Technology program GAAR 2024-2028

Infrastructure Technology Asset Management (TAM – Infra)

missionzero

Table of Contents

1   Document Background

1.1   Purpose of this document

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

1.2   References

Document	Version	Author
AusNet Services FY19-FY23 Technology Plan	V1.0	AusNet Digital
GAAR Technology Strategy 2024-2028	V1.0	Ausnet Digital

1.3   Document History

Date	Version	Comment	Person
08/11/2021	V0.1	Initial draft	Sara Taylor
15/2/2022	V0.2	Initial review amendments	Mathew Abraham
01/06/2022	V0.3	Amendments for review	Mathew Abraham
13/06/2022	V.04	Post review amendments	Mathew Abraham

1.4   Approvals

Position
Technology Leadership Team

2 Executive summary

2.1 Program summary

The table below provides a summary of the Infrastructure Technology Asset Management (TAM) program. Additional information is provided throughout the brief.

Table 2-1 Summary table

Key objective(s) of the program	To mitigate operational and security risks by ensuring AusNet meets lifecycle and capacity obligations. This program reflects the move to cloud hosting necessitated by mitigating the risk of end-of-life assets, improved efficiency and flexibility, and the impact of COVID-19 and working from home. This program maintains some Data Centre (DC) infrastructure assets, including platforms, hardware and licenses, and uplifts cloud-based infrastructure to remain up to date, robust, scalable and continue to meet customer expectations, service obligations of business and regulatory requirements.
Key benefits	• Enables continued delivery of safe and reliable electrical services to customers with the least possible disruption, also meeting regulatory compliance and strategic business objectives. • Prudent mitigation of key operational risks by ensuring systems are up to date and supported by vendors. • Value for customers through controlled capex expenditure through effective lifecycle management to manage a growing asset base. • Appropriate risk management over the life of assets to ensure costs of delivering technology services are managed. • Removes potential security vulnerabilities through ensuring security patching is up to date, thereby reducing the risk of unauthorised access leading to data loss or loss of service to customers.

Cost allocation	Electricity Distribution	49%	Electricity Transmission	30%
	Gas Distribution	21%		

Program type	**Recurrent**	⊠
	Non-Recurrent	☐
	Client Devices	☐

Program timings	Program duration:	5 years				

Expenditure forecast	($m)	FY2023	FY2024	FY2025	FY2026	FY2027	Total
	CAPEX	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$6.96
	OPEX	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$5.13
	Gas Distribution Cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$12.08**
	Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$57.54

Program Brief

Estimated life of system	The expected life of systems are three to seven years, including servers, software and licenses and hardware compliance.
Customer engagement	This program was proposed (and approved) as part of AusNet's Electricity Distribution Price Reset (EDPR) and Transmission Revenue Review (TRR) submissions. This brief pertains to the Gas Access Arrangement (GAAR) allocation of these costs. We have undertaken significant stakeholder engagement. As part of the EDPR process, we held deep dive workshops with stakeholders on ICT. In that engagement, we described the importance and need for ICT expenditure to meet our customers' evolving needs and to support compliance with regulatory and legal obligations. We acknowledge the feedback received from both sessions and have taken it into consideration when proposing the most appropriate option for this business case. This brief has also taken into consideration: • The challenge we received from stakeholders as part of the GAAR engagement process to minimise discretionary IT spend where possible – a challenge consistent with the broader feedback we received on our capital investments. • Recent customer engagement studies conducted by AusNet, including the Energy Sentiments Survey (2021) and the AusNet Listening Report "Engaging Victorians on the Future of the Gas Networks" (2021).

AusNet is required to deliver safe and reliable gas services with the least possible disruptions to customers. IT infrastructure assets and systems underpin all operations at AusNet. To ensure the continued reliability of operations and in turn, the delivery of gas to customers, AusNet's infrastructure must remain up to date, be robust, scalable and agile to the changing demands of the business, regulatory and customer requirements.

Therefore, the objectives of the program are to serve these needs, including:

- Replacement of End-of-Life and Out-of-Support Hardware and Software to avoid infrastructure failure, disruption to customers, and increased security risk.
- Business improvements that will allow us to continue to address the increasingly challenging environment we face in a flexible manner.

The context in which AusNet operates its technology infrastructure has changed markedly in recent years, especially with respect to the growing importance of data and analytics, and remote access to technology infrastructure. During CY21, the business decision was made to bring the cloud adoption strategy forward, and self-fund the initial project migrating applications to cloud hosting. By the end of FY22, AusNet has migrated approximately over 60% of our applications to Cloud as part of our Digital Strategy.

The TAM Infrastructure technology program has consequently been amended from the program submitted as part of the EDPR and Transmission Revenue Rest (TRR), and now identifies four key initiatives to enable continuity of systems operations:

- Operating system version upgrades and license refresh.
- Hardware Assets Lifecycle refresh, including servers, etc.
- Application Hosting Initiatives (AHI) Server refresh.

Program Brief

- Maintenance and expansion of cloud hosted infrastructure.

This investment enables AusNet to avoid systems failure in AusNet's technology environments:

- Ensure AusNet meets its Lifecycle and Capacity obligations throughout FY2024-2028.
- Mitigate known operational risks and issues.
- Reduce effort for supportability of legacy infrastructure and applications.
- Maintain the technology environment in a vendor supported state.

Program Brief

Alignment with AER ICT expenditure assessment framework

In accordance with the AER - Guidance Note - Non-network ICT capex assessment approach for electricity distributors (28 November 2019), we have categorised this program as recurrent expenditure on the basis that it relates to ongoing refresh of AusNet's DC infrastructure assets, including platform, hardware and licenses, along with the capability shift to Cloud in the future periods. This allows AusNet's capacity and capability to remain up to date, robust, scalable and continue to meet service obligations of business and regulatory requirements.
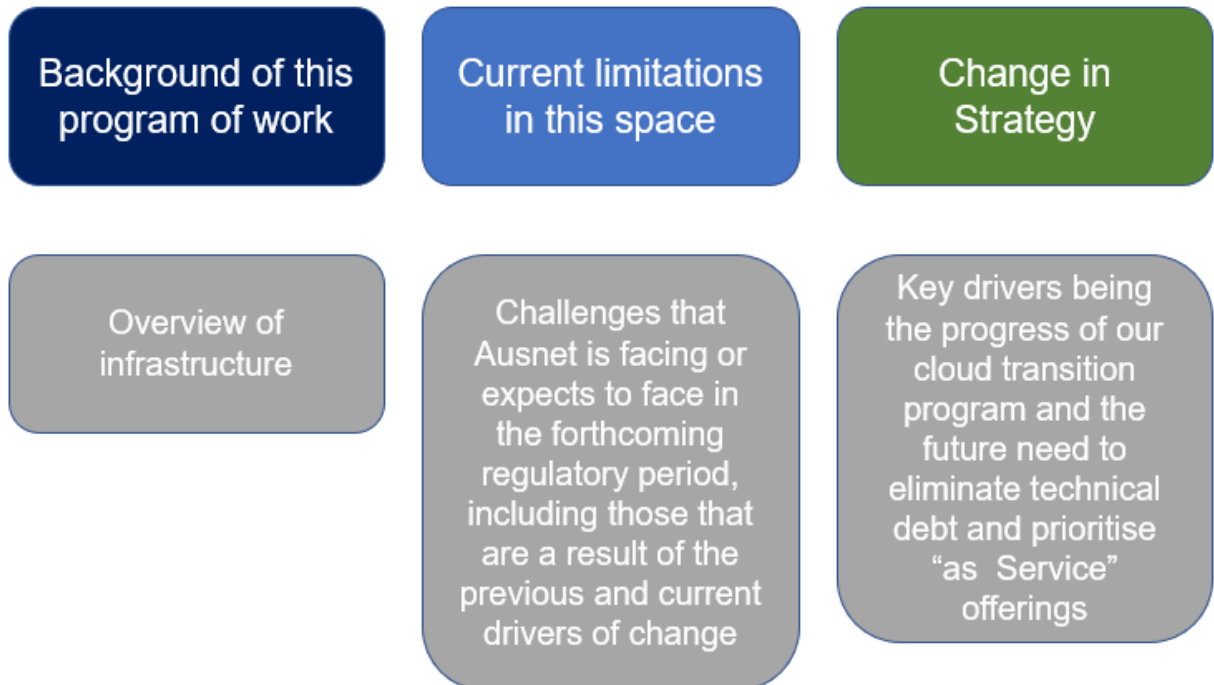
As the expected expenditure associated with this proposal must be incurred periodically, we have not undertaken NPV analysis in support of the project. However, consistent with AusNet's internal practices, we have developed a detailed business case for the chosen option.

3   Context

This chapter provides an overview of the context in which this program of work is operating within, and the figure below lists out key areas to be discussed.

Figure 3-1 Key areas of the context to be discussed

Background of this program of work	Current limitations in this space	Change in Strategy
Overview of infrastructure	Challenges that Ausnet is facing or expects to face in the forthcoming regulatory period, including those that are a result of the previous and current drivers of change	Key drivers being the progress of our cloud transition program and the future need to eliminate technical debt and prioritise "as Service" offerings

3.1   Background

The TAM Infrastructure program provides lifecycle refresh of infrastructure assets, end user assets and shared platforms (e.g., DC facilities and IT equipment). It is made up of specific assets requiring replacement during the regulatory period and the introduction of operational expenditure for hosting ICT infrastructure in the cloud.

The proposed expenditure on lifecycle refreshes secures the platform's support and technology spending in a controlled manner so that capacity, performance, and service levels can be maintained through the next regulatory period. By ensuring these systems continue to be supported by suppliers, AusNet gains access to the expertise required to resolve incidents, as well as patches for security vulnerabilities and bug fixes as they are available.
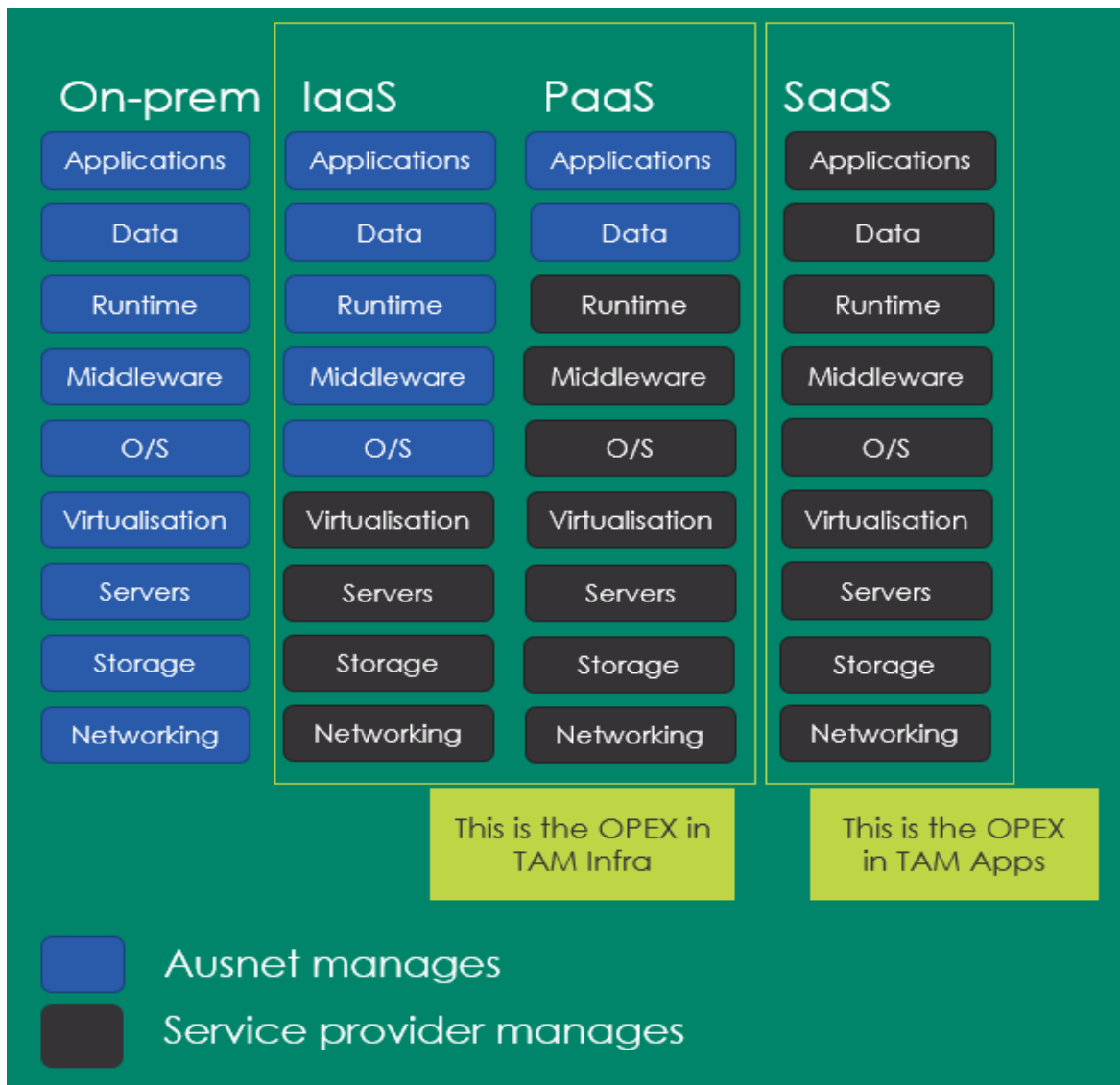
Critical assets such as SCADA, and others will need to remain on premise through the 2024-28 period; hence, AusNet needs to maintain its current DC assets.

The TAM program forms AusNet's recurrent technology investment to ensure lifecycle currency and capacity management.

3.2   Overview of technology infrastructure

ICT Infrastructure are the machines and networks on which AusNet host, run and store its business-critical applications, systems and data. It enables AusNet to transmit, distribute and regulate electricity and gas across its networks.

Program Brief

On-prem | IaaS | PaaS | SaaS

- Applications
- Data
- Runtime
- Middleware
- O/S
- Virtualisation
- Servers
- Storage
- Networking

This is the OPEX in TAM Infra

This is the OPEX in TAM Apps

- Ausnet manages
- Service provider manages

ICT applications and infrastructure consist of:

Applications	Also called programs or software, that perform a specific function directly for an end user, or for another application.
Data	Information processed or stored by a computer.
Runtime	The time when a program is running in the computer's working memory (RAM): from when it's opened (or executed) until it is quit or closed.
Middleware	Software "glue" that enables two separate programs, or databases to work together.
Operating Systems	Software that communicates with hardware and allows other programs to run (e.g., Microsoft Windows Server 2016).
Virtualisation	Enables the creation of virtual machines by allowing hardware elements of a single machine to be split into multiple virtual components. Virtualisation also then allows the one machine to run multiple operating systems.
Servers	Are specialised machines that provide resources, data, services or programs to other computers on the AusNet network.
Storage	One or multiple disks that provide a platform for hosting data often in file format.
Networking	Connections between computers and connecting users to servers.

Program Brief

Where all the above are owned, operated, and managed by AusNet within a DC, this is referred to as 'on-premise infrastructure'. These investments are assets and are therefore categorised as capital expenditure.

Refreshes, upgrades, and replacements are required to manage and maintain capacity, performance, and service levels, as the industry lifespan of the assets are between 3-5 years. Where possible, AusNet uses strategic investments and improvements to extend these assets past their natural life and, where possible, maintain vendor support.

There are ongoing costs associated with on-premise infrastructure. For example, the ongoing costs of on-premise servers includes:

- Direct running costs, such as power, floorspace, storage, ICT operations to manage resources.
- Indirect costs: network and storage infrastructure and ICT operations to manage the general infrastructure.
- Overhead costs: procurement and accounting personnel and ICT management.

The alternative to on-premise is the use of off-site solutions, such as that available through the cloud. Under an off-site solution, the cloud provider owns and supports the ICT infrastructure that host AusNet's applications.

There are varying levels of service offerings from cloud providers:

- Infrastructure as a Service (IaaS).
- Platforms as a Service (PaaS).
- Software as a Service (SaaS).

The below diagram demonstrates the ownership and accountability structure of each of these solutions versus on-premise solutions.

3.3   Current limitations

Assets replaced during a regulatory period are driven by the application demand (i.e., capacity, performance, etc.) and volume demands of the business at the point in time (e.g., number of employees).

Within any year, capacity, lifecycle and operational enhancement changes are required for business systems to meet the following needs:

- Probabilistic risk avoidance, mitigating the following risk category types:
  - Legal & compliance
  - Regulation
  - Health & Safety
  - Reputation.
- Identification of business improvements which will allow us to manage the cost of delivering technology services at an acceptable level of risk over the life of the assets.
- Minimise the risk of system failure and disruption to customer services.
- Minimise security threats of unauthorised access.

Therefore, lifecycle refreshes and enhancements in the forthcoming regulatory period will be of particular importance as they will provide stability and dependability of the infrastructure and compliance with regulatory and vendor support requirements. If lifecycle refreshes are not carried out, AusNet could be impacted by service failures in an unsupported environment, representing a critical

Program Brief

risk to the distribution of gas and electricity to customers. To ensure this does not occur, lifecycle initiatives must be implemented in a timely manner.

The infrastructure requirements for additional and new demand (i.e., new applications hosted in the DC) is not part of the TAM infrastructure lifecycle refreshment.[1]

3.4   Change in strategy

In the EDPR and TRR proposals, AusNet set out TAM Infrastructure spend based on three overarching initiatives.

1. The first initiative being refreshing the operating environment which included a version upgrade and license refresh of the current operating system, Citrix and firewalls. This accounted for approximately [C-I-C] the total program cost. This spend also included upgrades to servers, storage, networking and environmental hardware within the data centres, including air-conditioning and monitoring.

2. The second initiative refreshed largest IT infrastructure platform, AHI, and [C-I-C] of the on-premise applications (weighted by size). This platform runs the majority of corporate applications, and requires life-cycling to modernise, adhere to security standards and allow for ongoing supportability.

3. The final initiative involved the AOD (applications on demand) platform which required upgrades as its end-of-useful life falls in CY2022. The original plan was to refresh the platform [C-I-C] of AusNet's on-premises applications.

However, during CY21 AusNet decided to bring the cloud adoption strategy forward, and self-fund the initial phase (Horizon 1), which involved migrating of applications to cloud hosting. Consequently, by the end of FY22, AusNet will have migrated [C-I-C] of its applications to Azure cloud infrastructure as part of Horizon 1 of the Cloud Strategy.

Horizon 2 of the Cloud Strategy involves greater use if cloud infrastructure use with the AOD platform decommissioned at the end of its useful life. That is, this phase begins to retire legacy applications to optimise cloud costs and start simplifying the tech stack. The consolidation of AHI will require a mix of capex and opex, while the continued cloud migration is classified as opex.

[C-I-C]

[C-I-C]

3.5   Decision drivers

The two key drivers of the decision to migrate to cloud are the AOD platform rapidly approaching end-of-life and a shift in industry to cloud based offerings.

---

[1] This aligns with the definition of recurrent expenditure in the AER's Consultation paper – ICT Expenditure Assessment.

Program Brief

As technology ages, the cost of maintenance increases as the manufacturer stops providing maintenance or component upgrades (such as additional disk or memory). The reliability of the equipment reduces to the point that replacement is the most effective option to address this risk. In the case of AOD, the cost to ensure reliability and performance of the platform was   [C-I-C] of the on-premise applications, compared to   [C-I-C]   , the cost to modernise AOD appeared increasingly inefficient and alternative, more prudent and efficient options, needed to be considered.

Across industries and government, organisations have adopted a "cloud first" architecture principle. The Australian Government has been actively promoting the approach, as stated in its Cloud Strategy "Improved adoption of cloud services by the government sends an important signal to the private sector. If government agencies were perceived to be treating cloud services as risky, this could reduce adoption in the economy more generally." (Australian Government- Department of Finance, 2014). The ACCC and AER's own Annual Report for 2020-2021 also calls out its cloud-first approach in order to enhance flexibility (Australian Energy Regulator, 2021).

The move to adopt cloud-first approaches stem from the technology industry itself moving to cloud offerings. Application vendors have been shifting to cloud-based solutions as a way to nimbly adapt to customer demands. Cloud infrastructure can leverage economies of scale deliver multi-benefit offerings at a lower cost than designed in-house. These on-demand offerings have become increasingly attractive to manage lumpy capex requirements to upgrade on-premises data centres.

3.6   Technology risk drivers

All TAM expenditure initiatives proposed by AusNet reflect the least cost option at the maximum level of risk that the business (and the customer services they support) can reasonably tolerate:

1. **Technology risk increases over time.** Hardware failures follow a pattern of fail in the first months of operation, stable operation for a number of years, and exponential increase in failures after the end of life as defined by the manufacturer. This failure curve is known as the 'bathtub curve'[2]. Extending the life of technology after the vendor end of life date increases business and service performance risk as the likelihood of failure increases.

2. **As technology ages the cost of maintenance increases.** Equipment vendors will provide cost effective support until a point is reached where their costs increase. Vendors need to provide internal capability to support both old and new products, where the old products are used by a decreasing customer base. This cost is passed on to the customer and often exceeds the cost of deploying and maintaining new technology.

3. **Spare parts become unavailable.** Technology relies on a supply chain of components and suppliers, which are subject to component lifecycle management. After a number of years, a manufacturer will be unable to source component parts making it impossible to produce spare parts. Reliable access to spare parts is then compromised and the risk of unserviceable outages increases.

4. **The price-performance of technology infrastructure continues to improve over time**, lowering the total cost of delivering like-for-like services. Failing to refresh infrastructure locks in higher costs and lower service capabilities.

5. **Security.** AusNet's DC assets need to be protected against cyber security threats. Ongoing patching is required to remove vulnerabilities which allow for unauthorised access leading to major business disruption or loss of critical information. When technology is no longer supported by a manufacturer no new patches are made available to address security vulnerabilities. The

---

[2] *Basic terms and models used for reliability evaluation*, National Institute of Standards and Technology at https://itl.nist.gov/div898/handbook/apr/section1/apr124.htm and *Software Reliability,* Jiantao Pan (Carnegie Mellon University) at https://users.ece.cmu.edu/~koopman/des_s99/sw_reliability/

Program Brief

risk of unauthorised access leading to data loss, loss of service, or non-compliance with regulatory requirements, increases over time.

3.7   Business drivers

In the face of significant industry disruption resulting in a period of substantial uncertainty and increasing complexity across the industry, AusNet has selected four key business drivers which set the direction for the business.

These business drivers are:

- Maintaining current service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid.
- Updating and implementing new technologies to enable AusNet to respond to changes within the growing renewable generation market.
- Complying with new obligations.
- Delivering improvements requested by our customers regarding sustainability and cost.

All expenditure programs identified and proposed by AusNet will have regard to the business drivers and can be directly linked to at least one of these initiatives.

This program of work is most relevant to the following business driver:

- **'Maintaining current service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid'**, as it contributes to increased effectiveness and capability in managing and maintaining a robust technology environment.

3.8   Approach to developing expenditure forecast

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

A full overview of the approach can be found in section 3.2 of the GAAR Technology Strategy 2024-2028 document.

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

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

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

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

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

4   Options

4.1   Overview

This section provides an overview of a select number of options that may feasibly alleviate the current limitations as addressed in section 3.2. Each option represents a combination of initiatives within the program of work.

Table 4.1 Brief overview of the options

Brief overview of each of the options	
Option 1	Minimise Capex Investment This option refers to "sweating the assets", which does not adopt a proactive approach to ensure continued vendor support and mitigation of operational risks. Key initiatives include: • Operating Systems version and license refresh. • Application Hosting Initiative Platform and Server Refresh. • AOD Refresh only to extend use past end of life. • Service Now platform buildout & GRC for security and IT.
Option 2 (Recommended)	Managing cloud-based infrastructure services - IaaS and PaaS, while decommissioning AOD and refreshing AHI on-premise infrastructure to mitigate operational and security risks. Key initiatives include: • Option 1 initiatives except AOD refresh. • Hardware Lifecycle Refresh, including air-conditioners (AC) for Data Centers, backup storage, and Network Attached Storage (NAS). • Furthering cloud adoption framework and migration strategy associated planning. • Including an opex step-change for operational costs of cloud infrastructure services.
Option 3	Strategically migrate AusNet to cloud-based infrastructure services – IaaS and PaaS while sweating hardware assets in the transition period. Key initiatives include: • All Option 1 initiatives during transition period (except AOD refresh), plus • Cloud adoption framework & migration strategy associated planning. • Establish SDN (software define networking) platform for DC infrastructure. • Rollout workload automation and orchestration capability. • Cloud Migration - IT & OT Workloads. • IT / OT Convergence.

4.2   Option #1 Sweat hardware assets

This option is involves extending the life of existing hardware assets and requires that AusNet does not adopt a proactive approach to improving infrastructure hardware assets impacted by capacity and lifecycle constraints when falling out of vendor support. This option is presented as a "do nothing"

Program Brief

approach demonstrating a high risk of system failure with critical consequences likely to result in non-compliance with regulations or business objectives. Therefore, this option is not recommended.

Alignment to objectives

Table 4-2 Objectives analysis of Option 1

Objective	Outcome	Comments
Mandatory requirements, including safety, legal, regulatory and technical compliance.	Partial	Partially aligned as this option involves the adoption of significant risks and system failure could result in the following critical risk category types: a. Legal & Compliance b. Reputation c. Regulation d. Health & Safety.
Business improvements that will improve efficiency and manage costs and risk over time	Partial	Partially aligned as it may seem to be a lower upfront expenditure option. However, a higher risk environment would lead to an unsupported operating environment, potentially higher long-term support costs and lower productivity in business.
Replacement of End-of-Life and Out-of-Support Hardware and Software to avoid infrastructure failure, customer disruption and increased operational expenditure.	✗	Not aligned as infrastructure assets failure will result in disruption to customers and increased operational expenditure.

Costs

The direct cost of Option 1 addresses platform and license maintenance requirements excluding hardware asset refresh.

Table 4-3 Costs of Option 1

($m)	FY2024	FY2025	FY2026	FY2027	FY2028	Total
Capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$18.02
Opex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$0.94
Gas Distribution Cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$8.13**
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$38.71

Importantly, the costs in the table above do not include the costs associated with critical system failure - either to AusNet or its customers. Such costs have not been modelled but are related to safety obligations/initiatives, regulatory, compliance and/or reputational costs. The risk of incurring these costs, which may be significant, is higher under this option compared to Option 2 or 3.

Program Brief

Benefits

Sweating assets could save AusNet investment expenditure, with   [C-I-C]   compared to Option 2 across the three businesses.

However, this approach does not consider the increased risk of system failure and increased expenditure, both capex and opex, due to a change of environment. For example, avoiding refreshes now would require greater investment in the future should an unsupported system failure occur. This will allow us to manage the cost of delivering technology services at an acceptable level of risk over the life of the assets.

Risks

There are several risks associated with this option, as highlighted in the table below. Based on the consequence and likelihood of each risk, we have rated each of the individual risks blue, green, yellow, orange or red (in order of severity). Below in Table 5-3, we have identified techniques or actions to mitigate the risks identified for this option.

Table 5-3 Option 2 risks and mitigation actions

	Risk	Rating	Mitigation
R2.1	Lower operational risk due to system failure.	D	Lifecycle maintenance as per manufacturer's specification.
R2.2	Increased cost and complexity of maintaining datacenter centric infrastructure assets.	E	Lifecycle maintenance as per manufacturer's specification Continue optimizing on premise data centre to move towards cloud-based services.
R2.3	Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	D	This is a common risk across all business areas.

Attachment 1 – Risk level matrix for additional information on this rating system.

Table 4-4 Risks of Option 1

	Risks	Consequence	Likelihood	Risk rating
R1.1	Hardware that is out of support and has gone end of life places the business at risk in the event there is a hardware failure, firmware issue or BIOS issue.	Level 2. Business impact in the form of productivity loss.	Likely	C
R1.2	Unsupported systems may fail, and no support or maintenance services will be available to call upon.	Level 2. Customer / community affected by loss of service.	Likely	C

Program Brief

R1.3	Increased cost and complexity of maintaining Data Centre infrastructure assets.	Level 1. An impact that would have otherwise required minor management attention.	Likely	D
R1.4	Reduced or loss of employee productivity and business functions.	Level 1. Impact of event absorbed through normal activity.	Likely	D
R1.5	Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	Level 1. An impact that would have otherwise required minor management attention.	Possible	E

Overall, we consider this option is rated medium risk.

Alignment to mitigation of key risk drivers

As discussed in Section 3.3, there would be no alignment in respect of maintaining vendor support of current assets with security benefits.

Table 4-5 Alignment to key risk drivers of Option 1

Risk Driver		Achieved by
Technology risk increases over time	X	N/A
Cost of maintenance increases as technology ages	X	N/A
Spare parts unavailable	X	N/A
Availability of new technology	X	N/A
Security	X	N/A

Alignment to business related drivers of expenditure

As discussed in Section 3.4, there are four Gas Distribution business drivers that AusNet has identified and is focussing on over the next regulatory period. In summary, the business drivers are not directly relevant to this option.

4.3   Option #2 Tactical Cloud Migration and Lifecycle Refresh (RECOMMENDED)

This option is a shift away from the TAM lifecycle program proposed in the EDPR and the TRR. The recommended option now involves carrying out lifecycle refresh on-premises infrastructure within data centres for the applications that will continue to remain on-premises, including the consolidation of the AHI platform. This recommendation includes an opex step-change reflecting the tactical migration of some applications from the end-of-life AOD platform to cloud.

Our policy for the frequency with which individual on-premise assets are refreshed is aligned to our Technology Asset Management Policy and is dependent on the business criticality of the services they

Program Brief

support and the risk of their failure with age. The introduction of cloud hosted infrastructure transfers the risk of lifecycle related failure to the cloud infrastructure provider.

Alignment to objectives

Table 4-6 Objectives analysis of Option 2

Objective		Comments
Mandatory requirements, including safety, legal, regulatory and technical compliance; and	✓	Lifecycle maintenance, as per manufacturer's specification. Reliable and vendor supported system contributes to mitigate the operational and security risks
Business improvements that will improve efficiency and reduce Operational Expenditure; and	✓	Mitigate the risk of system failure and disruption to business operations.
Replacement of End-of-Life and Out-of-Support Hardware and Software to avoid infrastructure failure and increased operational expenditure	✓	Lifecycle maintenance delivers more efficient technology, so subsequent refreshes have lower capital costs.

Costs

Infrastructure assets that will be required to be refreshed within TAM include storage and compute appliances, security operational tools and licensing. Lifecycle refreshes include Database, Virtualisation Software, Environment Management and other shared platform-based refreshes. This also includes refreshes to other physical equipment used to run the IT environment such as air-conditioning.

As the cloud migration project has already commenced, the costs originally proposed to upgrade the AOD platform has been shifted from capex to opex to support cloud infrastructure costs. The proposed opex step-change aligns with the expected costs of the cloud migration roadmap set out within the cloud strategy.

ServiceNow (SNOW) is a service management tool and central source of truth for infrastructure assets and shared platforms (i.e. the CMDB). This provides evidence on the level of capacity management, ensures that infrastructure has appropriate monitoring in place and is delivering data to capacity management.

Table 4-7 Costs of Option 2

($m)	FY24	FY25	FY26	FY27	FY28	Total
Capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$6.96
Opex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$5.13
Gas distribution cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$12.08**
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$57.54

Benefits

Program Brief

Lifecycle maintenance delivers more efficient, stable technology at lower risk. Moving to the cloud as part of this lifecycle presents an opportunity for AusNet to better control its costs. As the digital transformation continues at AusNet, the demands on computing increases. Cloud infrastructure allows for faster time to provision and deprovision resources based on demand. As resources are only powered on demand, there is a significant increase in transparency and accountability of cost of ICT.

The flexibility to scale extends to increasing innovation. Cloud hosting empowers faster collaboration and problem solving as there is better access to programs, files and data. Ease of access to data is a key requirement for advanced analytics and data-driven decision making, which has been a key focus of the broader AusNet Digital Strategy. While the impact of the energy transition on gas is still uncertain, the ability to quickly adapt to new policy and fuels will require the type of data-driven decision making and cost flexibility cloud can provide.

This flexibility is dependent on the shift from capex investment to opex. In this context, an opex step-change is beneficial as it gives AusNet the flexibility to terminate costs at will, as opposed to purchasing servers and software and remaining fully committed to the investment and ongoing maintenance and support costs for full life of asset regardless of utilisation. The cost structure of cloud solutions encourages further efficiencies and improved utilisation, as pay as you go makes inefficiencies apparent sooner than on-premises.

Further, cloud hosted infrastructure mitigates the internal risk of end-of-life and underperforming hardware and transfers it to the cloud provider – who can use economies of scale to provide more and better service (bandwidth, RAM, monitoring etc) as part of their model. Cloud infrastructure also mitigates security issues as patching and upgrades is part of the service.

More broadly, there are other benefits to technology infrastructure lifecycle maintenance listed below:

Table 4-8 Benefits of Option 2

Benefits
Reduced likelihood and subsequently avoided cost of critical system failure and increase in support/maintenance costs.
Improved system and customer information security compared to Option 1.
Conservatively future proofing against potential changes in adjacent systems that may require an up-to-date systems to function and ensuring that AusNet has the ability to adapt to alternative technologies can reduce the cost to serve and in doing so, lower prices for customers.

Risks

There are risks associated with this option, as highlighted in the table below. Based on the consequence and likelihood of each risk, we have rated each of the individual risks blue, green, yellow, orange or red (order of severity). See Below in Table 5-3, we have identified techniques or actions to mitigate the risks identified for this option.

Table **5-3 Option 2 risks and mitigation actions**

	Risk	Rating	Mitigation
R2.1	Lower operational risk due to system failure.	D	Lifecycle maintenance as per manufacturer's specification.
R2.2	Increased cost and complexity of maintaining datacenter centric infrastructure assets.	E	Lifecycle maintenance as per manufacturer's specification Continue optimizing on premise data centre to move towards cloud-based services.
R2.3	Risks associated with solution design, implementation,	D	This is a common risk across all business areas.

	budgeting, planning, integration, future maintenance, refreshes and support.		

Attachment 1 – Risk level matrix for additional information on this rating system.

Table 4-9 Risks of Option 2

		Risks	Consequence	Likelihood	Risk rating
R2.1		Lower operational risk due to system failure	Level 2 business impact in the form of productivity loss.	Possible	D
R2.2		Increased cost and complexity of maintaining datacenter centric infrastructure assets.	Level 1. An impact that would have otherwise required minor management attention.	Possible	E
R2.3		Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	Level 2. An impact that would have otherwise required minor management attention over several days.	Possible	D

Overall, we consider this option is rated Low.

Alignment to mitigation of key risk drivers

As discussed in Section 3.3, this option is fully aligned in respect to reducing technology risk and providing a stable environment.

Table 4-10 Alignment to key risk drivers of Option 2

Risk Driver		Achieved by
Technology risk increases over time	✓	For on-premise infrastructure: By maintaining critical systems in line with their supplier lifecycle maintenance requirements. The shift to cloud infrastructure transfers the risk to the cloud provider.
Cost of maintenance increases as technology ages	✓	Staying in Vendor support window is more efficient and cost effective than getting customised vendor support. The shift to cloud infrastructure transfers the risk to the cloud provider.
Spare parts unavailable	✓	Maintaining infrastructure assets in line with its lifecycle ensures spare parts availability reducing down time. The shift to cloud infrastructure transfer the risk to the cloud provider.
Availability of new technology	✓	Obtain efficiency by replacing obsolete technology.

Security	✓	Critical lifecycle refresh remedies the vulnerabilities and ensure the security and reliability of the network

Alignment to business related drivers of expenditure

As discussed in Section 3.4, there are four Gas Distribution business drivers that AusNet has identified and is focussing on over the next regulatory period. The table below highlights how this option will input into the initiatives where relevant. Where we consider that a business driver is not directly relevant to the option, 'N/A' is applied.

Table 4-11 Business related drivers of Option 2

Business drivers	How this program achieves this
Maintaining current service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid;	Refreshing current applications and upgrading where prudent. Allow for increased effectiveness and capability in managing and maintaining a robust technology environment
Updating and implementing new technologies to enable AusNet to respond to changes within the growing renewable generation market;	Maintaining infrastructure assets in line with its lifecycle allows the business to continue to operate efficiently and limit system outages. System outages cause delays and increase the cost of operating the business
Complying with new obligations	N/A
Delivering improvements requested by our customers regarding sustainability and cost.	Operation risks are mitigated. Therefore, continuity and reliability of supply is maintained, which contributes to brand and reputation.

4.4   Option #3 Strategic Migration to Cloud

Option 3 involves the capabilities enablement and migration of IT and OT workloads to Cloud services. This means that AusNet will exit the on-premise data centers to Cloud services. Opportunities, costs and benefits to the business associated with this option are explored further in below sections.

Alignment to objectives

Table 4-12 Objectives analysis of Option 3

Objective		Comments
Mandatory requirements, including safety, legal, regulatory and technical compliance.	✓	Cloud infrastructure provides a stable and reliable platform for business deployment. The cloud platform minimizes the frequency of application downtime and reduces risk based on downtime. Cloud infrastructure further reduces risk with built in security hardening of servers and databases.

Program Brief

Business improvements that will improve efficiency and reduce Operational Expenditure.	✓	Cloud infrastructure allows for significant savings over on-premise data centers with utility-based metering and pricing model. This allows business to right-size their resources based on demand and shifts businesses away from large upfront capex to opex spend on infrastructure.
Replacement of End-of-Life and Out-of-Support Hardware and Software to avoid infrastructure failure and increased operational expenditure.	✓	Operational expenditure is optimised due to significantly reduced on premise requirements.

Costs

Migration to Cloud is a significant change. Necessary lifecycle refresh will still be included during the transition period, considering the implications for the continuity of operations during the transition period.

Table 4-13 Costs of Option 3

($m)	FY24	FY25	FY26	FY27	FY28	Total
Capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$13.53
Opex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$5.44
Gas distribution cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$18.97**
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$82.01

Benefits

While infrastructure optimisation is a benefit of Cloud Adoption, greater opportunities can be realised through adopting modern ways of working with increased agility and productivity. Efficiencies gained from cloud infrastructure have a significant impact beyond cost savings that enable businesses to respond quickly to market changes.
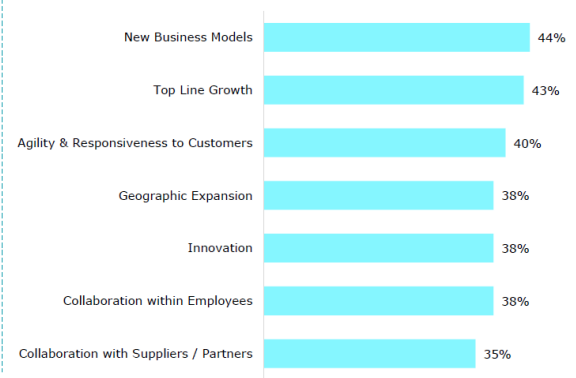
In addition, Cloud can enable improved effectiveness as shown in the diagram below.

Program Brief

Cloud is improving effectiveness

37% decrease in average time to deploy new applications — **INCREASED AGILITY**

118% increase in # of business applications deployed per year — **INCREASED OUTPUT**

22% decrease in size of app dev teams — **LEANER TEAMS**

80% reduction in unplanned downtime instances per year — **IMPROVED RELIABILITY**

% of companies seeing impact of Cloud adoption

New Business Models	44%
Top Line Growth	43%
Agility & Responsiveness to Customers	40%
Geographic Expansion	38%
Innovation	38%
Collaboration within Employees	38%
Collaboration with Suppliers / Partners	35%

Note: The results above are representative of AWS
Source: IDC Whitepaper | Quantifying the business value of AWS, 2015

4

[3]The table below summarizes the benefits associated with this option and quantifies them where appropriate data is available or reasonable assumptions can be applied over the 2024-2028 period.

---

[3] IDC Whitepaper. Quantifying the business value of AWS, 2015

Program Brief

Table 4-14 Benefits of Option 3

Benefits
Reduced on premise Data centre requirements, including: Reduced Linux OSI requirements   Reduced Wintel OSI requirements   Reduced Solaris OSI requirements   Reduced VMWare requirements   Reduced ESX Physical costs   Reduced Storage Costs   Reduced DC Cost Allocation   Reduced Service Provider Management Fees   Cloud infrastructure allows for significant savings over on-premise data centers. This allows business to right-size their resources based on demand and shifts businesses away from large upfront capex to opex spend on infrastructure.
Risk Mitigation   Cloud infrastructure provides a stable and reliable platform for business deployment. The cloud platform minimizes the frequency of application downtime and reduces risk based on downtime. Cloud infrastructure further reduces risk with built in security hardening of servers and databases.
IT Staff Productivity   Less downtime and higher levels of automation increase overall business productivity. Cloud infrastructure requires less time to manage, administer, and update, increasing employee productivity by allowing employees to focus on adding business value. As a result, this can introduce a reduction in head-count due to efficiencies in Cloud.
Agility   Businesses can leverage the flexible and fast provisioning that Cloud infrastructure provides to be able to spin up and down infrastructure without incurring high setup costs to enable businesses to respond business needs and drastically increase their procurement efficiency.
Scale   Scalability is a key feature of Cloud infrastructure that dramatically impacts business's ability to respond to market demand to support their core business. Capacity requirements are handled automatically to allow for seamless change in resources based on demand.

AusNet will transition to cloud progressively over the following regulatory periods as commercially prudent (when assets require replacing) and without exposing the business (and our customers) to undue transition risk. Many of these benefits require all elements of an organisation's ICT environment to be cloud hosted.

Risks

There are several risks associated with this option, as highlighted in the table below. Based on the consequence and likelihood of each risk, we have rated each of the individual risks blue, green, yellow, orange or red (in order of severity). See the table below:

Program Brief

Table 4-15 Risks of Option 3

	Risks	Consequence	Likelihood	Risk rating
R3.1	The investment in Cloud is perceived to not directly be beneficial to the customers in terms of costs.	Level 2. Minor impact on the level of service that would have resulted in a less 10% increase in customer complaints.	Possible	D
R3.2	Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	Level 2. An impact that would have otherwise required minor management attention over several days.	Possible	D
R3.3	A large component of risk associated with infrastructure is outsourced to the cloud provider.	Level 2. 3rd party risk Breach of law with investigation or report to authority with prosecution and/or moderate fine possible	Possible	D

Overall, this option is rated Low risk. Unlike Option 2 however migration to the cloud in Option 3 comes with transition risks. Attempting to migrate AusNet's entire infrastructure portfolio into the cloud in a five-year period would concentrate these transition risks.

Alignment to mitigation of key risk drivers

As discussed in Section 3.3, this option is fully aligned in respect to reducing technology risk and providing a stable environment.

Table 4-16 Alignment to key risk drivers of Option 3

Risk Driver		Achieved by
Technology risk increases over time	✓	By maintaining critical systems in line with their supplier lifecycle maintenance requirements.
Cost of maintenance increases as technology ages	✓	Staying in vendor support is more efficient and cost effective than requiring customised vendor support.
Spare parts unavailable	✓	N/A for cloud whereby assets are not maintained on premise.
Availability of new technology	✓	Obtain efficiency by replacing obsolete technology.
Security	✓	N/A for cloud whereby assets are not maintained on premise as long as the connectivity tunnels are secured.

Alignment to business related drivers of expenditure

Program Brief

As discussed in Section 3.4, there are four Gas Distribution business drivers that AusNet has identified and is focussing on over the next regulatory period. The table below highlights how this option will input into the initiatives where relevant. Where we consider that a business driver is not directly relevant to the option, 'N/A' is applied.

Table 4-17 Business related drivers of Option 3

Business drivers	How this program achieves this
Maintaining current service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid.	Refreshing current applications and upgrading where prudent.
Updating and implementing new technologies to enable AusNet o respond to changes within the growing renewable generation market.	Taking the advantage of Cloud platform, will enable AusNet having the capability and capacity to move towards real time monitoring and analytics capabilities positions.
Complying with new obligations.	N/A
Delivering improvements requested by our customers regarding sustainability and cost.	Cloud hosting to enable speed to market of solutions through fast access to required compute resources. New devices to provide broader mobility capabilities and improved network connectivity.

5 Assessment and recommended option

5.1 Assessment of the options

To identify a recommended option for this program of work, we have selected a number of criteria to assess each of the options. We consider these criteria ensue a comprehensive view of each options ability to achieve AusNet's customer and business objectives as well as the AER's requirements that any expenditure is both prudent and efficient.

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

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

	Option 1	Option 2	Option 3
Alignment to objectives	Does not achieve objectives	Aligned with program objectives	Aligned with program objectives
Costs ($m)	$8.13	$12.08	$17.22
Overall risk rating	Medium	Low	Low
Alignment to technology risk drivers	Low alignment (1/5)	High alignment (5/5)	High alignment (5/5)
Alignment to business related drivers of expenditure	No alignment (0/4)	High alignment (3/4)	High alignment (3/4)

5.2 Recommended Option – Risk Mitigation

Based on this assessment, **Option 2 is the recommended option**, as it reflects a prudent level of expenditure that will progress AusNet towards its objective of efficient and effective operations while maintaining current reliability levels and increasing expenditure flexibility. However, the implications for the continuity of operations while moving towards cloud-based services should be a key consideration in future design decisions.

The cloud migration experience to date has demonstrated a tolerable level of transitional risk.

Because Option 2 and Option 3 meet the objectives at a similar level of risk but Option 3 comes with a substantially higher transition risk, Option 2 represents a more prudent transitional approach as AusNet pursues a medium-term migration from on-premise infrastructure to the cloud.

Table 5-2 Confirmation of scope of recommended option

In scope	Out of scope	Dependencies
Operating system version and license refresh.	n/a	TAM Applications (separate program).
Hardware Assets Refresh, including network storage, servers and field mobility hardware.	n/a	Corporate Communications (separate program).
AHI Server Refresh and consolidation.	n/a	Broader business decisions on Cloud strategy.
AOD Decommissioning.	n/a	Broader business decisions on Cloud strategy.
Migration of some of DC to public cloud.	Establishing Private cloud in Co-location facility.	Broader business decisions on Cloud strategy.

Below in Table 5-3, we have identified techniques or actions to mitigate the risks identified for this option.

Table 5-3 Option 2 risks and mitigation actions

	Risk	Rating	Mitigation
R2.1	Lower operational risk due to system failure.	D	Lifecycle maintenance as per manufacturer's specification.
R2.2	Increased cost and complexity of maintaining datacenter centric infrastructure assets.	E	Lifecycle maintenance as per manufacturer's specification Continue optimizing on premise data centre to move towards cloud-based services.
R2.3	Risks associated with solution design, implementation, budgeting, planning, integration, future maintenance, refreshes and support.	D	This is a common risk across all business areas.

Attachment 1 – Risk level matrix

The figure below shows the risk level matrix to which we have assessed each of risks within the options. Risks of highest concern are rated red, whereas those of lowest concern are rated blue.

Figure 0-1

		Consequence				
		1	**2**	**3**	**4**	**5**
Likelihood	**Almost Certain**	C	C	B	A	A
	Likely	D	C	B	B	A
	Possible	E	D	C	B	A
	Unlikely	E	D	D	C	B
	Rare	E	E	D	C	C

Consequence Rating	
5	Catastrophic
4	Major
3	Moderate
2	Minor
1	Insignificant

Overall Risk Rating	
A	Extreme
B	High
C	Medium
D	Low
E	Very Low