Attachment 8.4

DBP IT Investment Plan 2021-25

January 2020

Dampier Bunbury Pipeline

Contents

1. Executive Summary

1.1. Introduction

Australian Gas Infrastructure Group (AGIG) is one of the largest gas infrastructure businesses in Australia. We serve more than two million customers across every mainland state and the Northern Territory through 34,000km of distribution networks, over 4,000km of transmission networks and 42 petajoules of storage capacity.

In Western Australia, trading as Dampier Bunbury Pipeline (DBP), we own and operate the Dampier to Bunbury Natural Gas Pipeline (DBNGP), which is Western Australia's most critical piece of domestic energy infrastructure and the backbone of the state's economy. The DBNGP transports large volumes of gas from the domestic gas producing plants on the North West Shelf and Pilbara Coast to demand centres in the Pilbara, Perth and South West.

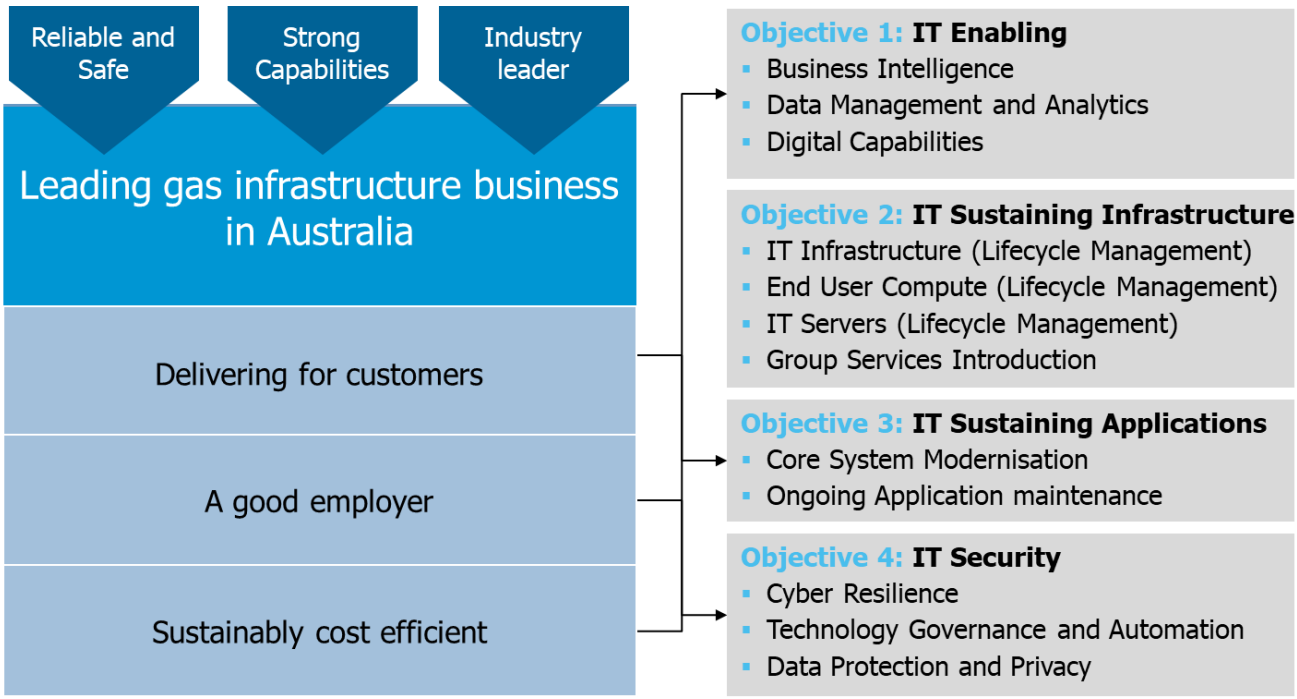
Our vision is to be the leading gas infrastructure business in Australia by delivering for customers, being a good employer and being sustainably cost efficient. Our values of respect, trust, perform and one team drive our culture, how we behave, and how we make decisions. As guardians of critical infrastructure which provide essential services to Australians, we must ensure we act with integrity and do the right thing for current and future generations. We have a strong asset management focus. Our information and technology systems (DBP IT) are integral to delivering safe, reliable and efficient services.

We must comply with a range of legal and regulatory obligations that can only be met with the information provided by DBP IT. We have ongoing asset management and maintenance plans for our critical information systems, based on appropriate risk assessments, to ensure continued compliance with our legal and regulatory obligations.

Our DBP IT Investment Plan is a component of our plans for the 2021-25 Access Arrangement (AA) period, also known as AA5. It has been developed with reference to the current state, emerging industry trends and drivers and a fit-for-purpose future state. It outlines a high-level budgetary model and roadmap of initiatives that will support our vision and values over the five years 2021-25.

Figure 1 below summarises our DBP IT strategic objectives that will support our vision of delivering for customers, being a good employer and being sustainably cost efficient.

Figure 1: DBP IT strategic objectives



1.2. IT expenditure for AA5

Our DBP IT expenditure for AA5 includes DBP IT capital expenditure (capex) projects and programs, as well as ongoing operating expenditure (opex) for hardware consumables, licencing, maintenance and support, our managed support costs, and software licencing, maintenance and support and purchases.

All costs, prices and benefits quoted in this document are unescalated dollars of June 2019, unless otherwise stated.

1.2.1. Capex

Over AA5, we propose total DBP IT capex investment of $16.9 million on projects and programs across four key areas (IT Enabling, IT Sustaining Infrastructure, IT Sustaining Applications and IT

Security). We also have a specific project related to our Customer Reporting System (CRS). The capex investment for each is summarised in Table 1 below.

Table 1: Summary of IT Capex in AA5

($'000)	2021	2022	2023	2024	2025	Total AA5
IT Enabling	1,459	1,259	1,321	547	556	5,142
IT Sustaining Infrastructure	733	1,022	452	687	1,063	3,958
IT Sustaining Applications	1,565	821	415	350	165	3,316
IT Security	384	559	355	221	221	1,740
CRS	603	250	150	1,635	150	2,787
Total IT Capex	**4,744**	**3,911**	**2,693**	**3,440**	**2,155**	**16,943**

The four key areas which will form our DBP IT capex Business Cases for AA5 are:

- **Enabling capex** which is an improvement and uplift to the delivery of DBP IT services, enabling effective and efficient services to the customer and ensuring compliance with regulatory obligations.
- **Sustaining infrastructure capex** which maintains the current levels of DBP IT infrastructure (servers, networks, end user computing devices) and mitigates risks associated with our IT infrastructure through a prudent cycle of system upgrades and replacements.
- **Sustaining applications capex** which maintains the current levels of DBP IT applications and mitigates risks associated with our core business systems through a prudent cycle of system upgrades and replacements.
- **Security capex** which ensures all DBP IT services are delivered safely and securely, are resilient to external threats and comply with our security obligations.

Falling out of our sustaining applications capex is a separate Business Case for CRS which looks to modernise the technology platform to make it mobile and secure support arrangements that will ensure the system remains current and fit-for-purpose.

1.2.2. Opex

Over AA5, we propose total DBP IT opex (which includes hardware consumables, licencing, maintenance and support, our managed support costs, and software licencing, maintenance and support and purchases only) of $29.0 million. This is made up of $20.8 million based on our latest forecast costs, and a predicted $8.2 million step change in our managed support costs.[1]

The MS Dynamics AX project forecast in CY2020 will introduce a step change increase in licences regardless of the final product decision.[2]

[1] Note we are proposing to absorb this in our 2021-2025 opex forecast
[2] Note we are proposing to absorb this in our 2021-2025 opex forecast

The step change in our managed support costs is driven by two ongoing uplifts in 2021 and 2023 related to the new Finance platform due to be implemented in CY2020, Business Intelligence (BI) and Digital Capabilities initiatives delivered in those years, plus natural growth in our digital IT services and therefore support requirements each year.

Our total DBP IT opex is summarised in Table 2 below.

Table 2: Summary of DBP IT Opex in AA5

($'000)	2021	2022	2023	2024	2025	Total AA5
Base year roll forward IT opex	4,167	4,167	4,167	4,167	4,167	20,834
Step change	737	1,040	1,709	2,110	2,551	8,146
Ongoing uplift in managed services costs	*193*	*193*	*472*	*472*	*472*	*1,802*
Natural growth in managed services costs	*543*	*847*	*1,237*	*1,638*	*2,079*	*6,344*
Total DBP IT Opex	**4,904**	**5,207**	**5,876**	**6,277**	**6,718**	**28,982**

1.3. How we have developed our DBP IT Investment Plan

Our DBP IT Investment Plan has been developed using typical elements of a business strategy (outlined in Figure 2), drawn from industry standards, popular strategy frameworks and our investment governance framework. The key elements of this framework include:

- ensuring consistency with the National Gas Rules (NGR);
- alignment with stakeholder expectations and business needs analysis;
- a business-led prioritisation process;
- a robust standardised costing methodology;
- high-level business case outline development with clear links to business strategy and defined benefits aligned to customer expectations and priorities; and
- formal approval and governance oversight.

The first stage diagnosed the current state opportunities and challenges we face, then defining a direction in response to that diagnosis. This is followed by identifying the strategic actions that will move us in that direction, and the investment guardrails that will keep us on the right path as we plan and execute those actions. Figure 2 below shows the key components of our DBP IT Investment Plan.

Figure 2: Key components of the DBP IT Investment Plan

1.4. How we will deliver the DBP IT Investment Plan efficiently

We have robust controls in place to ensure successful delivery of the program of work planned for AA5. The key controls include:

1. executive management support;
2. strict governance processes;
3. a sound project management methodology (PMM) including robust risk analyses which are revisited regularly throughout the life of the project;
4. allocation of capex for a part-time contract Program Manager and opex for organisational change management across the program;
5. internal stakeholder involvement throughout the lifecycle of each project; and
6. partnering and external resourcing arrangements, with demonstrable access to appropriate skills and experience.

2. Current State

As described at 1.3 above, the first stage of developing our DBP IT Investment Plan was consideration of the current state of our technology, applications, key challenges and constraints.

2.1. Technology Profile

To date we have managed our Corporate IT and various Operational Technology (OT) environments separately, only engaging where there are joint requirements or interdependencies. Focus has been on OT, with resourcing and budget constraints restricting investment to those areas which pose a high risk to the delivery of contracted gas to our customers. This has resulted in a reactive, rather than proactive approach to lifecycle management in Corporate IT.

Further resourcing and budget constraints create conflicts between operations and projects as the same resources are responsible for both day-to-day operations and project delivery. This sees operational requirements take precedence over project delivery.

Table 3 below summarises our current Corporate IT technology profile. We have focused on our Operational Technology (OT), (our Corporate IT has only recently grown from 2 to 4FTE) and device and application lifecycle management has been ad-hoc therefore we have a significant amount of catch up required for our Corporate IT.

Table 3: Technology profile

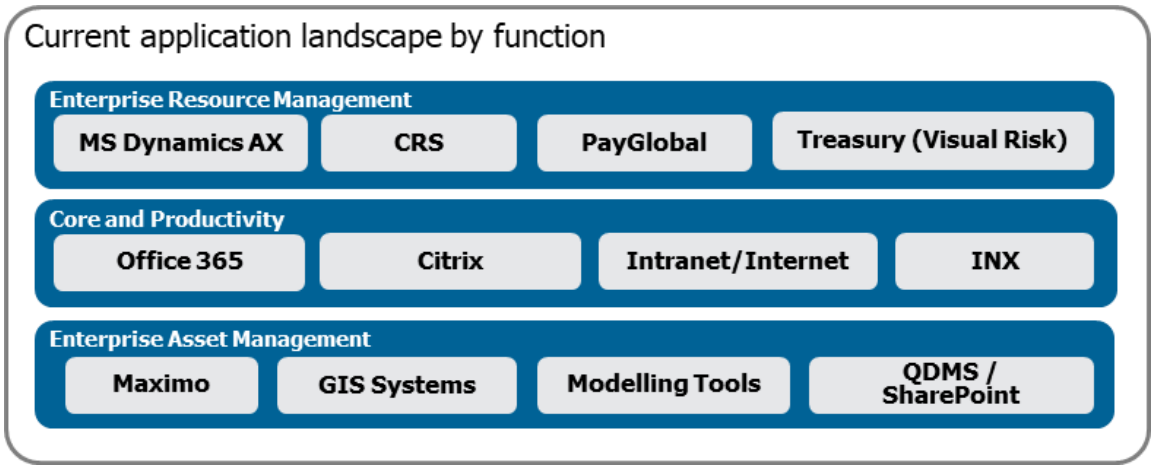
Profile Area	Metrics	Comments
DBP Organisation	227 (FTE 220.3)	
Operational Technology resourcing	5 FTE	Same resources running project and operational
Corporate IT resourcing	4 FTE	Same resources running project and operational
Desktops/Laptops	300	
Servers	68	
Printers	46	
Network / Communications Devices	87	Routers, Switches, WiFi, VC Rooms
DBP owned mobile devices	120	Enrolled devices only

2.2. Application Landscape by Function

Our current application landscape and key sourcing partners is summarised below in Figure 3. While our systems align with current business needs, over the longer term, uncertainties exist around the dependency and supportability of CRS.

In order to maintain the security and integrity of the DBP IT environment and to keep technology risks as low as reasonably practical (ALARP), our application landscape and delivery models require modernisation and ongoing renewal.

Figure 3: Current application landscape by function



2.3. Key Challenges and Constraints

We undertook interviews with key customers and stakeholders, both internal and external, to understand their expectations and analyse business needs.

Key challenges, assertions and pain points relating to the current state of the DBP IT environment include:

- CRS dependency and supportability long term;
- Lost productivity due to manual processing and lack of collaboration;
- Poor accessibility of CRS for staff and customers;
- Pressure to provide high quality services in the most affordable manner;
- Not fully exploiting the organisations existing information;
- Infrastructure to support Operational Technology data Business Intelligence may not meet the increased demand;
- Growing cyber threat to industrial control systems worldwide;
- Convergence of digital and physical assets and IT and industrial systems; and
- Pressure on talent and skills availability and evolution to meet emerging needs.

Key constraints and limitations include:

- Regulatory compliance and increased operating costs e.g. Foreign Investment Review Board (FIRB), Critical Infrastructure Act, National Gas Law (NGL) and NGR regulated by the Economic Regulation Authority (ERA) through Access Arrangements, etc.;
- There are five different IT/OT environments, managed and supported by different teams within DBP and vendors; and
- AGIG group approach to technology has not been finalised but our DBP strategy must ensure alignment.

3. Strategic Direction and Alignment

3.1. Business Context

Our DBP IT Investment Plan focuses on supporting our vision objections of:

- **Customer -** Delivering for Customers
- **Workplace -** A Good Employer
- **Efficiency -** Sustainably Cost Efficient

3.2. Strategic Objectives

The following summarises the DBP IT vision, strategic objectives and focus areas for strategic actions that will help us to successfully execute on this vision, including how information and technology will be used to achieve this.

VISION

To utilise **customer outcome** focused technology to **enable** AGIG to be the leading gas infrastructure business in Australia.

How will we achieve this?

- Partner with the business to understand needs and provide leadership on emerging technologies that enable an integrated digital business.
- Provide technical and operational excellence through a commitment to customer service.

OBJECTIVES

DBP IT's **Strategic Objectives** to support AGIG's Vision of delivering for customers, being a good employer and being sustainably cost efficient:

1. **IT Enabling** – accelerate productivity and asset performance with a connected workforce.
2. **IT Sustaining Infrastructure** – maintain fit-for-purpose technology infrastructure to support users access DBP applications.
3. **IT Sustaining Applications** – maintain fit-for-purpose applications to support users and Shippers to access the organisations information.
4. **IT Security** – secure, resilient and evolving to support AGIG's digital ambitions.

The strategic objectives have been developed with consideration of the current DBP IT environment, constraints, resourcing, strength weakness opportunity and threat (SWOT) assessment and improvement focus areas. Analysis identified foundational requirements for:

- Strong business line of sight across all functions to understand needs (accelerating productivity and asset performance), to enable an integrated digital business, and to adapt quickly to change;
- Increased investment in technology for AA5 to drive cost and productivity savings across frontline functions, whilst maintaining high reliability and service quality levels; and

- Positioning to realise the benefits of convergence of all technology and security, whilst supporting AGIG's digital ambitions.

3.3. Consistency with NGL and NGR

We operate the DBNGP in accordance with the NGL and NGR. The overarching objective of the NGL is set out in the National Gas Objective (NGO). The NGO is to

> *promote efficient investment in, and efficient operation and use of, natural gas services for the long term interests of consumers of natural gas with respect to price, quality, safety, reliability and security of supply.*[3]

Our proposed investment in AA5 is consistent with this objective as it will enable us to prudently maintain and expand our IT systems, infrastructure and processes to ensure the ongoing safety, reliability and security of supply is managed in a cost effective way, in the long-term interests of our customers.

The proposed capex also complies with the new capex criteria in rule 79 of the NGR because it is:

- such as would be incurred by a prudent service provider acting efficiently, in accordance with accepted good industry practice to achieve the lowest sustainable cost of providing services (rule 79(1)(a));
- justifiable under rule 79(2)(a) where there is an overall economic benefit; and
- justifiable under rule 79(2)(c) because it is required to maintain and improve the safety of services, maintain the integrity of services and comply with regulatory obligations and commitments.

Table 4: Consistency of the proposed IT capex with rule 79 of the NGR

#	NGR Criteria	Justification of the proposed expenditure
79(1)	Conforming capital expenditure is capital expenditure that conforms with the following criteria:	
(a)	such as would be incurred by a prudent service provider acting efficiently, in accordance with accepted good industry practice to achieve the lowest sustainable cost of providing services	Proposed capex is: *Prudent* – it is necessary in order to maintain services and comply with regulatory and market obligations and requirements. Further IT Enabling capex will also lead to: • more informed and prudent business decisions, including in asset and workforce management; • seeking out improvements in customer service delivery and customer experience, monitoring the safety and integrity of services and compliance with regulatory obligations; and • likely benefits that exceed the estimated cost of the program.

[3] *National Gas (South Australia) Act 2008*, s23.

#	NGR Criteria	Justification of the proposed expenditure
		Efficient – it will enable us to maintain and improve operational efficiency and address the high risks of non-compliance with Cyber Security obligations and other relevant regulations and legislation, potential customer and business interruptions and corresponding adverse financial and reputation impacts. We will deliver the program using a combination of internal and external resources, in line with our asset management, project governance, procurement and financial governance frameworks to ensure which will ensure efficient cost management. *Consistent with accepted good industry practice* – it will ensure we continue to operate in line with good industry practice in terms of having all critical systems, hardware and software up to date, secure and supported by vendors. It will enable more rapid access to critical information when making decisions, and improve our reporting and analytical capability. It is good practice to continue to develop service levels in line with opportunities from new technology. Further, the relative immaturity of our information management capabilities and cyber security framework highlight the fact we are behind others in our industry and require increased investment to catch up. *Achieves the lowest sustainable cost of delivering pipeline services* – it is necessary to mitigate the risks associated with operating on older versions of systems, hardware and software with the resultant performance, data integrity and cost implications should these systems fail. It will enable more informed decision making throughout the business, including being able to proactively offer new and more flexible services to our customers. It will reduce manual processing and costs, improve accuracy and contribute to developing a consistent culture across our remote workforce. It is therefore consistent with the objective of achieving the lowest sustainable cost of service delivery.
79(2)	Capital expenditure is justifiable if;	
(a)	the overall economic value of the expenditure is positive	IT Enabling capex will implement systems and processes that enable decision making based on more accurate and timely information which will translate into cost efficiencies which outweigh the costs of the capital investment and therefore lead to lower future prices than there otherwise would have been.
(c)	**the capital expenditure is necessary:**	
(i)	to maintain and improve the safety of services	The safety of our services will be adversely affected if any of our critical IT systems fail or if there is a security breach. More extensive access to accurate information about assets and the ability to predict failures will result in a safer network, with opportunities to reduce health and safety risk to both the workforce and to the public.
(ii)	to maintain the integrity of services	The integrity of the services will be adversely affected if any of our critical IT systems are unavailable. Further, more rapid and accurate access to asset information will help us to maintain the integrity of services through improved decision making.

#	NGR Criteria	Justification of the proposed expenditure
(iii)	to comply with a regulatory obligation or requirement	Our regulatory obligations (e.g. Privacy and Critical Infrastructure Act requirements for maintaining reasonable IT security controls commensurate with the cyber risks the organisation faces) will be breached if key systems are not available, compromised or customer data is compromised. Access to more extensive and accurate asset information will decrease the time and effort required to meet regulatory reporting requirements.

3.4. Alignment with stakeholder feedback and strategic objectives

We are committed to actively engaging with our customers and stakeholders to ensure our future plans are consistent with the long-term interests of our customers. To facilitate this, we have implemented a stakeholder engagement program to understand and respond to the priorities of both our internal business stakeholders and external customers and stakeholders.

The consistent feedback from internal business stakeholders was around the frustration associated with efficient information sharing and collaboration. This also extended to the other AGIG business units. There was also a growing recognition that the organisation is not fully utilising the information it currently has, or could be collecting, to make more informed business decisions.

External stakeholders expressed the desire to enable more digital interaction with us with the caveat of not increasing costs. They also said they were interested in greater flexibility and more proactive service offerings. The regulatory environment is also pushing greater accountability on organisations for their cyber security (e.g. Privacy Act, Critical Infrastructure Act and our FIRB conditions).

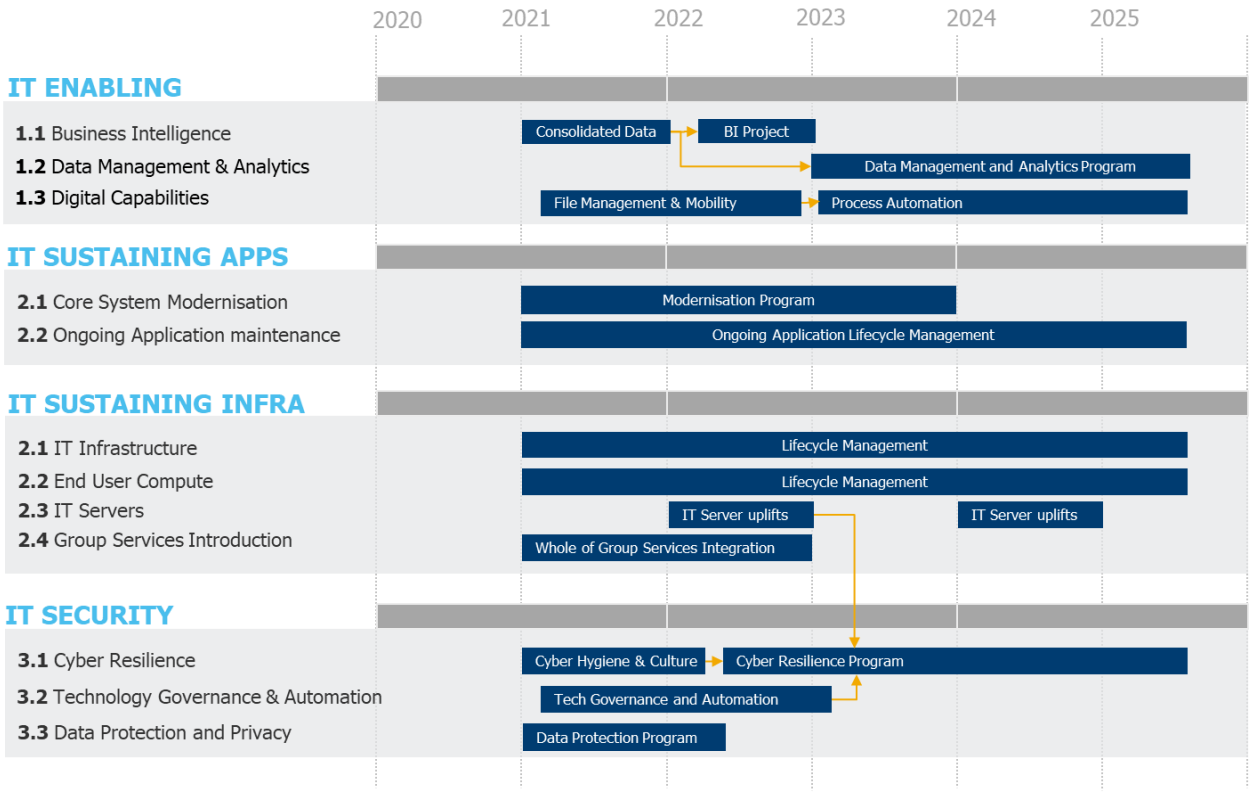
Accordingly, this DBP IT Investment Plan seeks to address a range of known gaps (IT Enabling objective), maintain fit-for-purpose systems (IT Sustaining Infrastructure and IT Sustaining Application objectives) and ensure that cyber security is fit-for-purpose (IT Security objective).

Importantly, we tested our understanding and incorporation of these objectives with management and our shippers who were supportive of the proposed intent, objectives and indicative costs but reserved their opinion pending the business cases that would be provided to support our Final Plan for AA5.

4. Future State Plan for AA5

As shown in Figure 4 below, we have developed a high-level roadmap which identifies the proposed scheduling of initiatives in AA5. The schedule is based on an analysis of initiative dependencies, resourcing, cross AGIG dependencies and business priorities. Each initiative will have a business case that identifies in more detail the interdependencies, business prioritisation and timeframes for management approval.

Figure 4: High-level DBP IT Investment Plan roadmap



The following sections provide an overview of the objectives, scope, and forecast costs and benefits of each of the IT capex programs.

We have used a mix of historic costs, vendor agreements and market pricing to estimate our forecast capex in AA5.

4.1. IT Enabling

IT Enabling is focused on accelerating productivity and asset performance through BI, data management and analytics, and pursuing a connected workforce through digital capabilities. The proposed capex for this program is set out in Table 5 below.

Table 5: Summary of IT Enabling capex ($2020)

$(000's)	2021	2022	2023	2024	2025	Total
Business Intelligence	775	641	398	0	0	**1,814**
Data Management and Analytics	0	0	765	449	458	**1,672**
Digital Capabilities	684	618	158	98	98	**1,656**
Total	**1,459**	**1,259**	**1,321**	**547**	**556**	**5,142**

4.1.1. Business Intelligence (Historical)

This project will centralise the business intelligence strategy to access all required information quickly, reliably and dynamically. It is enabled by strong data management practices. The focus of this project includes:

- Position business intelligence at the centre of digital technology platforms e.g. common data lake to consolidate disparate data sources and business intelligence toolsets for data driven decision making.
- Maintain effective data management and governance practices to support analytics value and data quality.
- Drive integration of operational data from (or about) assets with commercial data to improve decision-making intelligence, dashboards and reporting systems.

4.1.2. Data Management and Analytics (Predictive)

This project will align IT strategy, infrastructure planning and operating models toward predictive asset performance and enhancement. The focus of this project includes:

- Develop strong culture of data management to capture and store all business knowledge consistently and accurately.
- Develop data analytics capabilities (predictive), enabled by connected field assets e.g. Internet of Things, business intelligence capabilities and advanced analytics models e.g. for asset condition, asset optimisation and accurate asset management planning etc.
- Develop practical Artificial intelligence (AI) use cases, prototype and experiment to enhance predictive models.

4.1.3. Digital Capabilities

This project will create a workplace that can evolve quickly, with lower cost of change, automating processes and connecting with other digitally enabled organisations safely. The focus of this project includes:

Connected and Agile

- Process Automation - Continue to digitise manual practices and automate routine processes and inefficient work practices.

- Leverage new digital connectivity platforms and sourcing models.

Workforce Mobility and Productivity

- Create a workplace that can evolve quickly by moving key infrastructure to the cloud, mitigating the restrictions of legacy apps and adopting agile endpoint operations.

4.2. IT Sustaining Infrastructure

IT Sustaining Infrastructure is focused on maintaining high reliability and service quality levels. The program ensures systems are kept up to date enabling us to maintain reliable, compliant and efficient business processes and systems, preserving the ongoing integrity of our services. The proposed capex for this strategy is set out in Table 6 below.

Table 6: Summary of IT Sustaining Infrastructure capex

($'000)	2021	2022	2023	2024	2025	Total
IT Asset Renewal (Lifecycle Management)	52	0	25	0	635	**712**
IT Asset Renewal (End-User Compute)	427	427	427	427	427	**2,137**
IT Asset Renewal (Virtual Servers)	0	260	0	260	0	**520**
Group Services Introduction Program	254	335	0	0	0	**589**
Total	**733**	**1,022**	**452**	**687**	**1,063**	**3,957**

4.2.1. IT Asset Renewal (Lifecycle Management)

This initiative involves the ongoing replacement of IT infrastructure assets as per the asset management schedule (e.g. switches, routers, ISP connections, Wi-Fi network, telephony and meeting room technologies).

4.2.2. IT Asset Renewal (End User Compute)

This initiative involves continuing refresh of end-user computing devices that are reaching end-of-life and update/upgrade associated operating system and end user client software (e.g. laptops, tablets, desktops).

4.2.3. IT Asset Renewal (Virtual Servers)

This initiative involves continuing refresh the virtual IT infrastructure and associated operating software (e.g. servers).

4.2.4. Group Services Introduction Program

This initiative positions us to realise greater integration of AGIG group-wide services potentially enabling whole-of-group services to be introduced realising economies of scale.

4.3. IT Sustaining Applications

IT Sustaining Applications is focused on maintaining high reliability and service quality levels. The program ensures systems are kept up to date enabling us to maintain reliable, compliant and efficient business processes and systems, preserving the ongoing integrity of our services. The proposed capex for this strategy is set out in Table 7 below.

Table 7: Summary of IT Sustaining Applications capex ($2020)

($'000)	2021	2022	2023	2024	2025	Total
Core System Modernisation	1,287	601	250	250	0	2,388
Ongoing Application Maintenance	278	220	165	100	165	928
Total	**1,565**	**821**	**415**	**350**	**165**	**3,316**

4.3.1. Core System Modernisation

Ongoing System and Software Renewal programs are required to maintain the security and integrity of the IT environment and to keep technology risks at an acceptable level. The focus of this project includes:

- Create a platform-independent environment by modernising relevant applications to enable a mobile workforce e.g. responsive design, mobile, software as a service (SaaS) and virtualisation.
- CRS, Maximo, MS Dynamics AX modernisation.
- Optimise core capabilities leveraging new platforms and sourcing models.
- New technologies to advance the cyber security capabilities.

4.3.2. Ongoing Application Maintenance

Ongoing Application Maintenance initiatives are required to maintain core IT applications that are current, fit for purpose and to versions in line with an industry standard approach to maintain the integrity of the overall IT environment, manage technology risks and prevent material outages that impact the ability of the business to function.

4.4. IT Security

IT Security is focused on being secure, resilient and evolving to support our digital ambitions. The proposed capex for this strategy is set out in Table 8 below.

Table 8: Summary of IT Security capex

($'000')	2021	2022	2023	2024	2025	Total
Cyber Resilience	170	313	322	221	221	**1,247**
Technology Governance and Automation	32	64	33	0	0	**129**
Data Protection and Privacy	182	182	0	0	0	**364**
Total	**384**	**559**	**355**	**221**	**221**	**1,740**

4.4.1. Cyber Resilience

This project will build upon sound security policies and systems base to increase cyber resilience and foster a strong cyber culture. The focus of this project includes:

- Develop a secure software development life cycle approach that builds security in by design
- Continuing cyber security culture improvements
- Proactive third-party cyber risk improvements e.g. due diligence and monitoring
- Extend disaster recovery strategy to consider business processes not just components
- Threat intelligence capabilities and cyber incident response framework, processes and exercising.

4.4.2. Technology Governance and Automation

This project will evolve DBP IT's operating model to support intensifying digital ambitions and growing edge-to-enterprise connectivity. The focus of this project includes:

- Evolve DBP IT's operating model with clear definition of digital responsibilities and then aligning IT strategy with operating model redesign.
- Develop a shared technology architecture so the enterprise can start to consolidate the separate IT and OT architectures.
- Improve cyber security capabilities across industrial controls systems e.g. hardening, education, change management, patching, monitoring and incident response.

4.4.3. Data Protection and Privacy

This project will ensure obligations are met for protecting data and ensuring data privacy, earning the trust of customers, users, partners and employees. The focus of this project includes:

- Meet legal and regulatory obligations, including under the Critical Infrastructure Act and FIRB conditions.
- Maintain a risk assessed inventory of all sensitive and personally identifiable information stored, processed, or transmitted by technology systems, including those located onsite or at remote service providers.

- Implement data protection controls to prevent exfiltration and/or privacy data breaches e.g. data loss prevention, cloud access security broker, data breach response plans, etc.

4.5. CRS

This project will modernise the CRS technology platform to allow employees and customers to access CRS on mobile devices and provide enhanced support arrangements to ensure new business requirements can be met in a timely manner without the need for manual workarounds. The proposed expenditure to deliver the CRS project is provided in Table 9.

Table 9: Summary of CRS capex

($'000)	2021	2022	2023	2024	2025	AA5
CRS platform improvements	603	250	150	1,635	150	2,787
Total	**603**	**250**	**150**	**1,635**	**150**	**2,787**

4.6. Over the Horizon

This section outlines stretch possibilities to extend foundational strategies for how the business will compete and succeed in the long term to achieve business success. The projects are unplanned, unfunded and have been identified for future consideration only.

4.6.1. Digital Twins and Machine Learning

This project will turbocharge innovation and continuous intelligence. The focus of this project includes:

Intelligent Simulation

- Creating or acquiring reliable digital twin models for key operating assets, prioritising decoupling systems from their physical assets.
- Assess sourcing options – i.e. create own vs purchase from the asset manufacturer.
- Enable testing of "what if" scenarios in a fast, safe and inexpensive virtual environment.

Machine Learning

- Expand artificial intelligence (AI) prototypes, partnering with data science resources to build machine learning (ML) capabilities.

4.6.2. Robotic Process Automation

This project will turbocharge innovation and automation. The focus of this project includes:

Robotic Process Automation

- Develop and implement practical use cases for robotic process automation (RPA) – including supporting governance and standards. Currently in use at scale by companies including Woodside, Fortescue Metals Group, Royal Automobile Club, etc. in WA.

4.7. Benefits

Table 10 below provides a summary of the key benefits associated with the proposed IT initiatives. These have been analysed further, and quantified where possible, in the detailed business cases which have been developed for each IT initiative.

Table 10: Summary of benefits

IT Initiative	Key Benefits
Business Intelligence	• Enabling management to make more timely, informed, data based decisions ultimately leading to operating efficiency, improved customer service and safety. • Providing a control against the risk of an aging workforce by systemisation of how business decisions are made. • Accelerate productivity and improving management decisions by identifying trends and correlations that humans would not see. • Improved compliance with the risk based approach to managing and operating assets. • Improved ability to predict asset failures due to enhanced capability for informed decision making in relation to the network asset lifecycle processes. • Reduced risk of non-compliance with regulatory reporting requirements because of improved data quality and integrity. • Takes advantage of the increasing volumes of data being captured in disparate systems as well as deliver constantly changing reporting requirements to key stakeholders. • Will help to maintain and improve the safety of services as it will provide more extensive access to accurate information about assets and the ability to predict failures will result in a safer network.
Data Management and Analytics	• Improved asset management decisions as a result of more reliable, data driven information and options. • Extending analytics out to the supply chain will continue to drive smarter asset planning, maintenance and ongoing asset viability. • Providing a control against the risk of an aging workforce by systemisation of how business decisions are made. • Improved ability to predict asset failures due to enhanced capability for informed decision making in relation to the network asset lifecycle processes. • Reduced risk of non-compliance with regulatory reporting requirements because of improved timeliness, data quality and integrity.
Digital Capabilities	• Continued digitisation of manual practices and automation of routine processes will lead to workforce efficiencies and a reduction in manual errors. • An enabled workforce that can collaborate effectively and efficiently will improve workforce capacity and lead to more informed management decisions.

IT Initiative	Key Benefits
Core System Modernisation	• Ensuring that the core systems the organisation is critically dependent on remain fit-for-purpose, supportable and secure so that the business does not have to undertake an unscheduled core system replacement. • Enabling new system functionality that provides stakeholders with improved capabilities, ongoing support of business processes and more efficient use of the system. • Enabling the retirement of legacy infrastructure and systems to enhance the IT security and reduce ongoing IT operating costs and operational maintenance issues. • Providing systems with increased IT Security capabilities to manage the ever changing IT security threats. • Ensures validity of support requirements with technology vendors. • Enables compliance of core systems with market requirements. • Manages alignment with other co-existing applications and infrastructure. • Maintaining a predictable cost profile for information technology systems. • Provide a modern digital customer experience resulting in improved customer service for bookings, billing, reporting and queries.
Asset Renewal	• A stable technology platform to ensure the right people have access to the right information at the right time. • Fit-for-purpose systems to ensure that 'technology frustration' does not reduce operational efficiencies or introduce asset, security of safety risks. • Reduces exposure to system and security related vulnerabilities and unplanned outages from the failure of critical infrastructure; • Reduces the risk of non-compliance with Retail Market Procedures and other legal and regulatory obligations; • Enables compliance of the IT systems and infrastructure with market requirements. • Maintaining a predictable cost profile for information technology systems.
Group Services Introduction Program	• An enabled workforce across the AGIG Group that can collaborate effectively and efficiently will improve workforce capacity and lead to more informed management decisions. • A more secure but useable information environment leading to operational efficiencies and more timely information for management decisions.
Cyber Resilience	• A fit-for-purpose IT Security approach, systems and culture that balances preparation, detection and the ability to respond to any IT security incident ensuring that the organisation has done as much as is reasonable but can also respond appropriately. • A cyber culture that is owned and driven by the users which will result in cyber controls that enable secure business processes rather than being barriers to efficiency. • Will work to address the low benchmark comparison scores for IT security comparative to the utilities industry.
Technology Governance and Automation	• The technology environment that will be necessary to enable the Business Intelligence and Data Management and Analytics initiatives. • Improved and uniform cyber capabilities across both the IT and OT environments.

IT Initiative	Key Benefits
Data Protection and Privacy	• Ensuring the organisation meets its ongoing privacy obligations. • Ensuring the organisation meets its regulatory obligations and operational needs to protect the sensitive and critical information it holds and uses. • Will work to address the low benchmark comparison scores for IT security comparative to the utilities industry.

4.8. Driver Mapping

The IT investment initiatives align to capex criteria rule 79 of the NGR and our vision objectives as per Table 11.

Table 11: Aligning initiatives to the NGR and digital strategy objectives

IT Investment Objectives	Key Area	IT Initiative	Customer	Workplace	Efficiency
Maintain the current levels of IT services	IT Sustaining	Core System Modernisation	✓	✓	✓
	IT Sustaining	Asset Renewal	✓		✓
	IT Sustaining	Group Services Introduction Program		✓	✓
	IT Security	Cyber Resilience		✓	✓
	IT Security	Technology Governance and Automation		✓	✓
Enable effective & efficient delivery of services to the customer	IT Enabling	Business Intelligence	✓	✓	✓
	IT Enabling	Data Management and Analytics	✓		✓
	IT Enabling	Digital Capabilities	✓	✓	✓
	IT Security	Data Protection and Privacy		✓	✓
	All	Program and Change Management		✓	

5. IT Benchmark Analysis

Our DBP IT Investment Plan has been developed to ensure that DBP IT will support our vision objectives. We have also had regard to accepted good industry practice in terms of activities, lifecycle management and levels of investment.

Table 12 below summarises the benchmarking indicator comparison we undertook in 2018 as we started to develop this strategy. We consider our AA5 investment plan and the initiatives within it will bring us more in line with organisations in similar industries.

Table 12: IT Benchmark comparison to organisations in similar industries

Benchmark	Utilities Industry averages	Our Value CY18	Indicator
IT Spending – Utilities Industry (% of Total Revenue $381m)	3.2% - 3.5%	1.82%	
IT Spending – Utilities Industry (% of Operating Expenses $92.9m)	4.0% - 4.6%	4.7%	
IT CAPEX Distribution (Sustain vs Enable)	70% sustaining 30% enabling	99% sustaining 1% enabling	
CAPEX vs OPEX Distribution	28%:72%	21% : 79%	
IT Spending per Employee – Utilities Industry	$26,592	$23,448.28	
IT FTE's as a % of Employees – Utilities Industry	7.3%	1.8% (IT) 2.2% (OT)	
IT Security Spending as % Total IT Spending - Energy	5% - 6%	18.9%	
IT Security FTEs as a % of Total FTEs - Industrial	6.1%	0.33%	

Notes:

- Indicators of inadequate staffing levels or sourcing model imbalance with low IT support and IT intensity from a human capital perspective.
- Very low levels of enabling capital allocated to transformative projects as opposed to 'keeping the lights on'
- High ratio of IT security vs IT spend was caused by several large IT Security CAPEX projects.
- Under investment in technology and IT security compared to the utilities industry.

Sources:

- Gartner IT Key Metrics Data 2018 (G00341718)
- Gartner IT Key Metrics Data 2019: Key IT Security Measures: by Industry (G00375661)

Key:

Above the average for similar organisations

On par with the average for similar organisations

Below the average for similar organisations