	326	465	230	2,051
Data centre						
Data Centre Platform	50	12	12	19	12	106
Infrastructure tools	2	2	2	2	2	10
Data centre total	52	14	14	20	14	115
Total	1,112	552	497	641	400	3,203

Table 0.40: IT sustaining infrastructure capex, by cost type, \$'000 January 2025

	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Internal Labour	252	207	208	152	152	971
Contractors /Consultants	-	-	-	-	-	-
Materials & Services	860	345	290	489	248	2,232
Travel & Others	-	-	-	-	-	-
Total	1,112	552	497	641	400	3,203

1.6.4 Consistency with the National Gas Rules

Option 2, deliver proactive IT sustaining infrastructure initiatives, is the recommended solution and will maintain IT Infrastructure in line with accepted good industry practice.

NGR 79(1)/91

The proposed expenditure on our IT sustaining infrastructure is also consistent with NGR 79(1)(a), specifically we consider the capital expenditure is:

- *Prudent* – The expenditure is necessary in order to address the identified risks to AGN. The project is based on the proactive replacement of IT infrastructure assets which have arrived at the end of their useful economic life, avoiding operational inefficiencies due to outages or deteriorated performance. The proposed expenditure can therefore be seen to be of a nature that would be incurred by a prudent service provider.
- *Efficient* – The forecast expenditure is based on historic costs for similar replacements. Pricing for these assets is sought through a competitive tender process, and is subject to regular market testing to ensure efficient prices are achieved. The proposed expenditure can therefore be considered consistent with the expenditure that a prudent service provider acting efficiently would incur.
- *Consistent with accepted good industry practice* – The proposed asset lifecycle for our IT infrastructure assets is consistent with that employed across industries.
- *Achieves the lowest sustainable cost of delivering pipeline services* – The proposed proactive replacement of IT infrastructure is more cost effective than a reactive, or lower frequency replacement program. Repair costs, and lost productivity, for IT infrastructure assets which fail, are typically more costly than replacement over the medium to longer term.

NGR 79(2)

The proposed expenditure on our IT sustaining infrastructure project is required to maintain the integrity of services through current, supported and fit for purpose IT infrastructure, managing technology risks and preventing material outages that impact the ability of the business to function (including tracking and reporting of business information to meet our regulatory obligations and requirements). Therefore, this expenditure is consistent with NGR 79(2)(c)(ii) and (iii).

NGR 74

The forecast costs in this business case are based on the latest market rate testing, and project options consider the asset management requirements as per the IT Investment Plan. Cost assessments have been conducted for each option based on the best information available at the time of developing 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

A.1 IT data centre platforms

This category 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 for various business applications. Data centre platform equipment is typically replaced every five years in line with asset depreciation cycles.

A.2 Data centre core network

This is comprised of high performance switching and routing equipment that enables network connectivity from AGN'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 five years in line with asset depreciation cycles.

A.3 Data centre appliances

This is comprised of specialised equipment such as wireless local area network (LAN) controllers that define the perimeter of the internal and external (internet) networks through which all traffic into and out of the data centre flows. Data centre appliance equipment is typically replaced every five years in line with asset depreciation cycles.

A.4 Office networking equipment

This includes network switching and routing equipment located at end points of the connected network, i.e. the AGN office locations that provides a secure and private network connection to the central AGIG data centres within which the AGN applications are hosted and run. Office networking equipment is typically replaced every five years in line with asset depreciation cycles.

A.5 Operating systems

This comprises the virtualised server operating systems and the workstation operating systems () on the end user desktops and laptops. Typically, the standard operating environment (SOE) for each type is updated and replaced every three to five years. For servers a staged program of replacement is performed over a number of years to opportunistically align with application upgrades or replacements. For end user devices, a new SOE is developed and deployed to the fleet within a shorter period to ensure standardisation of the user experience as quickly as possible. 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 both for server based and workstation-based applications.

A.6 Databases

This comprises the database software products upon which business and infrastructure related applications are reliant. Typically, databases are updated or replaced every three or four 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.

A.7 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 three to four years to remain current and take advantage of new functionality to improve infrastructure management.

A.8 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 three to four years to remain current, take advantage of new or improved functionality and remain supported by the product vendor. AGIG has multiple corporate AD instances, of which one is provided to AGN. A program to consolidate and upgrade the disparate AD 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.

A.9 End user compute equipment

This comprises all equipment required by end users to perform their work and includes:

- End user compute devices (e.g. laptops, tablets, mobile phones)
- Office equipment (e.g. desktops, monitors, docking stations)
- Peripheral equipment such as keyboards, mice, etc.
- Working from home (WFH) hardware
- Printers and multi-function devices (MFPs)
- Mobile devices including mobile phones and tablet devices

End user compute equipment is typically replaced every two to five years in line with warranty and asset depreciation cycles. It is worth noting that approximately 50% of AGN devices operate in remote (red dust) environments and have a shorter than average lifespan. End user computing equipment has been maintained and 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.

A.10 Meeting room equipment

Meeting room equipment includes video conferencing, presentation and digital signage technology for AGN offices.

The existing meeting rooms in the AGN offices have video conferencing capabilities including screens, cameras, microphone, speakers and control systems that require a hardware refresh every five years to ensure vendor support, reliability and compatibility with [REDACTED] functionality.

Across the AGN offices there are digital signage screens that present information to staff. This hardware and associated platforms require a hardware and software refresh every five years to ensure vendor support, reliability and compatibility with [REDACTED] functionality.

This current AV equipment was purchased and installed in 2021 under the office fit out budget and requires a refresh in 2026.

A.11 End user computer software

This comprises the workstation operating systems, optimisation technologies and collaboration tools required by end users to function effectively. This includes the following components.

- 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

Typically, the SOE image is updated and replaced every three to five 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.

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 three to five 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 AGN'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 three to five years.

A.12 IT service management tools

This category includes the software that provides digital workflows and procedures to support standard IT processes, including:

- Incident Management

- Request Management
- Change Management
- Knowledge Management
- IT Purchasing

Appendix B Comparison of risk assessments

B.1 End user devices

Untreated	Health & Safety	Environ-ment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	High
Consequence	Minimal	Minimal	Minor	Minimal	Significant	Significant	Significant	
Risk level	Low	Low	Intermediate	Low	High	High	High	

[illegible][illegible]

B.2 Network and currency

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	High
Consequence	Minor	Minor	Minor	Minor	Significant	Significant	Significant	
Risk level	Intermediate	Intermediate	Intermediate	Intermediate	High	High	High	

Option 1	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Low
Consequence	Minor	Minor	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Negligible	Negligible	Low	Low	Low	

[illegible]

B.3 Data centre

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	High
Consequence	Minor	Minor	Minor	Minor	Significant	Significant	Significant	
Risk level	Intermediate	Intermediate	Intermediate	Intermediate	High	High	High	

Option 1	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Hypothetical	Hypothetical	Remote	Hypothetical	Remote	Hypothetical	Remote	Negligible
Consequence	Minimal	Minimal	Minor	Minimal	Minor	Minimal	Minor	
Risk level	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	

Option 2	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Hypothetical	Hypothetical	Remote	Hypothetical	Remote	Hypothetical	Remote	Negligible
Consequence	Minimal	Minimal	Minor	Minimal	Minor	Minimal	Minor	
Risk level	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	Negligible	

Option 3	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Hypothetical	Hypothetical	Unlikely	Hypothetical	Unlikely	Hypothetical	Unlikely	Low
Consequence	Minimal	Minimal	Minor	Minimal	Minor	Minimal	Minor	
Risk level	Negligible	Negligible	Low	Negligible	Low	Negligible	Low	

SA240 – Cyber security (SOCI Act PROTECTED)

1.1 Project approvals

Table 0.1: SA240 Cyber security – Project approvals

Prepared by	Darryl Argus, Head of Cyber Security and Risk Trev Dunstan, Cyber Security Architect
Reviewed by	Brooke Palmer, Head of IT Business Engagement
Approved by	Brett Miller, Chief Information Officer

1.2 Project overview

Table 0.2: SA240 Cyber security – Project overview

Description of problem /opportunity	<p>As a responsible pipeline operator, not only must we ensure the ongoing security of network assets, we must also ensure our data and our customers' data is secure. This is required by our Foreign Investment Review Board (FIRB) conditions, as well as Security of Critical Infrastructure (SOCI) and Privacy legislation.</p> <p>The cyber security threat landscape continues to evolve and increase in complexity, with breaches causing significant issues for organisations. There have been multiple publicised high profile breaches of data privacy requirements within Australia in the last few years, with damages running to tens of millions of dollars per breach event. There have also been several threats against critical service providers, including breaches of operational networks. We must therefore ensure that we not only maintain our existing controls but also continue to add controls, improving our cyber security maturity in order to be able to identify and respond to the new threats posed.</p> <p>Our risk assessment has identified several specific key gaps, verified by independent review, that must be addressed in the upcoming period in order to mitigate the highest risks to both our information technology (IT) and operational technology (OT) environments. Left untreated, these gaps leave a high risk, with the potential for significant consequences for AGN and our customers.</p> <p>Over the next access arrangement (AA) period we need to continue to maintain our existing capability, and uplift our maturity to address the identified gaps to keep our IT and OT systems safe and reliable.</p>
Untreated risk	As per risk matrix = High
Options considered	<ul style="list-style-type: none"> • Option 1 – Maintain current environment (\$0.5 million) • Option 2 – Uplift maturity to address key identified risks (\$1.4 million capex, \$1.1 million opex) • Option 3 – Uplift maturity to meet security profile 3 standards (\$1.9 million capex, \$2.0 million opex)
Proposed solution	<p>Option 2 is the proposed solution. This option will allow us to maintain the currency of our cyber security platforms and services in line with our legislative requirements, and uplift our maturity levels related to:</p> <ul style="list-style-type: none"> • Data privacy and security • Access control for remote access and consistency of access between internal and cloud-based applications

Estimated cost	<p>These initiatives are critical to continue to operate our IT and OT systems in a safe and reliable manner to meet our legislative requirements in relation to SOCI and privacy. The proposed solution reflects the AGN SA contribution to our AGIG-wide investment plan, which will achieve a balance between security outcomes and cost impact on customers. It has been designed to deliver a risk-based prioritised program of work over the next five years.</p> <p>Option 1 would not be compliant with our obligations under SOCI or relevant privacy laws and would leave our cyber security risks as high if left untreated. It would also result in higher costs over the long term as we would need to reactively respond to cyber security incidents, which is more costly and affects the reliability of our IT and OT systems. Maintaining the current environment (not uplifting security to mitigate contemporary threats) also places the business at greater risk of data theft or unauthorised access to personal customer data that could be used for malicious purposes and fraudulent activities.</p> <p>Option 3 provides the greatest reduction in cyber risk. It would significantly improve the resilience of our IT and OT landscape, and will allow us to meet the standards of security profile 3 (SP-3) under the Australian Energy Sector Cyber Security Framework (AESCSF). However, we consider that a risk-based program of work designed to target identified weaknesses in our operating environment is more prudent and balances risk and cost when compared to the blanket adoption of generic standards such as is set out in SP-3.</p>																																																																													
	<p>The forecast direct cost (excluding overheads) during the next AA period is \$1.6 million in capex and \$1.3 million in opex.</p>																																																																													
	<table><tr><th>\$'000 Jan 2025</th><th>26/27</th><th>27/28</th><th>28/29</th><th>29/30</th><th>30/31</th><th>Total</th></tr><tr><td colspan="7">Capex</td></tr><tr><td>Maintain currency</td><td>388</td><td>-</td><td>16</td><td>-</td><td>51</td><td>455</td></tr><tr><td>Data privacy & security</td><td>524</td><td>-</td><td>-</td><td>-</td><td>-</td><td>524</td></tr><tr><td>Access control</td><td>127</td><td>296</td><td>2</td><td>-</td><td>-</td><td>574</td></tr><tr><td>Total capex</td><td>1,039</td><td>296</td><td>17</td><td>-</td><td>51</td><td>1,403</td></tr><tr><td colspan="7">Opex</td></tr><tr><td>Data privacy & security</td><td>-</td><td>142</td><td>142</td><td>142</td><td>142</td><td>567</td></tr><tr><td>Access control</td><td>25</td><td>127</td><td>135</td><td>135</td><td>135</td><td>558</td></tr><tr><td>Total opex</td><td>25</td><td>269</td><td>277</td><td>277</td><td>277</td><td>1,125</td></tr><tr><td>Total</td><td>1,065</td><td>564</td><td>294</td><td>277</td><td>328</td><td>2,528</td></tr></table>	\$'000 Jan 2025	26/27	27/28	28/29	29/30	30/31	Total	Capex							Maintain currency	388	-	16	-	51	455	Data privacy & security	524	-	-	-	-	524	Access control	127	296	2	-	-	574	Total capex	1,039	296	17	-	51	1,403	Opex							Data privacy & security	-	142	142	142	142	567	Access control	25	127	135	135	135	558	Total opex	25	269	277	277	277	1,125	Total	1,065	564	294	277	328	2,528
	\$'000 Jan 2025	26/27	27/28	28/29	29/30	30/31	Total																																																																							
	Capex																																																																													
	Maintain currency	388	-	16	-	51	455																																																																							
	Data privacy & security	524	-	-	-	-	524																																																																							
	Access control	127	296	2	-	-	574																																																																							
	Total capex	1,039	296	17	-	51	1,403																																																																							
	Opex																																																																													
Data privacy & security	-	142	142	142	142	567																																																																								
Access control	25	127	135	135	135	558																																																																								
Total opex	25	269	277	277	277	1,125																																																																								
Total	1,065	564	294	277	328	2,528																																																																								
Tables may not sum due to rounding																																																																														
Basis of costs	All costs in this business case are expressed in real unescalated dollars at January 2025 unless otherwise stated.																																																																													
Treated risk	As per risk matrix = Moderate																																																																													
Alignment to our vision	<p>The proposed cyber security program aligns with the <i>Customer Focussed</i> aspect of our vision. It delivers for customers by ensuring our IT and OT systems are secure and resilient to cyber threats, maintaining delivery of gas distribution services and keeping customer confidential information safe.</p> <p>The uplift in our data privacy and security also aligns with being <i>A Leading Employer</i>. It will help ensure the protection of employee sensitive information, reducing the likelihood of an employee data breach that may have adverse effects to employee mental wellbeing or cause other significant harm.</p> <p>The program reflects our vision of <i>Operational Excellence</i>, as it is the least cost option that delivers cyber technology and capabilities that are in line with good</p>																																																																													

<p>Consistency with the National Gas Rules (NGR)</p>	<p>industry practice, aligned across AGIG, and specifically designed to mitigate the key cyber security risks assessed to exist in the AGIG technology environment.</p> <hr/> <p>This program complies with the following National Gas Rules (NGR):</p> <p>NGR 79(1)/91 – Investing in cyber security capabilities will ensure our systems are resilient and robust, with security measures commensurate with the cyber risks impacting our business. The proposed cyber security capability uplifts are consistent with accepted good industry practice, several alternative options have been considered and unit rates and timing of equipment refreshes has been tested to achieve the lowest sustainable cost of delivering pipeline services.</p> <p>NGR 79(2) – All IT and OT systems and technology infrastructure are exposed to cyber threats. The confidentiality, integrity and availability of information and systems is critical to ensure the business can deliver its services effectively and in line with its various regulatory obligations and requirements, such as the SOCI Act, Privacy Act and our FIRB obligations. Our cyber security program will ensure our systems are secure and remain resilient to external threats and is therefore consistent with NGR 79(2)(c)(ii).</p> <p>NGR 74 – The forecast costs are based on the latest market rate testing, and project options consider the requirements of our application environment. Cost assessments have been conducted for each option based on the best information available at the time of developing this business case. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.</p>
<p>Stakeholder engagement</p>	<p>Customers consistently ranked price and affordability as their top priority. They also told us that they place a great deal of importance on safety and reliability of supply. Customers were clear they expect good communication and simple service that is resolution-focussed. Customers agreed that supplying cleaner energy was important, but that affordability is a key consideration for them.</p> <p>Our cyber security program is consistent with customers' top priorities of price and affordability and reliability and safety of supply as it will maintain the currency of our cyber security platforms and services in line with our legislative requirements, supporting reliability and safety of our services, and uplift our maturity levels to address the key identified cyber risks for our business.</p>
<p>Other relevant documents</p>	<p>This business case should be read in conjunction with:</p> <ul style="list-style-type: none"> • IT Investment Plan • Risk Management Policy and Operational Risk Model (together our Risk Management Framework) • Capitalisation Policy • Business case SA217: IT operational applications • Business case SA238: IT corporate applications • Business case SA239: IT sustaining Infrastructure • AGIG's Cyber Security Strategy

1.3 Background

Cyber threats continue to evolve, with both state and criminal cyber actors implementing new techniques and tactics to attempt to breach cyber defences. During the current AA period, the cyber security threats to which all businesses are exposed have continued to escalate, and energy utilities have been increasingly targeted globally.

Critical infrastructure entities in particular have come in for increasing attention, with multiple high profile attacks globally. The Australian Signals Directorate's (ASD) Annual Cyber Threat Report 2023-2024¹⁶ states that critical infrastructure made up 11% of all cyber security incidents, with the most frequently reported being electricity, gas and wastewater services. The report notes:

Australian critical infrastructure organisations are regularly targeted by malicious cyber actors because they provide critical services, hold sensitive data, and are often connected to other critical infrastructure organisations.

At AGIG this risk is not only applicable to our IT systems, but also our OT systems, and will only continue to escalate as the interconnectivity between IT and OT systems increases. The ASD notes that there has been an increase in malicious software developed specifically for OT networks as they:

...are increasingly interconnected and can have vulnerabilities that make them an easier cyber target. Secure information and communications technology and operational technology systems are necessary to protect Australia's critical services.

This increased cyber security threat level has been recognised by Government, with new and updated requirements for businesses providing essential services, such as AGIG, including the *SOCI Act*, *Cyber Security Act 2024*, *Australian Privacy Act 2018* and the more recent *Privacy Legislation Amendment (2022)*¹⁷.

1.3.1 Cyber security strategy

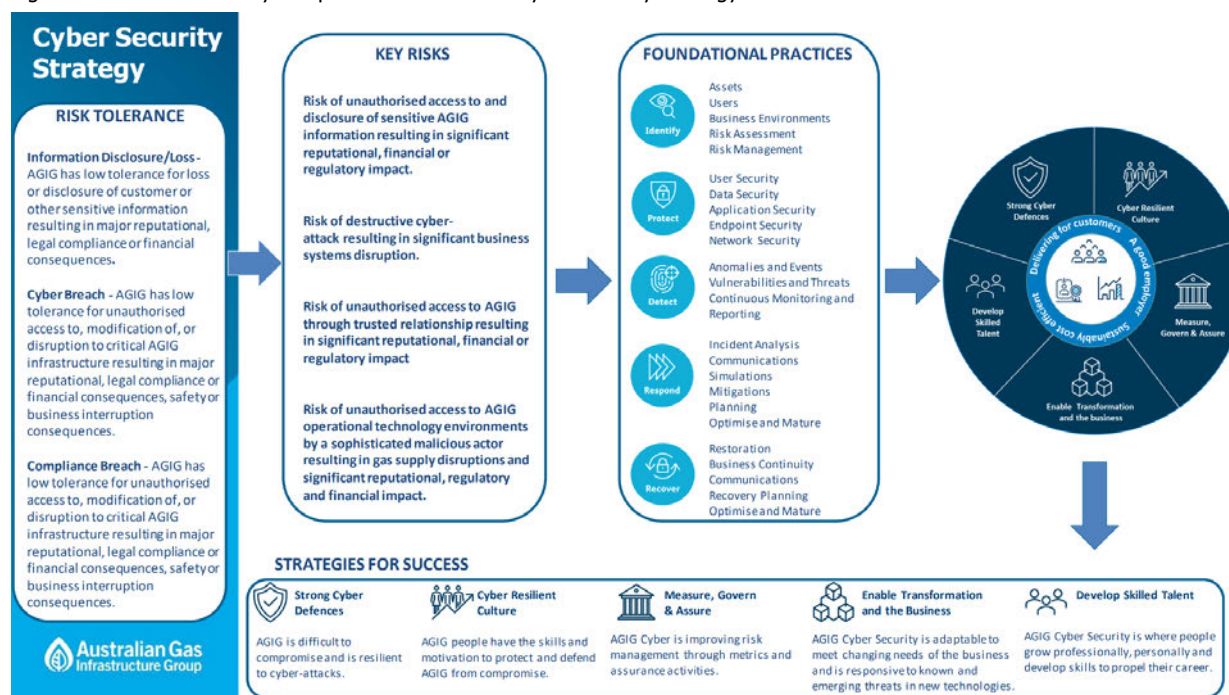
To meet our legislative requirements, address risks, and provide a stable framework from which to build our cyber programs, AGIG maintains its own cyber security strategy. This supports the AGIG strategy and values and the ongoing management of cyber security within all AGIG entities. The cyber security strategy drives an overarching cyber security risk management program which supports all AGIG business units, with costs shared appropriately between them.

¹⁶ <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/annual-cyber-threat-report-2023-2024>

¹⁷ Privacy Legislation Amendment, Australia Government Federal Register of Legislation (legislation.gov.au), available at: https://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id:%22legislation/bills/r6940_aspassed/0000%22

An overview of the AGIG Cyber Security Strategy is provided in Figure 0.1.

Figure 0.1: Overview of key components of the AGIG Cyber Security Strategy



A key component of the AGIG cyber security strategy is the cyber security risk management program, which is an ongoing program of activities to improve cyber controls and address weaknesses identified across AGIG.

1.3.2 SOCI Act amendments and new assessment framework

The recent amendments to the SOCI Act place new requirements on AGIG to:

- Identify and manage cyber hazards via an appropriate risk management program
- Formally select and adhere to a cyber security capability framework

Similar to most other Australian energy utilities, AGIG has adopted the Australian Energy Sector Cyber Security Framework (AESCSF) to meet this commitment.

Version 1 of the AESCSF was reviewed by AEMO with a formal working group over a period of 18 months. Version 2¹⁸ was released in November 2023. It has been updated to align with current international standards and address emerging technologies and evolving cyber threats, and better address the gas industry. Version 2 includes an additional 72 practices, reflective of a more mature framework for the energy industry. Figure 0.2 compares the changes to the security profiles between versions of the framework.

¹⁸ <https://aemo.com.au/-/media/files/initiatives/cyber-security/aescsf/2023/the-2023-aescsf-overview.pdf?la=en>

Figure 0.2: Comparison of security profiles between versions 1 and 2 of the AESCSF

	AESCSF v1				AESCSF v2			
	MIL-1	MIL-2	MIL-3	TOTAL	MIL-1	MIL-2	MIL-3	TOTAL
SP-1	57	27	4	88	62 (+5)	57 (+30)	4 (0)	123 (+35)
SP-2	0	94	18	200 (112+88)	0	123 (+29)	29 (+11)	275 (152+123) (+40)
SP-3	0	0	82	282 (82+200)	0	0	79 (-3)	354 (79+275) (-3)

Version 2 of the framework is currently recognised as an equivalent compliance framework for assessing cyber security maturity to support risk management program obligations under the SOCI Act. Under the SOCI Act, utilities must comply with security profile 1 (SP-1) of version 1 of the AESCSF. We currently comply with all requirements under SP-1.¹⁹

Using the AESCSF's 'Gas Criticality Assessment Tool', we have assessed the AGN SA gas distribution network as 'High Criticality'. The target state under the AESCSF for a high criticality utility network is SP-3. While this is not a regulatory obligation, the framework provides a method for assessing cyber security risks and guide our priorities and efforts in addressing weaknesses.

Our AGIG-wide cyber security program of works is therefore designed to:

1. Maintain our cyber security capabilities to achieve an adequate level of maturity across all cyber domains
2. Uplift our cyber security capabilities to achieve SP-3 over time where prudent and cost efficient to do so

1.3.3 Focus on data security and access control

During 2024, AGIG commissioned EY to assess the effectiveness of existing data security controls and other cyber security gaps within the IT space and recommend and prioritise cyber security uplift to better protect sensitive data. The engagement observed that

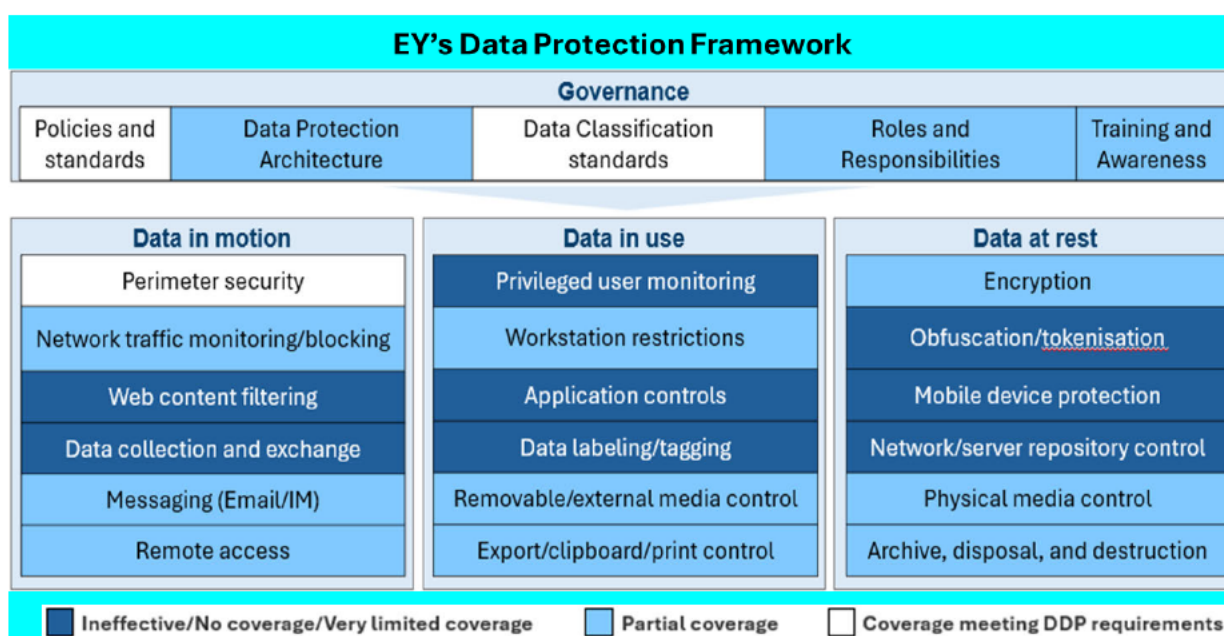
¹⁹ Following the release of version 2 of the framework, we engaged KPMG to assess the uplift required to meet the updated SP-1 standards across all technology areas. Several capability uplifts were identified, and these have now been implemented successfully, with AGIG Board attestation and formal submission to the Government in September 2024.

AGIG "had well defined security standards, policies and procedures and network reference architecture in alignment with industry standard frameworks". However:

- There is substantial effort required to uplift AGIG's own cyber security maturity for protecting sensitive data stored in several locations
- Some domains are identified as mature and do not require immediate attention
- Some domains have existing security controls and capabilities that require more effort to uplift the data protection maturity
- Some domains have missing controls and lack of these controls could potentially result in data breach or data exfiltration

EY assessed the AGIG data protection capabilities against their recommended data protection framework, shown in Figure 0.3. The shading on each box represents their assessment of AGIG's capability level associated with each control area.

Figure 0.3: EY's assessment of AGIG's data protection capability



EY used the above assessment and AGIG's enterprise risk management framework, to determine a roadmap of initiatives and recommendations to uplift data protection and access control maturity across all AGIG businesses. This prioritised initiatives with missing or weak controls and therefore the most potential to lead to a data breach. The resulting roadmap is shown in Figure 0.4.

Figure 0.4: Roadmap to uplift data protection and access control maturity across AGIG²⁰

Domains	Sub-Domains	Initiatives	Refer	Year 1	Year 2	Year 3
Governance	Training & Awareness	13 key recommendations guided through the AGIG Privacy Assessment report	2.4.1	←→		
Governance	DLP Architecture	Formalise the data protection architecture	2.4.2	←→		
Governance	Data Protection Ops Model	RACSI for Data management & governance	2.4.2	←→		
Data in Motion Data in Use	Web content filtering Applications Controls	Design and Implement CASB	2.4.5	←→		
Data at Rest	Mobile Device Protection	Design and Implement MDM solution	2.4.13	←→		
Data in motion	Messaging (Email / IM)	Uplift security design & controls for O365 & MS Teams	2.4.7	←→		
Data in Motion Data at rest	Data collection & exchange Network / Server Repository	Centralise data repository, i.e. MS SharePoint	2.4.6 & 2.4.15		←→	
Data in use	POC for Data Discovery tool	Run POC to finalise the data discovery tools across multiple data sources	2.1	←→		
Data in use	Data labelling / Tagging	Manual process & auto-labels	2.4.12	←→		
Data in use	Privileged Access Monitoring	Design and Implement a PAM solution	2.4.9		←→	
Data at rest	Encryption	Encryption strategy Consistent PKI Infra (including MDM SASE architecture (SD-WAN)	2.4.13	←→		
Data in use	Workstation restrictions	Enhance workstation security by developing & enforcing DLP policies and security controls	2.4.10	←→		
Data in motion	Perimeter security	Protect critical services from unauthorised lateral movement by blocking East-West traffic	2.4.4		←→	
Data in motion	Remote Access	Align remote VPN solution with ZTNA architecture	2.4.8		←→	
Data at rest	Physical media control Archive, Disposal & Destruction	Build process and controls related to data management lifecycle	2.4.16	←→		

This roadmap supports AGIG's internal assessment of the key risk areas over the upcoming AA period. Numerous initiatives are proposed in the new regulatory period to address these risks and implement the EY recommended controls, with the emphasis on those controls which best reduce risk to within AGIG's risk tolerance levels.

1.4 Risk assessment

Risk management is a constant cycle of identification, analysis, treatment, monitoring, reporting and then back to identification. 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.

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:

Figure 0.5: Risk management principles



²⁰ Cybersecurity & Technology Uplift Assessment & Recommendations, EY, October 2024

- AS/NZS ISO 31000 Risk Management – Principles and Guidelines
- AS 2885 Pipelines-Gas and Liquid Petroleum
- 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 AGN 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 moderate or higher, we will undertake investment to reduce the risk.

Seven consequence categories are considered for each type of risk:

8. **Health & safety** – Injuries or illness of a temporary or permanent nature, or death, to employees and contractors or members of the public
9. **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
10. **Operational capability** – Disruption in the daily operations and/or the provision of services/supply, impacting customers
11. **People** – Impact on engagement, capability or size of our workforce
12. **Compliance** – Impact from non-compliance with operating licences, legal, regulatory, contractual obligations, debt financing covenants or reporting / disclosure requirements
13. **Reputation & customer** – Impact on stakeholders' opinion of AGN, including personnel, customers, investors, security holders, regulators and the community
14. **Financial** – Financial impact on AGN, measured on a cumulative basis

The primary risk event being assessed is that our IT environment is not resilient enough to prevent a significant cyber incident or data breach. 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. This will result in organisational reputation and financial impact and corporate systems being unavailable for a prolonged period. The untreated risk²¹ rating is shown in Table 0.3.

Table 0.3: Untreated risk rating – Cyber security

Untreated	Health & Safety	Environ-ment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High

²¹ Untreated risk is the risk level assuming there are no risk controls currently in place. Also known as the 'absolute risk'.

Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

Security breaches, unavailability of corporate and operational systems and release of sensitive information gives rise to a number of significant consequences, as follows:

- *Operations* – The unavailability of operational systems (which are used to help us operate and maintain the network) may result in inefficient work order processing, an inability to make spatial and logical queries, and an inability to carry out timely repairs and maintenance. This can result in longer supply outages and slower emergency response
- *Compliance* – A security breach rendering our corporate IT 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 South Australian Gas Distribution Code and our obligations under the Retail Market Procedures
- *Reputation and customer* – A security breach may result in confidential customer data being compromised which in turn can impact on our reputation
- *Financial* – Non-compliance with the Retail Market Procedures, or other obligations relating to data management can result in financial penalties. There is also the risk of having to pay a premium to resolve compatibility issues with unsupported/obsolete infrastructure if the necessary renewals are not installed

1.5 Options considered

The following options have been considered to address the cyber security risks faced by AGIG and AGN:

- Option 1 – Maintain current environment
- Option 2 – Uplift maturity to address key identified risks
- Option 3 – Uplift maturity to meet SP-3 standards

Options associated with performing less than the current level of activity were considered but discounted as non-credible due to the high level of associated residual risk.

The options are discussed in the following sections.

1.5.1 Option 1 – Maintain current environment

Under this option, we would continue to maintain existing cyber security capabilities. This includes refreshing our:

- Server environment hosting on-premise cyber security platforms
- Core and internet firewall clusters in line with OEM recommendations

Under this option we would continue to maintain existing capabilities. However, we would not perform any activities that address new threats or mitigate the key OT, data security or identity access management risks that have been identified. We would not improve our maturity level beyond SP-1.

1.5.1.1 Advantages and disadvantages

The advantage of this option is that it requires no uplift in costs or resources compared with the current cyber security program. This means the program is predictable, deliverable and we will have certainty of costs.

The major disadvantage of this option is that it does not address the growing cyber security risk. The cyber threat environment is constantly evolving, so to not uplift our cyber security capabilities would expose the business and our customers to unnecessary, and exponentially increasing risk. Underinvestment during the next period also means we are likely to see a sharp rise in investment in future periods as existing firewalls and other cyber security assets become outdated and obsolete.

1.5.1.2 Achievement of objectives

Table 0.7 outlines how Option 1 will support the achievement of our vision objectives in the next AA period.

Table 0.4: Achieving objectives – Option 1

Vision objective	Alignment
Customer Focussed – Public Safety	N
Customer Focussed – Customer Experience	N
Customer Focussed – Cost Efficient	-
A Leading Employer – Health and Safety	N
A Leading Employer – Employee Experience	-
A Leading Employer – Skills Development	N
Operational Excellence – Profitable Growth	-
Operational Excellence – Benchmark Performance	N
Operational Excellence – Reliability	N
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	N

Option 1 does not align with our objective of being *Customer Focussed* or supporting *Sustainable Communities*, as it will not allow us to continue to uplift our cyber security capabilities to meet the increasing level of threat exposure. It will also not allow AGN to mitigate the risk to within our tolerance level and provide a level of service commensurate with that expected by our customers and would be considered socially responsible.

It does not align with being *A Leading Employer* as it will compromise our ability to understand and detect the evolve cyber security awareness needs of AGIG. It will also not support the protection of sensitive employee information. Such a breach could, for example, result in harm or adverse effects to an employee's financial or mental wellbeing.

Option 1 does not reflect *Operational Excellence* as it does not address data privacy risks that we are required by law to mitigate. Recent high profile cyber security breaches have

been documented as costing businesses tens of millions of dollars to rectify; in addition, the potential for a \$50 million or greater fine under modified privacy legislation. The lack of continued investment in managing our cyber security would increase our overall costs over time as we would need to manage incidents in a reactive manner which is generally more costly.

1.5.1.3 Cost assessment

Option 1 is estimated to cost \$0.5 million in capex. There is no uplift in opex associated with this option.

Table 0.5: Cost estimate – Option 1, \$'000 January 2025

Project	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Cyber Security technology refresh	117	-	16	-	51	183
Corporate Firewall/s refresh	272	-	-	-	-	272
Total	388	-	16	-	51	455

The delivery of AGIG shared capabilities (i.e. the IT refresh programs in Table 0.5) has been allocated to AGN based on revenue, resulting in a 16.9% share being allocated to AGN SA. The AGN specific components are a direct allocation of estimated costs for the refresh of these cyber security platforms.

1.5.1.4 Risk assessment

Option 1 does not moderate the threat, the frequency and/or consequence to reduce the risk rank from the untreated risk. This option is inconsistent with our risk tolerance as it does not lower the risk to intermediate or lower. This option is not ALARP.

Figure 0.6: Risk rating – Option 1

Option 1	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

1.5.2 Option 2 – Uplift maturity to address key identified risks

In addition to maintaining existing cyber security capabilities (Option 1), this option proposes uplifting our cyber security to address the key weaknesses in our data security and access control identified through our EY engagement. This program is designed to keep AGIG's customers and organisation data secure, reduce cyber security risk, increase cyber resilience and mitigate the increasing cyber security threat.

It is a holistic program that encompasses all AGIG business units, delivering improvements in IT and business management processes and supporting consistent, ongoing cyber security capability across all corporate IT environments. In addition to the refresh programs in Option 1, the Option 2 program includes the following capabilities:

- Data leakage protection
- Cloud access security broker
- Enhanced data governance and protection
- Enhanced identity access management (IAM) and privileged access management (PAM)
- Zero trust network

More information on these projects is provided in Appendix A.

1.5.2.1 Advantages and disadvantages

The advantage of this option is that it will help protect our most critical systems from the growing cyber threat. This option would also only require a moderate uplift in resourcing and expenditure, which means the program is deliverable and the level of maturity we are aiming for is attainable. This option reflects our target risk tolerance and is considered ALARP.

A disadvantage of this option is that some aspects of our IT and OT may be more vulnerable than if we were to achieve an SP-3 level of maturity. However, we are mitigating this risk by focusing on the most business-critical systems and making sure that they are suitably secure.

We consider this option achieves the best balance between expenditure and risk reduction.

1.5.2.2 Achievement of objectives

Table 0.6 outlines how Option 2 will support the achievement of our vision objectives in the next AA period.

Table 0.6: Achieving objectives – Option 2

Vision objective	Alignment
Customer Focussed – Public Safety	Y
Customer Focussed – Customer Experience	-
Customer Focussed – Cost Efficient	-
A Leading Employer – Health and Safety	Y
A Leading Employer – Employee Experience	-
A Leading Employer – Skills Development	Y
Operational Excellence – Profitable Growth	-
Operational Excellence – Benchmark Performance	Y
Operational Excellence – Reliability	Y

Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	Y

This option delivers against all of our vision objectives of being *Customer Focussed*, being *A Leading Employer* and displaying *Operational Excellence* as it proactively maintains a secure and resilient IT environment to support the operation of the South Australian network and corporate business processes, in line with good industry practice at a sustainable cost over the medium to longer term.

Option 2 aligns with our objective of being *Customer Focussed*. It provides robust and resilient IT systems with a reduced risk of a security breach that could compromise our network or business critical operations. Continuing to uplift our cyber security capability reduces the risk that a cyber-attack could result in our IT systems being rendered unusable for an extended period, potentially impacting customer supply. It would also help prevent a cyber-attack resulting in the release of customer information and data, thereby protecting our valuable customer relationships.

It aligns with being *A Leading Employer* as it will enhance our ability to continue to evolve our ongoing cyber security awareness program. In addition, it will help ensure the protection of sensitive employee information. A security breach resulting in harm to an employee may have adverse effects to employee mental wellbeing or other significant harm to these individuals.

It is consistent with the *Operational Excellence* strategic pillar as it is the least cost option that delivers cyber technology and capabilities that are in line with good industry practice, aligned across AGIG, and specifically designed to mitigate the key cyber security risks assessed to exist in the AGIG technology environment. It will keep our operational and corporate systems secure to ensure we are able to conduct work order processing, make spatial and logical queries, and carry out timely repairs and maintenance. This can result in longer supply outages and slower emergency response.

1.5.2.3 Cost assessment

The proposed forecast for the preferred option comprises \$1.6 million of capex as shown in Table 0.7.

Table 0.7: Capex – Option 2, \$'000 January 2025

Project	2026/2 7	2027/2 8	2028/2 9	2029/3 0	2030/3 1	Total
Total maintain currency IT – per option 1	388	-	16	-	51	455
Uplift data privacy & security (IT)						
DLP solution	230	-	-	-	-	230
CASB solution	145	-	-	-	-	145
Data governance and protection framework	149	-	-	-	-	149
Total	524	-	-	-	-	524

Uplift access control (IT)						
Zero trust network architecture	102	184	-	-	-	286
PAM session management	-	111	-	-	-	111
IAM platform enhancements	25	-	2	-	-	27
Total	127	296	2	-	-	424
Option 2 uplift total	651	296	2	-	-	1,066
Total	1,039	296	17	-	51	1,403

Tables may not sum due to rounding

There is also an opex step change of \$1.1 million required under this option, as shown in Table 0.8.

The increase related to data privacy and security includes funding for a Privacy Officer to provide guidance, direction and support for data security and governance, and the ongoing licensing costs associated with the DLP and CASB software which are both being provided as a software as a service²².

The opex uplift related to access control is required to provide licenses for all AGN SA users for Zscaler Internet Access (ZIA) and Zscaler Private Access (ZPA) services, and uplift to licence costs for our PAM software and SailPoint Identity Security Cloud to reflect recent historical costs.

Table 0.8: Opex – Option 2, \$'000 January 2025

Project	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Uplift data privacy & security (IT)						
DLP solution	-	75	75	75	75	300
CASB solution	-	67	67	67	67	266
Total	-	142	142	142	142	567
Uplift access control (IT)						
Zero trust network architecture	-	101	101	101	101	406
PAM session management	-	-	8	8	8	25
IAM platform enhancements	25	25	25	25	25	127
Total	25	127	135	135	135	558
Option 2 uplift total	25	269	277	277	277	1,125

Tables may not sum due to rounding

The delivery of AGIG shared capabilities (i.e. the IT refresh programs in Table 0.7 and Table 0.8) has been allocated to AGN based on revenue, resulting in a 16.99% share being allocated to AGN SA. The AGN specific components are a direct allocation of estimated costs for the refresh of these cyber security platforms.

²² More information on the capitalisation associated with SaaS solutions is provided in the IT Investment Plan.

1.5.2.4 Risk assessment

Implementing the initiatives in Option 2 results in a reduction in the likelihood of a significant cyber incident or data breach resulting in corporate IT system outage, data exfiltration or extortion attempt. This reduces the residual risk from high to moderate, as shown in Table 0.9. This is consistent with our operational risk framework, as it reduces the residual risk outcome from high to moderate or lower.

Table 0.9: Risk rating - Option 2

Option 2	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Low	Low	

1.5.3 Option 3 – Uplift maturity to meet AESCSF SP-3 requirements

Option 3 proposes uplifting all controls required for AGN to meet the AESCSF SP-3 standards, consistent with our rating as a 'high criticality' gas distribution service provider. In addition to the refresh programs in Options 1 and 2, the Option 3 program includes an uplift in the following capabilities:

- Asset discovery and management tools integration
- Monitoring and security alert functionality for assets
- Penetration testing and secure device configuration
- IAM and PAM
- Physical security

1.5.3.1 Advantages and disadvantages

The advantage of this option is that it will significantly improve the resilience of our IT and OT landscape, and will allow us to meet the AESCSF SP-3 standards. It will fully mitigate the identified risks in the energy sector for a high criticality network. This option will set a solid platform for ongoing cyber security investment, and would ensure we are best placed to address the emerging threats as they arise.

The disadvantage of this option is the cost and the resources required to meet all the requirements of SP-3. While we will invest to address key risks associated with our network and organisation, it is likely that we will not necessarily achieve all maturity levels across all capabilities. Taking a more general approach to meeting the SP-3 standards may mean that we spend more than we would in a more targeted, business-specific approach as we expect under Option 2. However, if there are risks we need to mitigate in the next AA period, we will increase our program as required.

1.5.3.2 Achievement of objectives

Table 0.10 outlines how Option 3 will support the achievement of our vision objectives in the next AA period.

Table 0.10: Achieving objectives – Option 3

Vision objective	Alignment
Customer Focussed – Public Safety	-
Customer Focussed – Customer Experience	Y
Customer Focussed – Cost Efficient	-
A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	Y
A Leading Employer – Skills Development	Y
Operational Excellence – Profitable Growth	N
Operational Excellence – Benchmark Performance	N
Operational Excellence – Reliability	Y
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	Y

Option 3 aligns with our objective of *Customer Focussed*. It provides robust and resilient corporate systems with a reduced risk of a security breach that could compromise sensitive customer information. Continuing to uplift our operational technology cyber security capability reduces the risk that a cyber attack could result in operational systems being rendered unusable for a period and potentially impacting customer supply.

It aligns with being *A Leading Employer* as it will enhance our ability to continue to evolve our ongoing cyber security awareness program. In addition, it will help ensure the protection of employee sensitive information. A security breach resulting in harm to an employee may have adverse effects to employee mental wellbeing or other significant harm to these individuals.

However, this option is not consistent with *Operational Excellence*. While it supports meeting SP-3 which is considered appropriate for a high criticality network, it includes developing controls that are outside of what is required to reduce risk to an acceptable level, and is consequently not the least cost appropriate option.

1.5.3.3 Cost assessment

Option 3 is a significant uplift above Option 2. It is \$1.9 million forecast capex for the period, as shown in the following table.

Table 0.11: Capex – Option 3, \$'000 January 2025

Project	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Total maintain currency – per option 1	388	-	16	-	51	455

Total risk-based uplift – per option 2	651	296	2	-	-	1,066
Additional cyber security capabilities (Achieve SP-3)						
Asset management capability uplift	113	-	-	-	-	113
Security baseline control and management	-	142	52	-	-	194
Security testing (technology (ITIL) change control driven approach)	47	17	-	-	-	64
Situational awareness (SA - SP3 capabilities)	49	-	-	-	-	49
IAM enhanced capability	17	-	-	-	-	17
PAM (AGN CSN) (capability uplift)	93	-	-	-	-	93
Physical security (central capability)	113	-	-	-	-	113
SP-3 uplift total	319	159	52	-	-	530
Total	1,358	454	70	-	51	1,933

There is also an opex step change of \$2.0 million required under this option, as shown in Table 0.12. This includes the uplift outlined in Option 2, and costs associated with the following initiatives to increase our capabilities in line with the requirements of SP-3.

The uplift to meet SP-3 requires the following:

- 1 additional cyber security personnel
- Uplift in asset management system licensing costs
- Ongoing costs associated with the new security configuration software provided as SaaS
- An ongoing program of security testing
- An uplift in our security information and event management, and threat intelligence solution
- An uplift in workforce vetting standards
- Uplift in physical security, including remote access control and surveillance subscriptions

More information on these requirements and how they map against SP-3 is provided in Appendix A.

Table 0.12: Opex – Option 3, \$'000 January 2025

Project	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Total risk-based uplift – per option 2	29	302	311	311	311	1,264
Additional cyber security capabilities (Achieve SP-3)						
Asset management capability uplift	-	21	26	26	26	100
Security baseline control and management	-	-	87	103	103	293
Security testing (technology (ITIL) change control driven approach)	-	23	46	46	46	161
Situational awareness	32	52	52	73	52	262
IAM enhanced capability	2	2	2	2	2	10

Project	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Physical security (central capability)	-	18	18	18	-	55
SP-3 uplift total	34	117	232	268	230	880
Total	59	385	509	545	507	2,005

Tables may not sum due to rounding

1.5.3.4 Risk assessment

While Option 3 does add more cyber security controls and mitigate risk further than Option 2, Table 0.13 shows that it does not reduce risk enough to move the residual risk rating for this option to less than the rating assessed for Option 2, i.e., the key risks driving the current high risk rating are already being addressed through the controls added under Option 2.

Table 0.13: Risk rating - Option 3

Option 3	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Low	Low	

1.6 Summary of options assessment

To assess the options, the costs, objectives and risk are considered for each option. A summary of the option assessment is shown in Table 0.17.

Table 0.14: Comparison of options

Option	Achievement of objectives	Costs	Treated risk
Option 1	This option would not be consistent with any of our strategic pillars	\$0.5 million capex	High residual risk Does not adequately address increasing cyber security threats risks associated with key risk areas
Option 2	This option is consistent with all our strategic pillars	\$1.4 million capex \$1.1 million opex	Moderate residual risk Addresses key risk areas ALARP
Option 3	This option achieves our objectives, however it does so at a substantially higher cost than Option 2 and therefore is less aligned with the strategic pillar of Operational Excellence	\$1.9 million capex \$2.0 million opex	Moderate residual risk Addresses key risk areas

1.6.1 Proposed solution

Option 2 is the proposed solution because it will allow us to:

- Continue to maintain the existing cyber security risk management program and capabilities established in prior regulatory periods
- Uplift AGN's cyber security capabilities to address the key identified risk areas of:
 - Data privacy and security

- Access control

1.6.2 Why is the recommended option prudent?

Option 2 is the most prudent option because:

- It provides the means for us to maintain compliance with AESCSF SP-1, our legislated SOCI requirement
- It reduces the untreated risk to an acceptable level in line with our risk management framework
- It is efficient and delivers a prudent reduction in cyber security risk, being the least cost option for reducing risk to within tolerance levels. While our cyber security framework, the AESCSF, suggests that SP-3 is an appropriate maturity level for our high criticality gas distribution business, and will address a broad range of risks across all domains, that alternative comes at a significant additional cost to customers whilst not significantly further reducing cyber risk at this time
- It avoids significant recovery costs associated with a cyber security breach as well as the potential for \$50 million or more in fines from the updated privacy legislation
- It is consistent with stakeholder requirements and our vision
- The delivery of the scope of works is achievable in the proposed time frame

1.7 Estimating the efficient costs

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

For all of the systems identified for change in the next AA period, estimates have been developed based on historical costs of similar projects, quotes from vendors based on products identified by the AGIG IT architects as being reasonable to base a budgeting process on. Vendors provided indicative pricing on their systems and maintenance costs and provided recommendations on ballpark implementation costs.

IT initiatives will be implemented by three potential groups of resources. Internal staff generally undertake IT project management, the management and finance aspects of IT, and all of the business user involvement (e.g. business requirements, testing, and training). An internal rate card has been agreed that defines the unit costs associated with all of the internal resources.

IT support is currently outsourced with these resources generally involved in all IT initiatives to implement products into the environment and support processes (e.g. installing an application on a server). A rate card for these resources is defined as part of the ongoing management of that contract.

Product or service specific skills are often required in IT initiatives to implement products (e.g. Vendor contractors configuring their systems). These rates are negotiated during the procurement phase using AGN's Purchasing Policy.

All procurement processes for IT applications will comply with our Procurement Policy and Purchasing Procedure and will follow transparent, competitive tendering processes to select the best value for money solution.

Overall, there does not appear to be many factors affecting the sensitivity of these estimations, however a small amount is costed in USD and therefore susceptible to foreign exchange fluctuations.

1.7.1 Consistency with the National Gas Rules

1.7.1.1.1 NGR 79(1)/91

The proposed expenditure on Cyber Security is consistent with the requirements of NGR 79(1) in relation to the capital expenditure, and NGR 91 in relation to the operating expenditure because it is:

- **Prudent** – the expenditure is necessary in order to address the risks of Cyber Security identified. The project is also based on taking a planned and proactive approach to cyber risk controls which is commensurate with the cyber risk exposure. The proposed expenditure can therefore be seen to be of a nature that would be incurred by a prudent service provider.
- **Efficient** – the forecast expenditure is based on historic costs for similar work as well as estimates from relevant vendors of likely solutions. A formal procurement process will be undertaken once the project enters its delivery phase to ensure efficient prices are achieved through a competitive tender process. The proposed expenditure can therefore be considered consistent with the expenditure that a prudent service provider acting efficiently would incur.
- **Consistent with accepted and good industry practice** – the proposed initiatives will improve our cyber maturity as measured against the relevant industry cyber framework (e.g. AESCSF)
- Achieves the **lowest sustainable cost of delivering services** – Uplifting our cyber security maturity by mitigating key identified risks represents the lowest sustainable cost for AGN. While uplifting maturity commensurate with our AESCSF high criticality rating would also mitigate risk appropriately, this option comes at a significantly higher cost to customers. A lower cost option could result in significantly higher costs to recover from cyber security incidents, including data breaches, as well as the potential for significant legislated fines.

1.7.1.1.2 NGR 79(2)

The proposed expenditure on Cyber Security is required to maintain the integrity of services through Cyber Security controls commensurate with the cyber risk we face and is therefore consistent with NGR 79(2)(c)(ii).

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 the business is able to deliver its services effectively and in line with its various regulatory obligations and requirements, such as Critical

Infrastructure Act, Privacy Act and FIRB obligations. This requires investment to ensure our systems are secure and remain resilient to external threats.

1.7.1.1.3 NGR 74

NGR74(2) requires that a forecast of estimate:

- a) must be arrived at on a reasonable basis; and
- b) must represent the best forecast or estimate possible in the circumstances.

The forecast costs in this business case are based on the latest market rate testing, and project options consider the asset management requirements as per the IT Investment Plan. Cost assessments have been conducted for each option based on the best information available at the time of developing this business case. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.

Country	Region	Year	Value
Country A	Region A	2010	Value A1
		2011	Value A2
		2012	Value A3
		2013	Value A4
Country B	Region B	2010	Value B1
		2011	Value B2
		2012	Value B3
		2013	Value B4
Country C	Region C	2010	Value C1
		2011	Value C2
		2012	Value C3
		2013	Value C4
Country D	Region D	2010	Value D1
		2011	Value D2
		2012	Value D3
		2013	Value D4
Country E	Region E	2010	Value E1
		2011	Value E2
		2012	Value E3
		2013	Value E4

Appendix B Summary of risk assessments

Untreated	Health & Safety	Environ-ment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

Option 1	Health & Safety	Environ-ment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	Unlikely	High
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Low	Negligible	High	Low	Moderate	Moderate	Moderate	

Option 2	Health & Safety	Environ-ment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Low	Low	

Option 3	Health & Safety	Environ-ment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Moderate
Consequence	Minor	Minimal	Major	Minor	Significant	Significant	Significant	
Risk level	Negligible	Negligible	Moderate	Negligible	Low	Low	Low	

SA241 – AGN transition

1.1 Project approvals

Table 0.1: SA241 AGN transition – Project approvals

Prepared by	Brooke Palmer, Head of IT Business Engagement – Distribution
Reviewed by	Peter Bucki, Head of Regulation
Approved by	Brett Miller, Chief Information Officer

1.2 Project overview

Table 0.2: SA241 AGN transition – Project overview

Description of problem /opportunity	<p>APA Group operates the South Australian gas distribution network on behalf of AGIG. AGIG owns the network, with APA being the delivery partner under a longstanding contractual relationship. That contract is coming to an end in 2027, after which AGIG will commence operating the network itself. As part of this transition, the IT services used by APA to operate the network must transition from APA's IT environment to AGIG's environment.</p> <p>The scope of the AGN transition includes:</p> <ul style="list-style-type: none"> • Software applications • Infrastructure, security and connectivity arrangements • IT support model <p>The APA IT transition period is scheduled to commence from 1 July 2027 and is expected to take around 18 months. The transition is an AGN-wide program, as APA also operates the AGN Victoria and AGN Queensland networks. Transition costs are allocated between the AGN networks based on customer numbers, with the AGN SA allocation being 35.24%.</p> <p>This business case considers the options for delivering the AGN transition. The costs presented in the main body of this business case are the AGN SA allocation only. Whole of IT transition costs (AGN wide) are presented in Appendix B.</p>
Untreated risk	As per risk matrix = High
Options considered	<ul style="list-style-type: none"> • Option 1 – Lift/shift: Replicate the current APA environment and parallel run as a separate standalone end-state environment within AGIG (\$37.9 million capex and \$56.0 million opex) • Option 2 – Lift/shift & Merge: Transition to an interim replica of APA's current environment for AGN within AGIG, before merging and transforming the two environments into one consolidated and optimised end-state environment (\$57.8 million capex, \$53.0 million opex) • Option 3 Merge: Merge and transform the existing APA environment into a consolidated and optimised end-state environment within AGIG (\$75.3 million capex, \$41.9 million opex)
Proposed solution	Option 2 is recommended because it is low risk and is the lowest overall cost option over the longer term (10 years). A lift, shift and merge approach gets critical IT systems into our environment in a short timeframe and provides opportunity for rationalising process/systems and leveraging the broader AGIG IT environment.

Estimated cost	The forecast direct capital and operating cost during the next AA period is shown below.						
	\$'000 Jan 2025	26/27	27/28	28/29	29/30	30/31	Total
	Total capex	2,971	32,237	6,954	14,033	1,559	57,755
	Total opex	-	14,237	17,136	12,379	9,285	53,036
Basis of costs	All costs in this business case are expressed in real unescalated dollars of January 2025 unless otherwise stated.						
Treated risk	As per risk matrix = Low						
Alignment to our vision	<p>This project aligns with the <i>Operational Excellence and Customer Focussed</i> aspects of our vision, as we are transitioning IT systems that are fundamental to the operation of the network to the AGIG IT environment. The transition will ensure critical IT data and applications are available to AGIG staff and within AGIG control. This is essential for the ongoing reliability of operations, as well as being consistent with the practices of other network owners and of increasing importance as a responsible entity of critical infrastructure.</p> <p>End-to-end control and visibility of operational applications, data, and IT support will also allow us to seek the most efficient mix of delivery methods and external partners for ongoing network operations post-June 2027. This will promote cost efficiency over the longer term.</p>						
Consistency with the National Gas Rules (NGR)	<p>NGR 79(1)/91 – Transitioning IT data, applications and processes from APA to AGIG is fundamental to the ongoing operation of the network. As a critical infrastructure owner, it is essential IT systems such as enterprise asset management and the metering & billing system are available and in the control of AGIG staff, therefore it is prudent to lift and shift them to the AGIG operating environment as quickly as practicable, and then merge them into AGIG’s broader IT framework. The merge process will identify opportunities for rationalisation and efficiency improvements. This lift, shift and merge approach is the lowest risk and most expedient method of getting these IT systems within AGIG’s control. Though the initial IT transition cost is substantial, bringing operational IT systems into the AGIG environment offers longer term opportunities for efficiencies and productivity improvements. This is because AGIG (as the network owner) will have full autonomy and operational control over IT upgrades, strategies and investments. The transition is therefore consistent with the actions of a prudent network operator and will ultimately achieve the lowest sustainable cost of delivering pipeline services.</p> <p>NGR 79(2)/91 – The proposed expenditure is required to maintain integrity of services by ensuring operational IT systems are available to AGIG staff.</p> <p>NGR 74 – The forecast costs are based on the latest market rate testing, and project options consider the requirements of our application environment. Extensive option assessments and project planning has been undertaken, underpinned by advice from a third-party expert consultancy.</p> <p>Cost assessments have been conducted for each option based on the best information available at the time of developing this business case. The estimate has therefore been arrived at on a reasonable basis and represents the best estimate possible in the circumstances.</p>						
Stakeholder engagement	<p>Customers consistently ranked price and affordability as their top priority. They also told us that they place a great deal of importance on safety and reliability of supply. Customers were clear they expect good communication and simple service that is resolution-focused. Customers agreed that supplying cleaner energy was important, but that affordability is a key consideration for them.</p> <p>Transitioning IT systems from APA to AGIG is fundamental to maintaining the safe and reliable operation of our gas distribution network in South Australia. Core applications such as the enterprise asset management system, metering and billing system, call</p>						

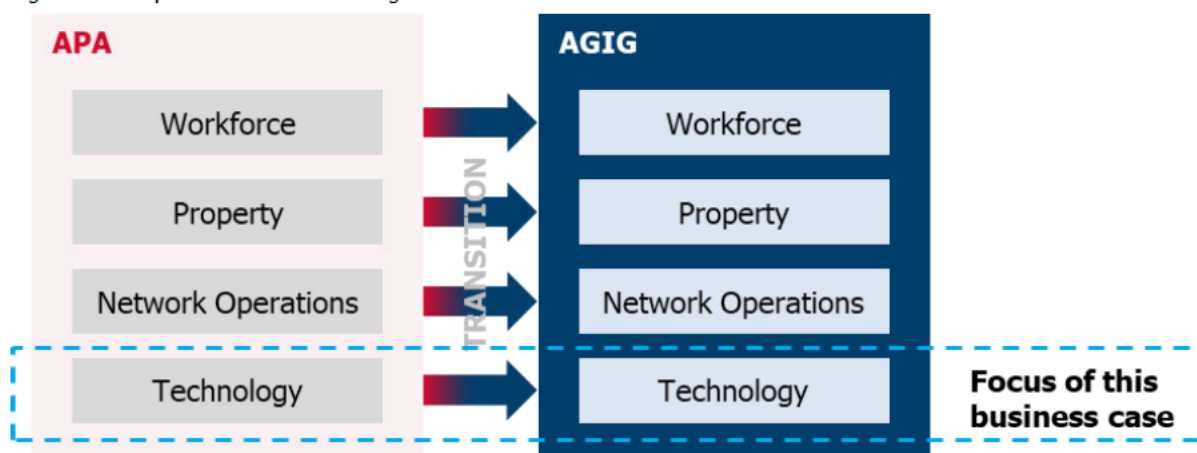
Other relevant documents	centre, field mobility and the full retail contestability (FRC) gateway are central to our daily operations. It is therefore critical we transition these applications to the AGIG IT environment and make them accessible to our people. This will enable us to maintain continuity of service to our customers.
	<p>This business case should be read in conjunction with:</p> <ul style="list-style-type: none"> IT Investment Plan Other technology Business Cases: IT Operational Apps, IT Corporate Apps, IT Sustaining Infrastructure and IT Cybersecurity

1.3 Background

AGIG is party to a longstanding service agreement with the APA Group for the provision of asset management, field services, finance, HR and IT support. This service agreement applies to the AGN South Australia, AGN Victoria and AGN Queensland networks, which APA operate on AGIG's behalf. This service agreement is set to expire on 30 June 2027.

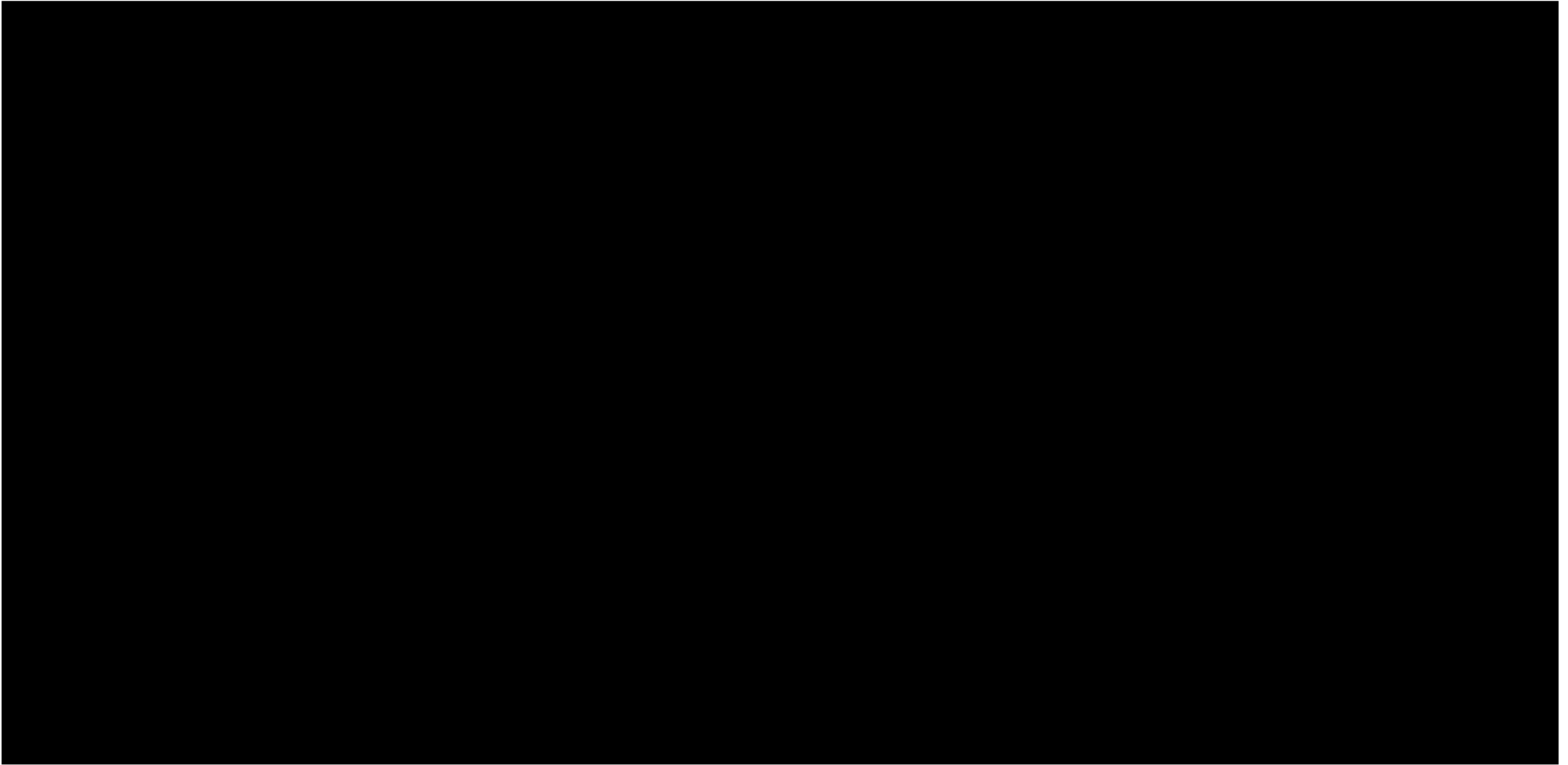
AGIG is seeking to consolidate the management and operations of its various gas networks, essentially bringing network operations 'in-house' rather than relying on a single delivery partner. The transition of operational activities is an exhaustive and complex exercise, which will see workforce, property, network operations and technology transfer to AGIG. This business case covers the **technology transition only**.

Figure 0.1: Scope of services transferring from APA to AGIG



The transition period is scheduled to commence from 1 July 2027 and is expected to take around 18 months, with cutover and hypercare activities extending into the first half of 2029 (see Figure 0.4).

The IT transition will be a period of intensive work and considerable risk. It features migration of around 50 applications from APA's IT environment to AGIG's IT environment, as well as data, infrastructure, security and connectivity arrangements, and the IT support model. Figure 0.2 summarises the scope of applications and data being transferred to AGIG.



To help refine options and guide the transition process, we have developed the following IT integration principles, split into three key principles with seven sub-principles. These principles will be used to assess IT integration options within this business case and act as a starting point for joint IT transition planning and execution with APA.

Figure 0.3: IT integration principles

Speed to Value

- 1 Transfer before transform**
Move business functions, processes, data and technology as-is where possible (i.e. Lift/Shift)
- 2 Shortest path to Day 2**
Minimise separation requirements and required TSA duration where possible

Cost Certainty

- 3 Minimise migration costs to target state**
Select cost-effective solutions and minimise technology uplift during transition, while balancing risk
- 4 Minimise stranded costs (including write-offs)**
Consider in solution and separation approach, and TSA exits

Business Continuity

- 5 Minimise business impacts**
Ensure business continuity, seamless customer and supplier operations
- 6 Transition all necessary data**
Satisfy legal and regulatory requirements, protect confidentiality
- 7 Staged go lives**
Application and infrastructure go live waves to reduce risk and ensure rapid TSA exits (no single event)

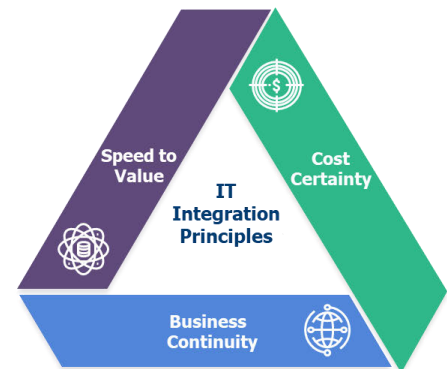
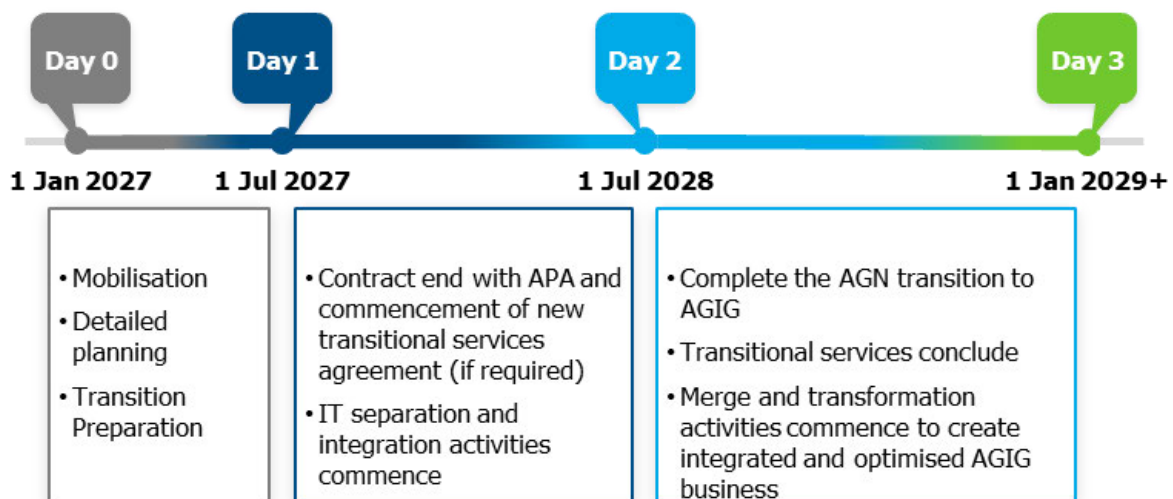


Figure 0.4: Transition timeline



This IT Transition business case takes a bottom-up approach (across three different options) to estimating the resourcing and costs required to execute the AGN IT transition. The analysis builds on previous work conducted at a high-level to capture the start of the transition activities for the purposes of the Victorian regulatory submission (2024-28). It now includes:

- A more detailed bottom-up analysis for each of the applications involved based on application criticality, size and complexity
- Build costs for infrastructure to support both the applications and the people (i.e. end user devices) transitioning in
- Security considerations for both the applications and infrastructure builds
- Integration management office costs for overall program and project management, governance, oversight and change management

- Ongoing operating costs for application support, infrastructure support, security, that were not incorporated into the Victorian submission as the cutoff date for the regulatory period only resulted in the transition occurring not the ongoing operation and maintenance of the environment

An important part of the options assessment is baselining the current costs. AGN SA currently pays around \$7.7 million per year for the technology services provided by APA. This is 35.24% of the total AGN/APA shared services cost, allocated to AGN SA based on customer numbers.

Table 0.3 shows the estimated costs that would be paid by AGIG to APA over the next five years for the provision of IT services to support the AGN business under the current agreement between the two parties. An annual growth rate of 4.9% p.a. has been applied to the shared service recharge, which is the 3-year average historical increase incurred by AGIG prior to FY25 (net of inflation).

Table 0.3: Baseline IT costs paid to APA annually – AGN SA allocation, \$'000 January 2025

Baseline IT costs (opex) SA allocation of total AGN costs 35.24%	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Shared service recharge	7,759	8,141	8,541	8,961	9,402	42,804

All options in this business case can be compared against this baseline opex. It is important to note that the opex assumptions in Table 0.3 are an extrapolation of current costs and should be considered indicative only and not a definitive forecast of future opex.

1.4 Risk assessment

Risk management is a constant cycle of analysis, treatment, monitoring, reporting and then identifying once again, with a commitment to balance outcomes sought with delivery and cost implications considered and assessed.

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.

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 and activities required to ensure safety and compliance are not compromised, while delivery of this outcome is done as efficiently and effectively as possible.

The risk rating assesses the consequence and likelihood of the risk. The risk of an event associated with failure of an asset is rated based on the combined effect of the consequence and likelihood rating to provide an overall risk rating. This risk rating guides the risk management and mitigation activities and facilitates prioritisation.

Figure 0.5: Risk management principles



Our Operational Risk Framework is based on AS/NZS 2885 and requires all identified risks ranked as intermediate or above to be addressed. For risks ranked as high we must *'Modify the threat, the frequency or the consequence to reduce the risk rank to intermediate or lower'*.

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 moderate or higher, we will undertake investment to reduce the risk.

Seven consequence categories are considered for each type of risk:

- **Health & safety** – injuries or illness of a temporary or permanent nature, or death, to employees and contractors or members of the public
- **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
- **Operational capability** – disruption in the daily operations and/or the provision of services/supply, impacting customers
- **People** – impact on engagement, capability or size of our workforce
- **Compliance** – the impact from non-compliance with operating licences, legal, regulatory, contractual obligations, debt financing covenants or reporting / disclosure requirements.
- **Reputation & customer** – impact on stakeholders' opinion of AGN, including personnel, customers, investors, security holders, regulators and the community
- **Financial** – financial impact on AGN, measured on a cumulative basis

The primary risk event being addressed by the AGN transition is that critical operational data and applications are not available for AGIG to be able to operate the network, and therefore we cannot provide network services.

The overall risk rating associated with not transitioning the APA IT applications, infrastructure and security arrangements to AGIG's environment is rated high. If the IT transition is not delivered, then AGIG's ability to operate the network will be significantly compromised as access to critical systems is likely to be constrained or available only subject to cost premia. The likelihood of the primary risk event occurring would become 'frequent' (many times in one year), meaning that the following operational, compliance and financial risks would be high:

- **Operational** – if AGIG has limited access to critical applications (for example [REDACTED])
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
- **Compliance** – the metering and billing system, meter data management system and the FRC gateway (which provides the interface with AEMO for retail market obligations) are all currently owned and operated by APA. [REDACTED]
[REDACTED]
[REDACTED]

- **Finance** – if IT systems are not transitioned, AGIG would have to procure new applications, infrastructure and security arrangements, developing an operational IT environment virtually from scratch. Even if this were feasible, AGIG still may not have access to historical data. Alternatively, AGIG may need to enter into a new contractual agreement with APA, leasing applications and data access under a hosting arrangement. This is likely to be priced at a premium and would not be a preferable or sustainable arrangement for either party.

The untreated risk rating is summarised in the following table.

Figure 0.6: Untreated risk rating – IT operational apps

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	High
Consequence	Minimal	Minimal	Significant	Minor	Significant	Minor	Significant	
Risk level	Low	Low	High	Moderate	High	Moderate	High	

1.5 Options considered

The options considered are:

- **Option 1 – Lift/shift** (\$37.9 million capex and \$56.0 million opex)
- **Option 2 – Lift/shift & Merge** (\$57.8 million capex, \$53.0 million opex)
- **Option 3 – Merge:** (\$75.3 million capex, \$41.9 million opex)

These options are discussed in the following sections. All options assume the AGN Transition commences 1 July 2027.

The APA contract is ending and operations are shifting to AGIG. This business case only contemplates methods for shifting critical IT systems from APA's IT environment to AGIG's IT environment. The option to not transition APA systems to AGIG (i.e. maintain status quo) was considered and discounted on the basis that:

- A similar suite of systems are already utilised within AGIG for our Multinet Gas Networks (MGN) and Dampier to Bunbury Pipeline (DBP) businesses
- An optimised operations and management approach for AGIG going forward will look quite different to the current arrangements in place
- Ownership of core operational technology systems is key to enabling AGN, as well as MGN and DBP, to seek the most efficient mix of delivery methods and external partners for the ongoing operations and management of pipelines and distribution networks post-June 2027
- We see benefits to our business and our customers in bringing these operational systems in-house, regardless of the future contracting model for operations

A summary of the options is provided in the following sections, and in Appendix A.1.

1.5.1 Option 1 – Lift / Shift

Under this option, we would replicate the current APA environment and run it in parallel as a separate standalone end-state environment within AGIG. The transition pattern for lifting and shifting IT systems from APA to AGIG is summarised in Appendix D.

1.5.1.1 Advantages and disadvantages

The advantage of a lift and shift (with no subsequent merge) is that it provides the fastest and lowest risk method for transitioning IT applications and infrastructure into the AGIG environment. Under the lift/shift approach, the APA applications, processes, data, and infrastructure are replicated in the AGIG environment with little or no change. This means workflows already exist and we can leverage existing processes and technical design for integrations and data transfer. As a result, the lift/shift has a minimal impact on business operations. Data does not have to be transferred to new applications, staff do not need to be trained to use different software, and network operations can migrate to AGIG in a seamless fashion.

The major disadvantage of Option 1 is that we would forego the opportunity to rationalise our application suite. If we simply lift and shift, we may be in a position where we have multiple instances of the same or similar applications.

For example, as part of a lift/shift we would bring across the Oracle CC&B application along with the associated market systems. However, AGIG already owns / runs billing and market systems (SAP ISU, etc.) that offer similar functionality for billing customers and interacting with AEMO and other market participants. Under a lift/shift and merge, we would bring CC&B across and then, once it is in our environment, seek to merge the data and functionality with SAP S4/HANA ISU, ultimately leading to a single system for customer billing and market interactions and therefore reducing a duplication of systems, processes and costs. Under a pure lift/shift (with no merge), we would have to retain both CC&B and SAP ISU, meaning we would own and operate two different applications that perform the same function.

Similarly, under a lift/shift we would bring across APA's enterprise asset management system Maximo and its associated data. AGIG currently uses Maximo in its DBP operations, therefore there may be an opportunity to merge the two instances of Maximo once the lift/shift has occurred. If we take the pure lift/shift option, AGIG would retain two instances of the same application.

The advantages and disadvantages of each option is presented further in Appendix A.

1.5.1.2 Cost assessment

The estimated capital and operating expenditure for Option 1 is \$93.9 million (see Table 0.4).

Table 0.4: APA IT transition 2026-31, AGN SA allocation, \$'000 January 2025 – Option 1

Option 1 – Lift / Shift SA allocation 35.24% of total AGN cost	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex						
Solution delivery	1,798	18,868	-	-	-	20,666
Integration management office	1,206	3,409	-	-	-	4,615
Infrastructure delivery	-	9,960	330	785	1,559	12,635
Total capex	3,004	32,237	330	785	1,559	37,916
Opex						
Transitional services agreement	-	8,528	4,757	-	-	13,285

Option 1 – Lift / Shift SA allocation 35.24% of total AGN cost	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Application licencing and production support	-	529	3,848	3,848	3,848	12,073
Infrastructure, security and connectivity	-	1,912	1,912	1,912	1,912	7,648
IT support	-	3,268	6,574	6,574	6,574	22,990
Total opex	-	14,237	17,092	12,334	12,334	55,997
Totex (capex + opex)	3,004	46,474	17,422	13,120	13,894	93,914

Cost estimates are based on current market rate testing, considering the requirements of our IT environment, using the best information available at the time of developing this business case. Refer to Appendix 0 for an overview of the costs estimation process.

1.5.1.3 Risk assessment

Option 1 reduces the risk to low. Migration of IT systems into AGIG's environment will reduce the likelihood of the primary risk event to remote (every 20 years). This risk outcome is consistent across both Option 1 and Option 2, as both propose a process whereby applications are lifted and shifted to the AGIG IT environment quickly and without immediate modification. This reduces the likelihood that applications will be unavailable from day one of the transition.

It could be argued that Option 1 is slightly lower risk than Option 2, as Option 1 does not feature any merging with existing AGIG systems and applications. Business continuity would not be an issue as existing APA applications are simply being replicated, meaning operations would continue as before. However, Option 1 forgoes the opportunity to merge applications, consolidate processes and eliminate duplication.

Table 0.5: Risk rating - Option 1

Option 1	Health & Safety	Environ-ment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Low
Consequence	Minimal	Minimal	Significant	Minor	Significant	Minor	Significant	
Risk level	Negligible	Negligible	Low	Negligible	Low	Negligible	Low	

A more granular risk assessment of each option is provided in Appendix 1.7.3A.4.

1.5.1.4 Achievement of objectives

Table 0.7 outlines how Option 1 will support achievement of our vision objectives.

Table 0.6: Achieving objectives – Option 1

Vision objective	Alignment
Customer Focussed - Public Safety	-
Customer Focussed – Customer Experience	-
Customer Focussed – Cost Efficient	N
A Leading Employer – Health and Safety	-

A Leading Employer – Employee Experience	-
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	-
Operational Excellence – Benchmark Performance	Y
Operational Excellence – Reliability	Y
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

Option 1 aligns with our *Operational Excellence* objectives, in that bringing the suite of operational technology systems within AGIG’s IT environment will ensure business continuity and reliability of service. End-to-end control and visibility of operational applications, data, and IT support will allow us to seek the most efficient mix of delivery methods and external partners for the ongoing operation of our networks post-June 2027. The network owner also having ownership of critical operational IT systems is also consistent with the practices of other network businesses.

However, Option 1 is not cost efficient. Although the lift/shift approach allows us to transfer applications to the AGIG IT environment at the lowest short term cost, it will lead to higher business as usual (BAU) costs due to extended parallel running of applications. Under Option 1 we are forgoing the opportunity to consolidate and merge systems in order to reduce costs. It can therefore be argued that Option 1 is not *Customer Focussed*.

1.5.2 Option 2 – Lift / Shift & Merge

Under this option we would transition to an interim replica of APA’s current environment for AGN within AGIG, before merging and transforming the two environments into one consolidated and optimised end-state environment. The transition pattern for lifting and shifting IT systems from APA to AGIG is summarised in Appendix D.

1.5.2.1 Advantages and disadvantages

Option 2 has many of the advantages of Option 1 (pure lift/shift), in that it is a relatively fast and low risk method of transitioning the IT systems. However, the primary advantage of Option 2’s lift/shift & merge approach is that it provides the opportunity to combine and rationalise applications and IT systems, improving efficiency and keeping costs lower than they would otherwise be over the long term. Once the lift and shift has occurred and the APA systems are replicated in AGIG’s IT environment, we can commence eliminating duplication and seek to leverage the broader applications suite within AGIG’s portfolio. This gives us greater control over ongoing transformational activities and the standard of our customer service.

The disadvantage of Option 2 is that until the ‘merge’ phase of the transition is complete, we will be running two IT environments for an interim period.

The advantages and disadvantages of each option is presented further in Appendix A.

1.5.2.2 Cost assessment

The estimated capital and operating expenditure for Option 2 is \$110.8 million (see Table 0.9).

Table 0.7: APA IT transition 2026-31, AGN SA allocation, \$'000 January 2025 – Option 2

Option 2 – Lift / Shift & Merge SA allocation 35.24% of total AGN cost	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex						
Solution delivery	1,798	18,868	5,000	9,999	0	35,665
Integration management office	1,173	3,409	1,624	3,248	0	9,454
Infrastructure delivery	0	9,960	330	785	1,559	12,635
Total capex	2,971	32,237	6,954	14,033	1,559	57,755
Opex						
Transitional services agreement	-	8,528	4,757	-	-	13,285
Application licencing and production support	-	529	3,848	3,848	2,309	10,534
Infrastructure, security and connectivity	-	1,912	1,912	1,912	1,147	6,883
IT support	0	3,268	6,618	6,618	5,829	22,334
Total opex	0	14,237	17,136	12,379	9,285	53,036
Totex (capex + opex)	2,971	46,474	24,090	26,411	10,844	110,791

Cost estimates are based on current market rate testing, considering the requirements of our IT environment, using the best information available at the time of developing this business case. Refer to Appendix 0 for an overview of the costs estimation process.

1.5.2.3 Risk assessment

Option 2 reduces the risk to low. Migration of IT systems into AGIG's environment will reduce the likelihood of the primary risk event to remote (every 20 years). This risk outcome is consistent across both Option 1 and Option 2, as both propose a process whereby applications are lifted and shifted to the AGIG IT environment quickly and without immediate modification. This reduces the likelihood that applications will be unavailable from day one of the transition.

Table 0.8: Risk rating - Option 2

Option 2	Health & Safety	Environ-ment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Low
Consequence	Minimal	Minimal	Significant	Minor	Significant	Minor	Significant	
Risk level	Negligible	Negligible	Low	Negligible	Low	Negligible	Low	

1.5.2.4 Achieving objectives

The following table outlines how Option 2 will support achievement of our vision objectives.

Table 0.9: Achieving objectives – Option 2

Vision objective	Alignment
Customer Focussed - Public Safety	-

Vision objective	Alignment
Customer Focussed – Customer Experience	-
Customer Focussed – Cost Efficient	Y
A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	-
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	-
Operational Excellence – Benchmark Performance	Y
Operational Excellence – Reliability	Y
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

Option 2 aligns with our *Operational Excellence and Customer Focussed* objectives. Bringing the suite of operational technology systems within AGIG's IT environment will ensure business continuity and reliability of service. End-to-end control and visibility of operational applications, data, and IT support will allow us to seek the most efficient mix of delivery methods and external partners for the ongoing operation of our networks post-June 2027. The network owner having ownership of critical operational IT systems is also consistent with the practices of other network businesses.

Option 2 is also the most cost efficient. While a higher short term cost than Option 1, the total cost over 10 years is lower (see Appendix 1.7.3B.3). This is because after the lift/shift we will merge systems where practicable, rationalising our BAU operating costs.

1.5.3 Option 3 – Merge

Under this option we would merge and transform the existing APA environment into a consolidated and optimised end-state environment within AGIG.

1.5.3.1 Advantages and disadvantages

The advantage of Option 3 compared with Option 2 is that it eliminates the interim state of having two IT environments running in parallel. The merge approach provides the ability to consolidate applications and IT systems as per Option 2. However, unlike Option 2, the merge phase runs in parallel with the transition, with applications migrating directly from APA into their AGIG end state. Option 3 eliminates duplication, but it also requires greater time and discretion for moving systems from APA to AGIG.

The major disadvantage of the merge approach is the complexity. The quantity of systems and data being transitioned from APA is substantial, requiring careful planning and coordination. With this complexity comes risk, both in terms of delivery and the potential for critical applications to be unavailable.

A merge approach takes longer than a lift and shift. Option 3 could potentially be the most efficient form of transition, however, it requires all of the components of the merge to run

perfectly, with limited room for error or delay. The interdependency of IT systems means that if one aspect of the transition stalls, it can have significant flow-on effects on other parts of the merge, which leads to higher costs and potential for system unavailability.

As a result, Option 3 comes at a significantly higher estimated cost than Option 1 or 2 both over the short term (5 years) and long term (10 years) (see Appendix B.3).

The advantages and disadvantages of each option is presented further in Appendix A

1.5.3.2 Cost assessment

The estimated capital and operating expenditure for Option 3 is \$114.4 million (see Table 0.13).

Table 0.10: APA IT transition 2026-31, AGN SA allocation, \$'000 January 2025 – Option 3

Option 3 – Lift & Merge SA allocation 35.24% of total AGN cost	2026/27	2027/28	2028/29	2029/30	2030/31	Total
Capex						
Solution delivery	2,631	23,947	23,947	-	-	50,525
Integration management office	1,408	4,091	4,091	-	-	9,590
Infrastructure delivery	-	11,95	396	942	1,871	15,162
Total capex	4,039	39,990	28,434	942	1,87	75,276
Opex						
Transitional services agreement	-	8,528	4,757	0	0	13,285
Application licencing and production support	-	529	846	2,309	2,309	5,992
Infrastructure, security and connectivity	-	1,912	1,912	1,147	1,147	6,119
IT support	-	3,268	3,268	4,977	4,977	16,489
Total opex	-	14,237	10,783	8,433	8,433	41,886
Totex (capex + opex)	4,039	54,227	39,217	9,375	10,304	117,162

Cost estimates are based on current market rate testing, considering the requirements of our IT environment, using the best information available at the time of developing this business case. Refer to Appendix 0 for an overview of the cost estimation process.

1.5.3.3 Risk assessment

Option 3 reduces the operational and compliance risk to low, as ultimately it will result core operational software and systems being migrated to the AGIG IT environment. However, the complexity of the merge approach means the potential for delay and increasing costs is high. This gives rise to a moderate financial risk.

We therefore do not consider Option 3 would reduce the overall risk any lower than moderate.

Table 0.11: Risk rating - Option 3

Option 3	Health & Safety	Environ-ment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Unlikely	Unlikely	Moderate
Consequence	Minimal	Minimal	Significant	Minor	Significant	Minor	Moderate	

Risk level	Negligible	Negligible	Low	Negligible	Low	Low	Moderate	
------------	------------	------------	-----	------------	-----	-----	----------	--

1.5.3.4 Achieving objectives

The following table outlines how Option 3 will support achievement of our vision objectives.

Table 0.12: Achieving objectives – Option 3

Vision objective	Alignment
Customer Focussed - Public Safety	-
Customer Focussed – Customer Experience	-
Customer Focussed – Cost Efficient	N
A Leading Employer – Health and Safety	-
A Leading Employer – Employee Experience	-
A Leading Employer – Skills Development	-
Operational Excellence – Profitable Growth	-
Operational Excellence – Benchmark Performance	Y
Operational Excellence – Reliability	Y
Sustainable Communities – Enabling Net Zero	-
Sustainable Communities – Environmentally Focussed	-
Sustainable Communities – Socially Responsible	-

Option 3 aligns with our *Operational Excellence* objective. Bringing the suite of operational technology systems within AGIG's IT environment will ensure business continuity and reliability of service. End-to-end control and visibility of operational applications, data, and IT support will allow us to seek the most efficient mix of delivery methods and external partners for the ongoing operations and management of our pipelines and distribution networks post-June 2027. The network owner also having ownership of critical operational IT systems is also consistent with the practices of other network businesses.

However, Option 3 is not cost efficient as it presents the highest overall cost over ten years (see Appendix 1.7.3B.3). This is because the lift and merge approach is a more complex and resource intensive solution.

1.6 Summary of options assessment

Table 0.17 presents a summary of how each option compares in terms of the estimated cost, the residual risk rating, and alignment with our vision objectives. A more detailed options assessment is provided in Appendix A.

Table 0.13: Summary of options assessment

Option	Capex	Opex	Totex	Risk outcome	Alignment with objectives
1. Lift / Shift	\$37.9 million	\$56.0 million	\$93.9 million	Reduces risk to Low	Aligns with Operational Excellence but not Customer Focussed
2. Lift / Shift & Merge	\$57.8 million	\$53.0 million	\$110.8 million	Reduces risk to Low	Aligns with Operational Excellence and Customer Focused
3. Merge	\$75.3 million	\$41.9 million	\$117.1 million	Reduces risk to Moderate	Aligns with Operational Excellence but not Customer Focussed

1.7 Proposed solution

Our proposed solution is Option 2, Lift/Shift & Merge.

1.7.1 Why is the recommended option prudent?

Option 2 is recommended because it is low risk and is the lowest overall cost option over the longer term (10 years). A lift, shift and merge approach gets critical IT systems into our environment in a short timeframe and provides opportunity for rationalising process/systems and leveraging the broader AGIG IT environment.

Option 1 is the lowest risk option in terms of business continuity, but forgoes the opportunity to merge systems and achieve synergies, and is therefore a higher cost over the longer term.

Option 3, while attractive in terms of eliminating duplication and allowing for a more strategic approach to the IT transition, carries the greatest risk and complexity and therefore the greatest cost.

1.7.2 Estimating the efficient costs

The cost estimates for the AGN transition have been developed by a third part expert consultancy, working in partnership with AGIG's subject matter experts.

Unit rates for internal IT and business resources are based on an established internal rate card. Specialist skills and additional capacity is required for the APA IT transition. Internal teams will be supplemented by outsourced IT support resources. The rates for outsourced IT support have been informed by the latest market analysis and quotes from vendors.

The cost estimation framework and approach to the IT cost model is summarised in Appendix 0 and B.5. Key assumptions applied in this business case are:

- Options analysis and estimations are based on the information provided by AGIG and interactions with APA IT architects. It is assumed further detailed planning and design will take place ahead of any transition activity, which is likely to further refine the cost estimates

- For the purposes of analysis and planning, it assumed that Day 1 of the separation will coincide with the expiration of the current Operations and Maintenance contract between APA and AGIG on the 1 July 2027
- The shared service recharge growth rate is based on inflation-adjusted SSRs from FY19 to FY25. The business case does not consider broader economic factors that may occur in the future
- It is assumed APA and AGIG, for the duration of the AGN transition program, will act collaboratively and in good faith to deliver timely and effective cutovers per the current roadmap and plan
- All licencing costs (opex) within this business case are assumed to be incurred at go-live not during the solution delivery and migration period prior to this
- Certain infrastructure and security licences are assumed to be on an initial 5-year subscription, which is incurred during acquisition of the hardware (capex)
- The current source systems and integrations in APA's environment are appropriate, operational and functional prior to commencement of migrations

All procurement processes for IT applications will comply with our Procurement Policy and Purchasing Procedure and will follow transparent, competitive tendering processes to select the best value for money solution.

1.7.3 Consistency with the National Gas Rules

NGR 79(1) and NGR 91

The proposed expenditure on our IT operational applications is consistent with Rule 79(1)(a), specifically we consider the capital expenditure is:

- **Prudent** – Transitioning IT data, applications and processes from APA to AGIG is fundamental to the ongoing operation of the network. It is essential IT systems such as Maximo and the metering & billing system are available to AGIG staff, therefore it is prudent to lift and shift them to the AGIG operating environment as quickly as practicable, and then merge them into AGIG's broader IT framework.
- **Efficient** – The forecast expenditure is based on historical costs for similar transition programs as well as estimates from vendors and APA. Actual costs will be reassessed during the APA transition and we will seek identify efficiencies through the merge processes, eliminating duplication as soon as practicable and identifying synergies with the broader AGIG application suite.
- **Consistent with accepted and good industry practice** – The network owner having control and ownership over critical operational IT applications is consistent with accepted industry practice.

- **Achieves the lowest sustainable cost of delivering pipeline services** – The merge process will identify opportunities for rationalisation and efficiency improvements. This lift, shift and merge approach is the lowest risk and most expedient method of getting these IT systems within AGIG's control. Though the initial IT transition cost is substantial, bringing operational IT systems into the AGIG environment offers longer term opportunities for efficiencies and productivity improvements. This is because AGIG (as the network owner) will have full autonomy and operational control over IT upgrades, strategies and investments. The transition is therefore consistent with the actions of a prudent network operator and will ultimately achieve the lowest sustainable cost of delivering pipeline services.

NGR 79(2)(c)

The proposed expenditure is required to maintain integrity of services by ensuring operational IT systems are available to AGIG staff. This expenditure is therefore consistent with NGR 79(2)(c)(ii).




NGR 74

The forecast costs are based on the latest market rate testing, and project options consider the requirements of our application environment. Extensive option assessments and project planning has been undertaken, underpinned by advice from a third-party expert consultancy. Cost assessments have been conducted for each option based on the best information available at the time of developing 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 Options analysis




A.1 Summary of options

Three different pathways have been explored for AGIG to transition current the APA IT services supporting AGN, with some notable opportunities and obstacles for AGIG to consider.

	Option 1 Lift/Shift	Option 2 Lift/Shift & Merge	Option 3 Merge
Approach	 <p>Lift/Shift from APA to AGIG where AGN systems and data are replicated into the AGIG IT environment with no subsequent migrations, once established.</p>	 <p>Lift/Shift to first migrate AGN applications to an 'interim' Day 2 state in AGIG. Once migrated, a subsequent migration, 'merge', is undertaken for select applications to export and migrate data from the 'interim' Day 2 application to the 'target' Day 3 application which is shared with DBP & MGN.</p>	 <p>Migration of data, 'merge', from AGN's systems directly to the existing applications identified in AGIG's environment without the migration to an 'interim' state.</p>
Pros	<ul style="list-style-type: none"> ✓ Faster timeline for AGIG to gain full control of AGN operations ✓ Existing processes and technical design for integrations, data transformations and workflows exist ✓ Reduced business transformation impact 	<ul style="list-style-type: none"> ✓ Faster timeline for AGIG to gain full control of AGN operations ✓ Greater control over transformation activities for AGIG ✓ Existing processes and technical design for integrations and data transformations exist for initial separation and interim period ✓ Results in consolidated end state for AGIG with associated operational cost synergies 	<ul style="list-style-type: none"> ✓ AGIG consolidated end state IT environment will be operational, presenting opportunities to migrate from APA solutions directly to AGIG end state (reducing 'double hop' activities) and realisation of synergies sooner ✓ Effective utilisation of longer lead-time to plan and transition to AGIG end state ✓ Opportunities may be present to stage migration of solutions over remaining life-time of O&M contract reducing the need for a 'big bang' migration of all capability within a comparatively shorter timeframe
Cons	<ul style="list-style-type: none"> ✗ AGIG IT environment remains in federated state with no realisation of operational synergies ✗ Greater long-term operating costs as a result of AGIG operating two environments in parallel 	<ul style="list-style-type: none"> ✗ Will result in 'double hop' of IT capability as AGIG consolidated IT environment will not yet be established. AGN IT assets will then need to be consolidated into AGIG end state post separation from APA ✗ Increased sunk cost in standing up interim environment ✗ Greater cost of running 'two environments' in parallel for an interim period ✗ Running consecutive projects will likely introduce change fatigue 	<ul style="list-style-type: none"> ✗ Longer timeline for AGIG to gain full control of AGN operations ✗ Increased delivery risk through additional complexity in moving to new solutions and systems ✗ Increased business risk as change to current processes and procedures required to leverage new systems ✗ Greater reliance on APA giving access to their environment and involvement throughout transformation

A.2 Alignment of options with IT integration principles

Option 2 is the most suitable when considering AGIG's IT integration principles. Whilst Option 1 achieves similar outcomes, there is expected to be a significant amount of stranded costs associated given the ongoing parallel run of the AGN IT environment within the AGIG landscape.

		Option 1 Lift/Shift	Option 2 Lift/Shift & Merge	Option 3 Merge
Alignment Summary		 <p>Option 1 largely aligns with AGIG's IT Integrations Principles. Migration complexity and risk are minimised as a Lift/Shift approach is adopted to efficiently reach Day 2. However, the ongoing parallel run of the AGN environment with AGIG's current IT landscape creates a higher degree of stranded costs than the other two options.</p>	 <p>Option 2 further builds on Option 1, with a subsequent migration to 'target' Day 3 state. This approach aligns with all IT Integration Principles.</p>	 <p>Option 3 deviates from AGIG's IT Integration principles as the integration approach will involve a direct transition to the 'target' Day 3 state. This presents higher complexity and risk and will require collaboration with APA to support extensive data migrations.</p>
Integration Principles	1	✓ Transfer before transform	✓ Transfer before transform	✗ Transfer before transform
	2	✓ Shortest path to Day 2	✓ Shortest path to Day 2	✗ Shortest path to Day 2
	3	✓ Minimise migration costs to target state	✓ Minimise migration costs to target state	✗ Minimise migration costs to target state
	4	✗ Minimise stranded costs	✓ Minimise stranded costs	✓ Minimise stranded costs
	5	✓ Minimise business impacts	✓ Minimise business impacts	✗ Minimise business impacts
	6	✓ Transition all necessary data	✓ Transition all necessary data	✓ Transition all necessary data
	7	✓ Staged go-lives	✓ Staged go-lives	✓ Staged go-lives
		KEY ✓ Aligned ✗ Not aligned		

A.3 Comparable delivery risk of each option

Options 1 and 2 are preferable for the AGN IT transition as they present lower risk to AGIG's business continuity and realisation of strategic goals.

	Preferred Options		Key: ■ No risk ■ Low risk ■ High risk ■ Neutral
	Option #1: Lift/Shift	Option #2: Lift/Shift & Merge	Option #3: Merge
Description (Solution Overview)	Lift/Shift from APA to AGIG where APA systems and data are replicated into the AGIG IT environment with no subsequent migrations, once established.	Lift/Shift to first migrate APA applications to an 'interim' Day 2 state in AGIG. Once migrated, a subsequent migration, 'merge', is undertaken for select applications to export and migrate data from the 'interim' Day 2 application to the 'target' Day 3 application which is shared with DBP & MGN.	Migration of data, 'merge', from APA's systems directly to the existing applications identified in AGIG's environment without the migration to an 'interim' state.
Strategic Alignment (AGIG's long term vision and goals)	<ul style="list-style-type: none"> ■ The IT transition of ~50 applications will not achieve target state at AGIG and will lead to duplicate applications for similar capabilities. ■ AGIG will incur higher BAU operating costs due to parallel run of applications. 	<ul style="list-style-type: none"> ■ Target state will be achieved after Lift/Shift of ~50 application at Day 2 and merge of 25 applications at Day 3. AGIG will have control of the applications to manage the merge, once Lift/Shift is complete. ■ After merge, the BAU operating costs will be rationalised. 	<ul style="list-style-type: none"> ■ Target state will be achieved after direct lift and merge of ~50 applications at Day 3, although AGIG will have no control of the applications, as only data files will transition over from APA. ■ After merge, the BAU operating costs will be rationalised.
Ability to Execute (Execution of IT transition, resourcing, skills and capability)	<ul style="list-style-type: none"> ■ 1 year timeline for Lift/Shift of the applications transitioning from APA to AGIG. ■ Compared to other options, the execution complexity is the lowest. ■ Resource intensive requirements in a time constraint environment (1 year period) to be managed by delivery partner. ■ Delivery partner to support the skills and capability required for the transition. 	<ul style="list-style-type: none"> ■ 1 year timeline for Lift/Shift and 2-year timeline for the merge of the applications to reach the target state. ■ Low to medium execution complexity of the IT transition to the target state. ■ Resource intensive requirements for Lift/Shift & Merge spread over 5 years, to be managed by delivery partner. ■ Delivery partner to support the skills and capability required for the transition. 	<ul style="list-style-type: none"> ■ 2-year timeline for lift and merge, that is beyond the TSA period and may not be adequate to get control of the application data and merge into target systems. ■ High complexity with data migration for all applications in a time constraint environment. ■ Resource intensive requirements in a time constraint; to be managed by the delivery partner. ■ Delivery partner to support the skills and capability required for the transition.
Impact to business operations (Business change)	<ul style="list-style-type: none"> ■ Least impact to business operations as AGN operations are expected to run as same with no merge into existing MGN applications. ■ Least effort on change management as compared to other options 	<ul style="list-style-type: none"> ■ Medium impact to AGN business operations due to merge into MGN applications however with more time and better control as an interim lift/shift state exists ■ Medium to high change management due to multiple systems in use. 	<ul style="list-style-type: none"> ■ The impact to business operations is expected to be highest as there is no interim state of AGN applications to absorb and understand their current operations ■ High change management due to multiple systems in use.

A.4 Recommendation based on cost and risk assessment




We recommend Option 2 'Lift/shift & Merge' is the approach taken for the AGN IT transition. This has been concluded following assessment against the integration principles, risks and costs.

Option 1: Lift/Shift	Recommended option	Option 3: Merge
<ul style="list-style-type: none"> ✗ Strategic Alignment - Does not meet AGIG's strategic and long-term objectives due to parallel run of AGN and MGN operations + Alignment to IT Integration Principles - Has the most alignment to IT integration principles. + Ability to execute - The execution complexity is the lowest and ability to execute is the highest due to Lift/Shift of existing AGN applications + Impact to the business operations - Least impact to business operations as AGN operations are expected to run as same with no merge into existing MGN applications + Cost of total operation - Total cost of Option 1 is the lowest over the 5-year regulatory period (\$258.8 M). 	<ul style="list-style-type: none"> + Strategic Alignment - Does meet AGIG's strategic and long-terms objectives of running a single set of systems for both AGN and MGN. However, there is an interim parallel run due to lift/shift + Alignment to IT Integration Principles - Has the moderate alignment to IT separation principles between Option 1 and Option 3 due to high separation and stranded cost. + Ability to execute - The execution complexity is low to medium given systems are first lifted and shifted and absorbed into the AGIG's environment before the merge + Impact to the business operations - Impact to AGN business operations due to Merge into MGN applications however with more time and better control as an interim lift/shift state exists ✗ Cost of total operation - Total cost of Option 2 is the second highest over the 5-year regulatory period (\$306.7 M), however is c.\$20 M less expensive than Option 3. 	<ul style="list-style-type: none"> + Strategic Alignment - Does meet AGIG's strategic and long-terms objectives of running a single set of systems for both AGN and MGN ✗ Alignment to IT Integration Principles - Has the least alignment to IT integration principles due to longest pathway to separation and biggest impact to business operations ✗ Ability to execute - The execution complexity is the highest and ability to execute is the lowest within the required timelines due to no control on AGN applications as they are directly lifted and merged from APA ✗ Impact to the business operations - The impact to business operations is expected to be highest as there is no interim state of AGN applications to absorb and understand their current operations. ✗ Cost of total operation - Total cost of Option 3 is the highest over the 5-year regulatory period (\$324.8 M).

Appendix B Cost estimates (Total AGN)

B.1 Incremental cost estimates for AGN IT integration options (FY27 – FY31)

Cost estimates have been developed for three IT transition options. Note these are whole of AGN costs (not just the AGN SA allocation). These estimates are based on application transition patterns and the IT components and resourcing profiles required to support them. Ongoing operating expenses have also been included over the period.

Option 1 Lift/Shift 18 Months		Option 2 Lift/Shift & Merge 42 Months		Option 3 Merge 30 Months	
					
<p>The costs for Option 1 have been calculated based on inputs from AGIG workshops. This includes the cost of 'Lift/Shift' of c.50 applications from the APA to AGIG environment.</p> <p>The operational costs include the licensing and IT support resources required for ongoing BAU support over a 5-year period.</p>		<p>The costs for Option 2 have been calculated by considering a 'Lift/Shift' approach for c.50 applications from Day 1 to Day 2 from APA's environment to AGIG's environment. This is followed by a subsequent 'merge' event for c.25 applications to achieve their target state in AGIG environment.</p> <p>The operational costs include the licensing and IT support resources required for ongoing BAU support over a 5-year period.</p>		<p>The costs for Option 3 have been calculated by considering a direct 'lift and merge' approach for c.50 applications to achieve the target state within the AGIG environment (as opposed to the 'lift/shift' approach in Option 1 and 2).</p> <p>The operational costs include the licensing and IT support resources required for ongoing BAU support over a 5-year period.</p>	
1 July 2026 – 30 June 2031	Total (\$AUD)*	1 July 2026 – 30 June 2031	Total (\$AUD)*	1 July 2026 – 30 June 2031	Total (\$AUD)*
Solution Delivery (Finance, Customer, Regulatory, People, Network, Technology)	\$58.6 M	Solution Delivery (Finance, Customer, Regulatory, People, Network, Technology)	\$101.2 M	Solution Delivery (Finance, Customer, Regulatory, People, Network, Technology)	\$143.4 M
Integration Management Office (IMO, Program Arch, Prog & Tech Assurance, GRC, CMO)	\$13.1 M	Integration Management Office (IMO, Program Arch, Prog & Tech Assurance, GRC, CMO)	\$26.8 M	Integration Management Office (IMO, Program Arch, Prog & Tech Assurance, GRC, CMO)	\$27.2 M
Infrastructure Delivery (incl. Security, EUC)	\$35.9 M	Infrastructure Delivery (incl. Security, EUC)	\$35.9 M	Infrastructure Delivery (incl. Security, EUC)	\$43.0 M
Total CAPEX	\$107.6 M	Total CAPEX	\$163.9 M	Total CAPEX	\$213.6 M
Transitional Services Agreement	\$37.7 M	Transitional Services Agreement	\$37.7 M	Transitional Services Agreement	\$37.7 M
Application Licencing & Product Support	\$34.3 M	Application Licencing & Product Support	\$29.9 M	Application Licencing & Product Support	\$17.0 M
Infrastructure, Security & Connectivity	\$21.7 M	Infrastructure, Security & Connectivity	\$19.5 M	Infrastructure, Security & Connectivity	\$17.4 M
IT Support (Labour)	\$65.2 M	IT Support (Labour)	\$63.4 M	IT Support (Labour)	\$46.8 M
Total OPEX	\$158.9 M	Total OPEX	\$150.5 M	Total OPEX	\$118.9 M
TOTEX (Option 1)	\$266.5 M	TOTEX (Option 2)	\$314.4 M	TOTEX (Option 3)	\$332.5 M

B.2 Breakdown of 5-year capex and opex by option (FY27 – FY31)

OPTION	CATEGORY	FISCAL YEAR	FY 2027	FY 2028	FY 2029	FY 2030	FY 2031	5-Year Total
		1-Jul-26	1-Jul-27	1-Jul-28	1-Jul-29	1-Jul-30	1-Jul-31	Total
Baseline	OPEX (Total)		\$22.0 M	\$23.1 M	\$24.2 M	\$25.4 M	\$26.7 M	\$121.5 M
	Shared Service Recharge (SSR)*		\$22.0 M	\$23.1 M	\$24.2 M	\$25.4 M	\$26.7 M	\$121.5 M
	TOTEX (Baseline)		\$22.0 M	\$23.1 M	\$24.2 M	\$25.4 M	\$26.7 M	\$121.5 M
Option 1	Solution Delivery		\$5.1 M	\$53.5 M	-	-	-	\$58.6 M
	Integration Management Office		\$3.4 M	\$9.7 M	-	-	-	\$13.1 M
	Infrastructure Delivery		-	\$28.3 M	\$0.9 M	\$2.2 M	\$4.4 M	\$35.9 M
	Total CAPEX		\$8.5 M	\$91.5 M	\$0.9 M	\$2.2 M	\$4.4 M	\$107.6 M
	TSA (excl. IT support)**		-	\$24.2 M	\$13.5 M	-	-	\$37.7 M
	Application Licensing & Product Support		-	\$1.5 M	\$10.9 M	\$10.9 M	\$10.9 M	\$34.3 M
	Infrastructure, Security & Connectivity		-	\$5.4 M	\$5.4 M	\$5.4 M	\$5.4 M	\$21.7 M
	IT support		-	\$9.3 M	\$18.7 M	\$18.7 M	\$18.7 M	\$65.2 M
	Total OPEX		-	\$40.4 M	\$48.5 M	\$35.0 M	\$35.0 M	\$158.9 M
	TOTEX (Option 1)		\$8.5 M	\$131.9 M	\$49.4 M	\$37.2 M	\$39.4 M	\$266.5 M
Option 2	Solution Delivery		\$5.1 M	\$53.5 M	\$14.2 M	\$28.4 M	-	\$101.2 M
	Integration Management Office		\$3.3 M	\$9.7 M	\$4.6 M	\$9.2 M	-	\$26.8 M
	Infrastructure Delivery		-	\$28.3 M	\$0.9 M	\$2.2 M	\$4.4 M	\$35.9 M
	Total CAPEX		\$8.4 M	\$91.5 M	\$19.7 M	\$39.8 M	\$4.4 M	\$163.9 M
	TSA (excl. IT support)**		-	\$24.2 M	\$13.5 M	-	-	\$37.7 M
	Application Licensing & Product Support		-	\$1.5 M	\$10.9 M	\$10.9 M	\$6.6 M	\$29.9 M
	Infrastructure, Security & Connectivity		-	\$5.4 M	\$5.4 M	\$5.4 M	\$3.3 M	\$19.5 M
	IT support		-	\$9.3 M	\$18.8 M	\$18.8 M	\$16.5 M	\$63.4 M
	Total OPEX		-	\$40.4 M	\$48.6 M	\$35.1 M	\$26.3 M	\$150.5 M
	TOTEX (Option 2)		\$8.4 M	\$131.9 M	\$68.4 M	\$74.9 M	\$30.8 M	\$314.4 M
Option 3	Solution Delivery		\$7.5 M	\$68.0 M	\$68.0 M	-	-	\$143.4 M
	Integration Management Office		\$4.0 M	\$11.6 M	\$11.6 M	-	-	\$27.2 M
	Infrastructure Delivery		-	\$33.9 M	\$1.1 M	\$2.7 M	\$5.3 M	\$43.0 M
	Total CAPEX		\$11.5 M	\$113.5 M	\$80.7 M	\$2.7 M	\$5.3 M	\$213.6 M
	TSA (excl. IT support)**		-	\$24.2 M	\$13.5 M	-	-	\$37.7 M
	Application Licensing & Product Support		-	\$1.5 M	\$2.4 M	\$6.6 M	\$6.6 M	\$17.0 M
	Infrastructure, Security & Connectivity		-	\$5.4 M	\$5.4 M	\$3.3 M	\$3.3 M	\$17.4 M
	IT support		-	\$9.3 M	\$9.3 M	\$14.1 M	\$14.1 M	\$46.8 M
	Total OPEX		-	\$40.4 M	\$30.6 M	\$23.9 M	\$23.9 M	\$118.9 M
	TOTEX (Option 3)		\$11.5 M	\$153.9 M	\$111.3 M	\$26.6 M	\$29.2 M	\$332.5 M

1 Option 1 has the highest Opex impact compared to other options

- Negligible difference in Opex compared to baseline 'do nothing' approach
- c.\$10 M higher than the Option 2 'Lift/shift & Merge' approach
- c.\$40 M higher than the Option 3 'Lift & Merge' approach

2 Option 2 has comparable Capex to Option 3, whilst presenting lower risk to AGIG

- \$163.9 M Capex to execute the Option 2 'Lift/shift & Merge' approach
- \$213.6 M Capex to execute the Option 3 'Lift & Merge' approach

3 Opex synergies from the merge are realised in both Options 2 & 3

- Option 3 realises synergies sooner (in FY30) due to faster completion of the merge event.
- Option 2 realises synergies in FY31/32. When viewed over a 10-year period, the total Opex for Option 2 is c.\$30 M higher than Option 3 (see next slide)

*Shared Services Recharge (SSR) reflects the estimated costs paid by AGIG to APA for the provision of IT services to support the AGN business under the current Operations & Maintenance agreement between the two parties. An annual growth rate of 4.9% p.a. has been applied to the SSR from FY26, which is the 7-year CAGR incurred by AGIG prior to FY25 (real values, excluding inflation).

**TSA is the total TSA charge for AGN services supplied by APA (IT and non-IT), exclusive of IT support (labour).

B.3 Breakdown of 10-year capex and opex by option (FY27 – FY31)

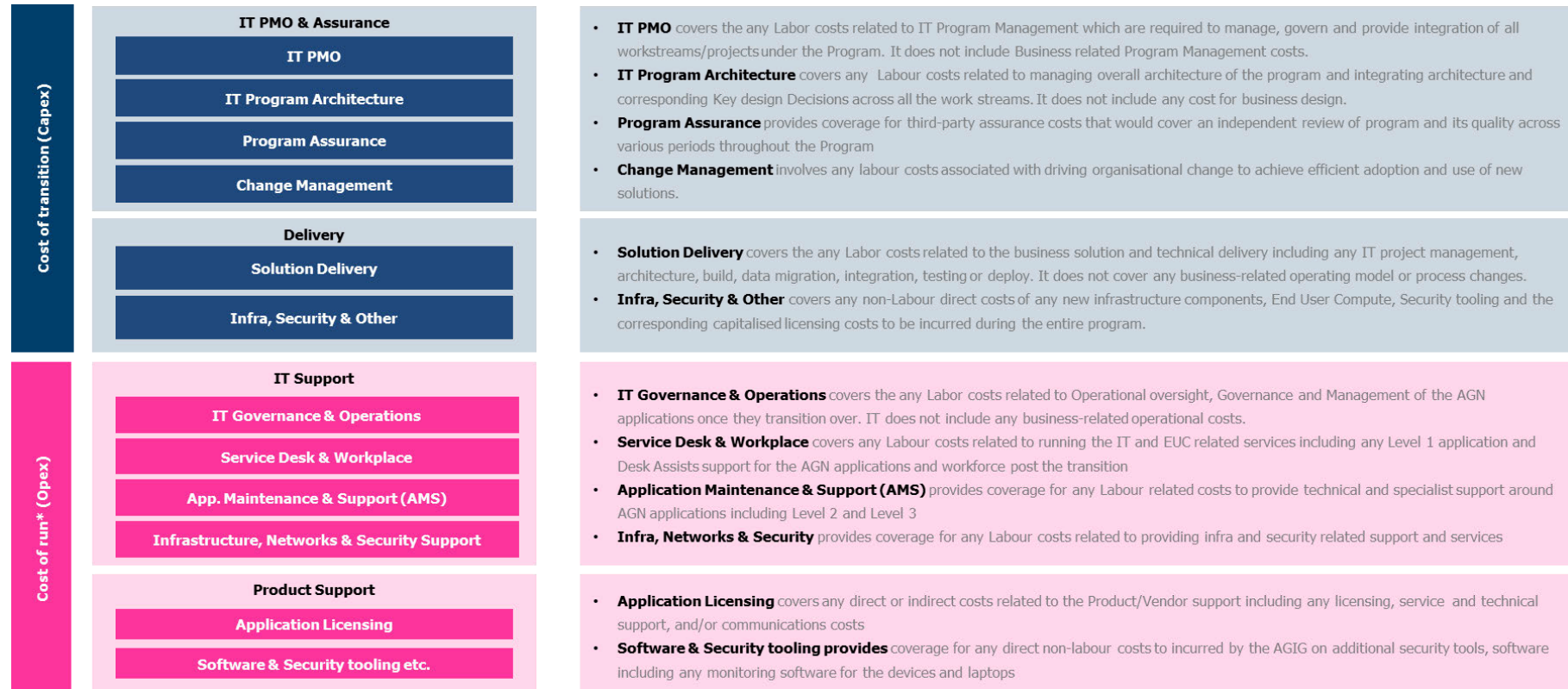
Regulatory Period													
FISCAL YEAR		FY 2027	FY 2028	FY 2029	FY 2030	FY 2031	FY 2032	FY 2033	FY 2034	FY 2035	FY 2036	10-Year Total	
OPTION	CATEGORY	1-Jul-26	1-Jul-27	1-Jul-28	1-Jul-29	1-Jul-30	2-Jul-30	3-Jul-30	4-Jul-30	5-Jul-30	6-Jul-30	Total	
Baseline	OPEX (Total)	\$22.0 M	\$23.1 M	\$24.2 M	\$25.4 M	\$26.7 M	\$28.0 M	\$29.4 M	\$30.8 M	\$32.3 M	\$33.9 M	\$275.9 M	
	Shared Service Recharge (SSR)*	\$22.0 M	\$23.1 M	\$24.2 M	\$25.4 M	\$26.7 M	\$28.0 M	\$29.4 M	\$30.8 M	\$32.3 M	\$33.9 M	\$275.9 M	
	TOTEX (Baseline)	\$22.0 M	\$23.1 M	\$24.2 M	\$25.4 M	\$26.7 M	\$28.0 M	\$29.4 M	\$30.8 M	\$32.3 M	\$33.9 M	\$275.9 M	
Option 1	Solution Delivery	\$5.1 M	\$53.5 M	-	-	-	-	-	-	-	-	\$58.6 M	
	Integration Management Office	\$3.4 M	\$9.7 M	-	-	-	-	-	-	-	-	\$13.1 M	
	Infrastructure Delivery	-	\$28.3 M	\$0.9 M	\$2.2 M	\$4.4 M	-	-	-	-	-	\$35.9 M	
	Total CAPEX	\$8.5 M	\$91.5 M	\$0.9 M	\$2.2 M	\$4.4 M	-	-	-	-	-	\$107.6 M	
	TSA (excl. IT support)**	-	\$24.2 M	\$13.5 M	-	-	-	-	-	-	-	\$37.7 M	
	Application Licencing & Product Support	-	\$1.5 M	\$10.9 M	\$10.9 M	\$10.9 M	\$10.9 M	\$10.9 M	\$10.9 M	\$10.9 M	\$10.9 M	\$88.9 M	
	Infrastructure, Security & Connectivity	-	\$5.4 M	\$5.4 M	\$5.4 M	\$5.4 M	\$5.4 M	\$5.4 M	\$5.4 M	\$5.4 M	\$5.4 M	\$48.8 M	
	IT support	-	\$9.3 M	\$18.7 M	\$18.7 M	\$18.7 M	\$18.7 M	\$18.7 M	\$18.7 M	\$18.7 M	\$18.7 M	\$158.5 M	
	Total OPEX	-	\$40.4 M	\$48.5 M	\$35.0 M	\$35.0 M	\$35.0 M	\$35.0 M	\$35.0 M	\$35.0 M	\$35.0 M	\$333.9 M	
	TOTEX (Option 1)	\$8.5 M	\$131.9 M	\$49.4 M	\$37.2 M	\$39.4 M	\$35.0 M	\$35.0 M	\$35.0 M	\$35.0 M	\$35.0 M	\$441.5 M	
Option 2	Solution Delivery	\$5.1 M	\$53.5 M	\$14.2 M	\$28.4 M	-	-	-	-	-	-	\$101.2 M	
	Integration Management Office	\$3.3 M	\$9.7 M	\$4.6 M	\$9.2 M	-	-	-	-	-	-	\$26.8 M	
	Infrastructure Delivery	-	\$28.3 M	\$0.9 M	\$2.2 M	\$4.4 M	-	-	-	-	-	\$35.9 M	
	Total CAPEX	\$8.4 M	\$91.5 M	\$19.7 M	\$39.8 M	\$4.4 M	-	-	-	-	-	\$163.9 M	
	TSA (excl. IT support)**	-	\$24.2 M	\$13.5 M	-	-	-	-	-	-	-	\$37.7 M	
	Application Licencing & Product Support	-	\$1.5 M	\$10.9 M	\$10.9 M	\$6.6 M	\$6.6 M	\$6.6 M	\$6.6 M	\$6.6 M	\$6.6 M	\$62.7 M	
	Infrastructure, Security & Connectivity	-	\$5.4 M	\$5.4 M	\$5.4 M	\$3.3 M	\$3.3 M	\$3.3 M	\$3.3 M	\$3.3 M	\$3.3 M	\$35.8 M	
	IT support	-	\$9.3 M	\$18.8 M	\$18.8 M	\$16.5 M	\$15.4 M	\$14.3 M	\$14.3 M	\$14.3 M	\$14.3 M	\$136.0 M	
	Total OPEX	-	\$40.4 M	\$48.6 M	\$35.1 M	\$26.3 M	\$25.2 M	\$24.1 M	\$24.1 M	\$24.1 M	\$24.1 M	\$272.2 M	
	TOTEX (Option 2)	\$8.4 M	\$131.9 M	\$68.4 M	\$74.9 M	\$30.8 M	\$25.2 M	\$24.1 M	\$24.1 M	\$24.1 M	\$24.1 M	\$436.0 M	
Option 3	Solution Delivery	\$7.5 M	\$68.0 M	\$68.0 M	-	-	-	-	-	-	-	\$143.4 M	
	Integration Management Office	\$4.0 M	\$11.6 M	\$11.6 M	-	-	-	-	-	-	-	\$27.2 M	
	Infrastructure Delivery	-	\$33.9 M	\$1.1 M	\$2.7 M	\$5.3 M	-	-	-	-	-	\$43.0 M	
	Total CAPEX	\$11.5 M	\$113.5 M	\$80.7 M	\$2.7 M	\$5.3 M	-	-	-	-	-	\$213.6 M	
	TSA (excl. IT support)**	-	\$24.2 M	\$13.5 M	-	-	-	-	-	-	-	\$37.7 M	
	Application Licencing & Product Support	-	\$1.5 M	\$2.4 M	\$6.6 M	\$6.6 M	\$6.6 M	\$6.6 M	\$6.6 M	\$6.6 M	\$6.6 M	\$49.8 M	
	Infrastructure, Security & Connectivity	-	\$5.4 M	\$5.4 M	\$3.3 M	\$3.3 M	\$3.3 M	\$3.3 M	\$3.3 M	\$3.3 M	\$3.3 M	\$33.6 M	
	IT support	-	\$9.3 M	\$9.3 M	\$14.1 M	\$14.1 M	\$14.1 M	\$14.1 M	\$14.1 M	\$14.1 M	\$14.1 M	\$117.4 M	
	Total OPEX	-	\$40.4 M	\$30.6 M	\$23.9 M	\$23.9 M	\$23.9 M	\$23.9 M	\$23.9 M	\$23.9 M	\$23.9 M	\$238.5 M	
	TOTEX (Option 3)	\$11.5 M	\$153.9 M	\$111.3 M	\$26.6 M	\$29.2 M	\$23.9 M	\$23.9 M	\$23.9 M	\$23.9 M	\$23.9 M	\$452.1 M	

*Shared Services Recharge (SSR) reflects the estimated costs paid by AGIG to APA for the provision of IT services to support the AGN business under the current Operations & Maintenance agreement between the two parties. An annual growth rate of 4.9% p.a. has been applied to the SSR from FY26, which is the 7-year CAGR incurred by AGIG prior to FY25 (real values, excluding inflation).

**TSA is the total TSA charge for AGN services supplied by APA (IT and non-IT), exclusive of IT support (labour).

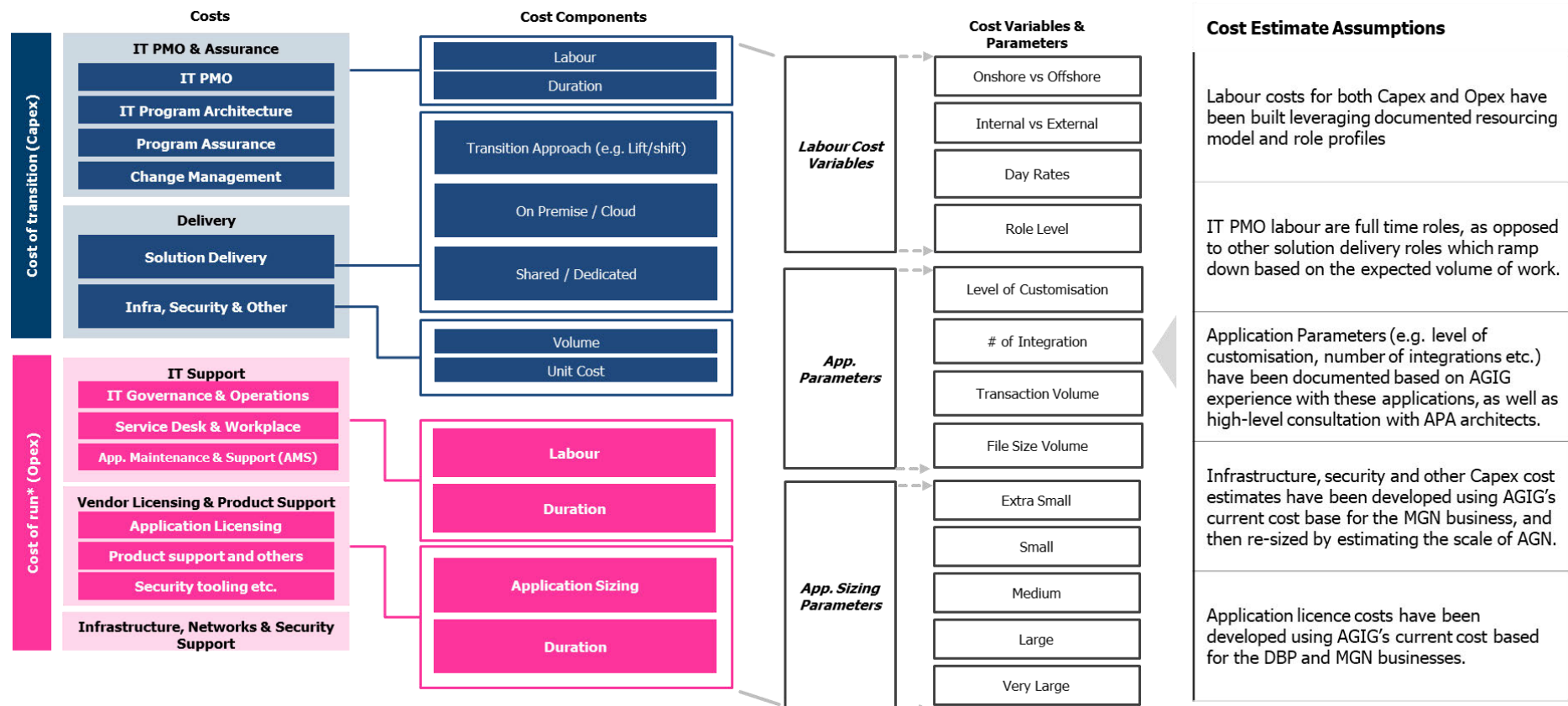
B.4 Overview of cost estimation framework

We have documented a cost estimation framework that holistically covers all aspects of IT Capex and Opex for the AGN transition



B.5 Approach to the IT Cost Model

The following diagram summarises the approach used in the IT cost model to estimate costs.



B.6 Estimated effort days and cost by system

Overview of Effort Days & Cost by System (Day 0 – Day 1) (1 Jan 2027 – 1 July 2027)						
			Effort Days	Estimated Cost (\$AUD)		
Function	Source System (Day 0)	Target System (Day 1)	Total	Separation	Integration	Total
People, Safety & Culture	Chris21	SuccessFactors- Payroll	434	\$0.3 M	\$0.4 M	\$0.8 M
People, Safety & Culture	Workday (People)	SAP SuccessFactors	168	\$0.1 M	\$0.2 M	\$0.3 M
People, Safety & Culture	Workday (LMS)	SAP SuccessFactors	168	\$0.1 M	\$0.2 M	\$0.3 M
People, Safety & Culture	Workday (Time & Attendance)	SAP SuccessFactors	289	\$0.2 M	\$0.3 M	\$0.5 M
People, Safety & Culture	Recruitment Extracts	SAP SuccessFactors	232	\$0.2 M	\$0.2 M	\$0.4 M
Technology	Email, SharePoint, MS Teams)	MS Office	2160	\$1.6 M	\$2.2 M	\$3.8 M
Technology	VPN (Internal); Citrix (External)	VPN (Internal); Citrix (External)	1167	\$0.9 M	\$1.2 M	\$2.0 M
Technology	ServiceNow	ServiceNow	897	\$0.7 M	\$0.9 M	\$1.6 M
Regulatory & Compliance	Vigilant	Protecht	623	\$0.5 M	\$0.6 M	\$1.1 M
Total			6,137	\$4.6 M	\$6.2 M	\$10.8 M

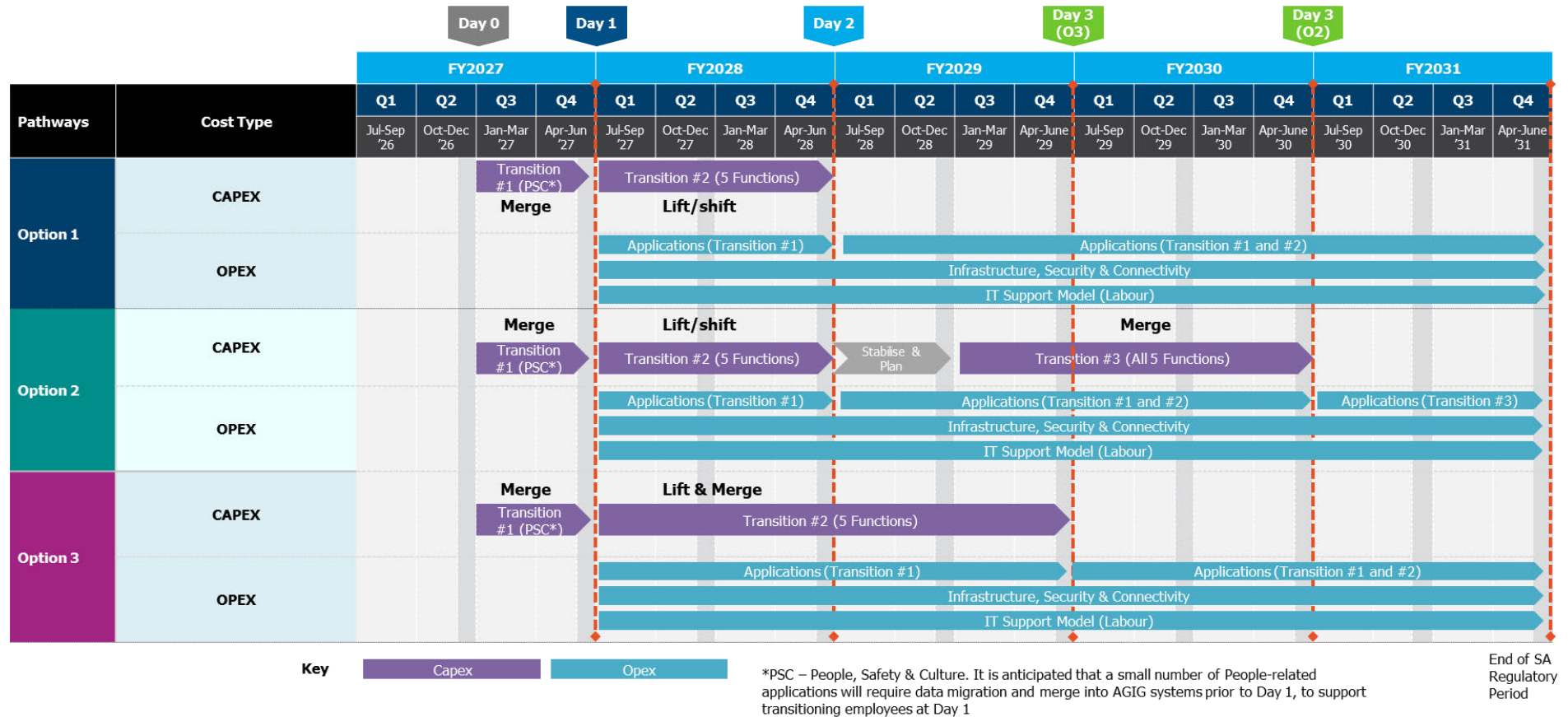
Overview of effort days & cost by system (Day 1 – Day 2) (1 July 2007 to 1 July 2008)						
			Effort Days	Estimated Cost (\$AUD)		
Function	Source System (Day 1)	Target System (Day 2)	Total	Separation	Integration	Total
Customer & Market Services	Oracle CC&B	Oracle CC&B	1113	\$1.1 M	\$0.8 M	\$1.9 M
Customer & Market Services	Control M	Control M	603	\$0.6 M	\$0.4 M	\$1.0 M
Customer & Market Services	CCB Batch	CCB Batch	603	\$0.6 M	\$0.4 M	\$1.0 M
Customer & Market Services	TOHT	TOHT	1503	\$1.5 M	\$1.1 M	\$2.6 M

Customer & Market Services	Heating Value Zone	Heating Value Zone	412	\$0.4 M	\$0.3 M	\$0.7 M
Finance & Procurement	Workday	Workday	1168	\$1.2 M	\$0.8 M	\$2.0 M
Finance & Procurement	Blackline/ Workday Adaptive	Blackline/ Workday Adaptive	575	\$0.6 M	\$0.4 M	\$1.0 M
Finance & Procurement	Smartsheet	Smartsheet	70	\$0.1 M	\$0.1 M	\$0.1 M
Finance & Procurement	MS Project (Online)	MS Project (Online)	70	\$0.1 M	\$0.1 M	\$0.1 M
Network Operations	GSA Lite (Mobility)	GSA Lite (Mobility)	807	\$0.8 M	\$0.6 M	\$1.4 M
Network Operations	GE Smallworld + nfold Third party products	GE Smallworld	1366	\$1.4 M	\$1.0 M	\$2.3 M
Network Operations	OSISoft PI (Historian) (NIMS)	OSISoft PI (Historian)	125	\$0.1 M	\$0.1 M	\$0.3 M
Network Operations	ClearSCADA	ClearSCADA	1171	\$1.5 M	\$1.2 M	\$2.7 M
Network Operations	Metromaps	Metromaps	48	\$0.0 M	\$0.0 M	\$0.1 M
Network Operations	X-Info Connect	X-Info Connect	108	\$0.1 M	\$0.1 M	\$0.2 M
Network Operations	X-Info Assurance (BYDA)	X-Info Assurance (BYDA)	108	\$0.1 M	\$0.1 M	\$0.2 M
Network Operations	Autodesk CAD	Autodesk CAD	618	\$0.6 M	\$0.4 M	\$1.1 M
Network Operations	Salesforce Lightning	Salesforce Lightning	831	\$0.8 M	\$0.6 M	\$1.4 M
Network Operations	SmartIQ	SmartIQ	464	\$0.5 M	\$0.3 M	\$0.8 M
Network Operations	UiPath	UiPath	412	\$0.4 M	\$0.3 M	\$0.7 M
Network Operations	Maximo + BIRT	Maximo + BIRT	1681	\$1.7 M	\$1.2 M	\$2.9 M
Network Operations	ESRI products (ArcGIS, ArcGIS Enterprise, etc)	ArcGIS (eSRI Products)	658	\$0.7 M	\$0.5 M	\$1.1 M
Network Operations	Synergi Gas	Synergi Gas	603	\$0.6 M	\$0.4 M	\$1.0 M
Network Operations	SQL Database for Smart IQ?	SQL Database for Smart IQ?	412	\$0.4 M	\$0.3 M	\$0.7 M
Network Operations	FME & FME Server	FME & FME Server	412	\$0.4 M	\$0.3 M	\$0.7 M
Network Operations	PowerApps	PowerApps	317	\$0.3 M	\$0.2 M	\$0.5 M
Network Operations	Vault	Vault	618	\$0.6 M	\$0.4 M	\$1.1 M
Network Operations	GSA Warehouse + SQL Database for GSA Lite(Mobility)	GSA Warehouse	917	\$0.7 M	\$0.9 M	\$1.6 M
Network Operations	GSA Desktop	GSA Desktop	854	\$0.9 M	\$0.6 M	\$1.5 M
Network Operations	Bluecurrent	Bluecurrent	747	\$0.7 M	\$0.5 M	\$1.3 M
Regulatory & Compliance	Avetta	Avetta	70	\$0.1 M	\$0.1 M	\$0.1 M

Regulatory & Compliance	Safeguard Plus (HSE Management)	Safeguard Plus (HSE Management)	603	\$0.6 M	\$0.4 M	\$1.0 M
Technology	NASA	NASA	412	\$0.4 M	\$0.3 M	\$0.7 M
Technology	PowerBI	PowerBI	904	\$0.9 M	\$0.6 M	\$1.5 M
Technology	webMethods	webMethods	807	\$0.8 M	\$0.6 M	\$1.4 M
Technology	Nice CXOne	Nice CXOne	881	\$0.9 M	\$0.6 M	\$1.5 M
Technology	AIS / Biztalk	MS Azure Integration Services	1054	\$1.1 M	\$0.7 M	\$1.8 M
Technology	IBM Cognos / Workday Adaptive	Workday Adaptive	552	\$0.6 M	\$0.4 M	\$0.9 M
Technology	SSRS	SSRS	446	\$0.3 M	\$0.5 M	\$0.8 M
Technology	Databricks/ Enterprise Data Platform?	Databricks	1509	\$1.5 M	\$1.1 M	\$2.6 M
Technology	Shared network drives (unstructured data) + 9 different data repositories	APA: Data Transfer	298	\$0.2 M	\$0.3 M	\$0.5 M
Technology	Datamart	Datamart	618	\$0.6 M	\$0.4 M	\$1.1 M
Total			23,775	\$18.1 M	\$24.4 M	\$42.6 M

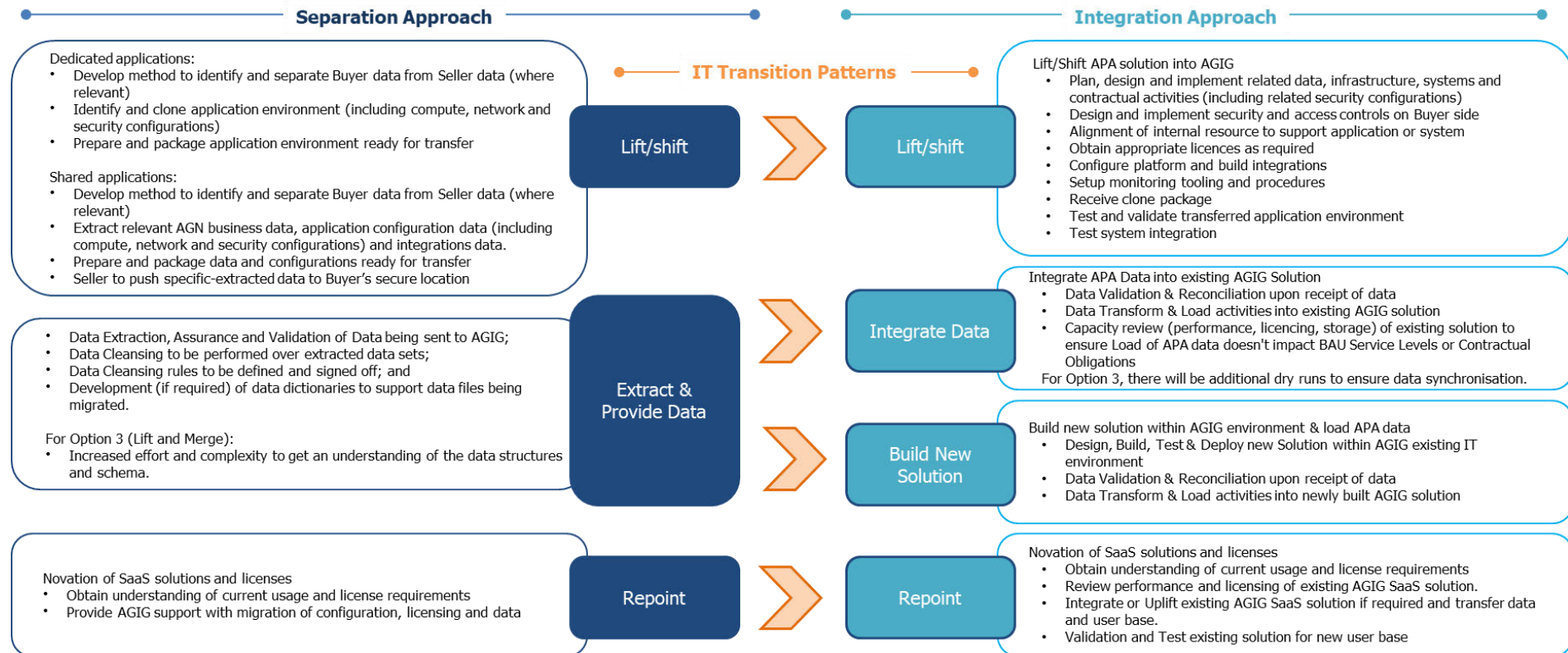
Appendix C Timeline for transition by option

This is the transition approach, and the associated timelines assumed for the 3 options. The timelines have been split as CAPEX / OPEX to distinguish between IT transition program and BAU support costs.



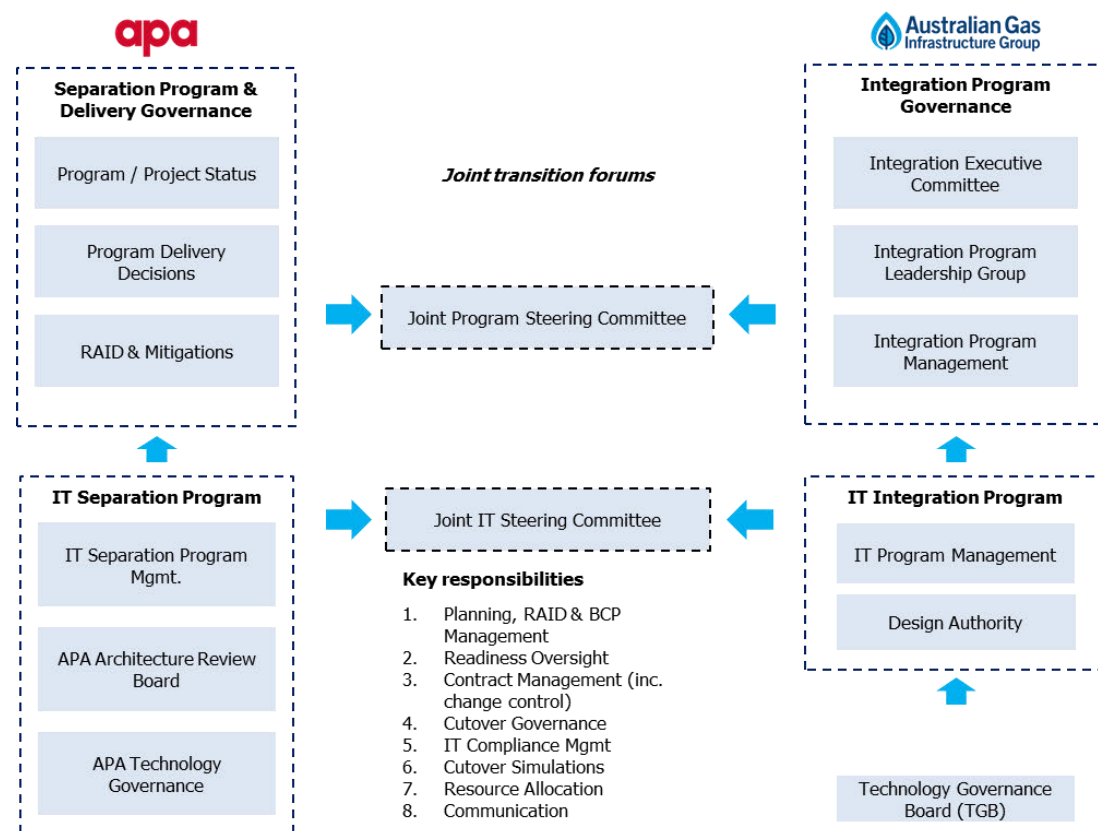
Appendix D Application transition patterns

Applications transitioning from APA to AGIG will follow a pre-defined IT separation and integration pattern, which is then used to determine effort and costs.



Appendix E Project governance

The proposed AGN transition governance model between APA and AGIG is summarised below.



Joint IT Governance

The proposed governance model enables AGIG's stakeholders to be engaged at all levels of decision-making.

- *Joint IT Steering Committee* – regular meeting between AGIG and APA representatives who are accountable for the IT transition program(s). The forum should provide transparency, operate under good faith and enable timely decision making.

Role of AGIG's Internal IT Governance

- *IT Integration Program Management* – Interacts with IT program delivery teams and AGIG IT PMO. Provides program reporting to other governance forums (as indicated).
- *Technology Governance Board (TGB)* – IT Leadership Team (LT) and Enterprise Architect to determine initiative alignment with AGIG's objectives.
- *Architectural Governance Authority (AGA)* – Cross-project architects and engineers to assess compliance of solutions with architecture & security standards and strategic objectives.
- *Design Authority* – Oversees compliance of designs with architectural and security standards by project teams.

Appendix F IT support model

There are five key layers of IT support that is required to be established to support AGN IT operations post transition



Appendix G Comparison of risk assessments

Untreated	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	Frequent	High
Consequence	Minimal	Minimal	Significant	Minor	Significant	Minor	Significant	
Risk level	Low	Low	High	Moderate	High	Moderate	High	

Option 1	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Low
Consequence	Minimal	Minimal	Significant	Minor	Significant	Minor	Significant	
Risk level	Negligible	Negligible	Low	Negligible	Low	Negligible	Low	

Option 2	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Remote	Remote	Low
Consequence	Minimal	Minimal	Significant	Minor	Significant	Minor	Significant	
Risk level	Negligible	Negligible	Low	Negligible	Low	Negligible	Low	

Option 3	Health & Safety	Environment	Operations	People	Compliance	Rep & Customer	Finance	Risk
Likelihood	Remote	Remote	Remote	Remote	Remote	Unlikely	Unlikely	Moderate
Consequence	Minimal	Minimal	Significant	Minor	Significant	Minor	Moderate	
Risk level	Negligible	Negligible	Low	Negligible	Low	Low	Moderate	