5.19

ICT project justifications (excluding ADMS)

Ausgrid

Content

1 PROGRAM 1 – REGULATORY AND COMPLIANCE SYSTEMS

1.1 Program description

The Regulatory and Compliance Systems Program consists of two major streams:

1. Market and Enterprise systems
2. Technology licence growth.

In the 2019-24 regulatory period our regulatory obligations with respect to the maintenance and licensing of critical infrastructure systems will remain steady. The forecast value of this program during the next regulatory period is $6.0 million ($, FY19).

1.2 Customer outcomes

This program is required so that we can continue to provide safe and reliable services to our customers. The implementation of this program will ensure that our systems remain compliant and meet our regulatory obligations. The result of not implementing this program may directly impact:

- Disconnect and reconnection of customers supply
- Collection of customer consumption data necessary for retail billing
- Information held by Ausgrid about a customer's metering installation compliance to employment regulations for payroll
- Compliance for financial and tax reporting
- Update and storage of critical information such as life support customer data and reading of meters including move in / move out readings
- Authorisation to operate as a DNSP due to breach of licence conditions.

More specifically, if we do not perform this program the data stored about our customers will lose currency. This can disrupt the timely disconnection or reconnection of customers, lead to incorrect billing, and may have an impact on customers wishing to transition to an advanced metering installation managed by retailers.

The health and safety of life support customers would also be placed at risk if this program does not go ahead. This is if a customer registers as a life support customer but our systems are not updated to reflect this change in status, potentially exposing them to an unplanned interruption without the minimum notice period required under the National Energy Customer Framework (NECF).

1.3 Stream 1 - Market and Enterprise systems background

We are subject to multiple regulatory obligations to create, collect and store data.

These obligations stem from our role as the operator of critical infrastructure which provides an essential service to more than 1.7 million customers. We are also subject to more general regulatory obligations as an employer and an incorporated entity.

1.3.1 Consumption and pricing data

Ausgrid is subject to the following regulatory obligations under the National Energy Retail Rules (NERR) with respect to the collection and storage of customer data:

- **Section 86: Provision of information -** A distributor must, on request by a customer or a customer's retailer, provide information about the customer's energy consumption or the distributor's charges.
- **Section 171: Distributor obligations –** electricity consumption information - Distributors must, for the purpose of the electricity consumption benchmarks, provide information to the AER in such a manner and form as may be requested by the AER.

Developments in regulatory/compliance obligations

The AEMC's Distribution Network Pricing Arrangements rule change is set to expand our existing regulatory obligations relating to the collection and storage of customer data.

Under this rule change, Ausgrid is required to introduce more efficient network tariffs. To limit the impact on customers and to accommodate existing technology constraints, this will be an iterative process – with the tariffs we introduce in later regulatory periods likely to be more efficient than those in 2014-19 and 2019-24.

This regulatory change will require us to expand the capabilities of our market enterprise systems. Greater efficiency in our network tariffs will lead to a corresponding increase in the complexity of our customer's consumption and pricing data. In the absence of expanding the capabilities of our current systems, Ausgrid would risk breaching our regulatory obligations to collect and store this data in accordance with section 86 and 171 of the NERR.

1.3.2 Critical Infrastructure Licence Conditions

In accordance with clause 9.2(a) of our Critical Infrastructure Licence Conditions, Ausgrid is required to put in place market and enterprise systems which are consistent with the following:

> [Ausgrid] must, by using **best industry practice** for electricity network control systems, ensure that operation and control of its distribution system, including **all associated ICT infrastructure, can be accessed, operated and controlled only from within Australia**, and that its distribution is not connected to any other infrastructure or network which could enable it to be controlled or operated by persons outside Australia (emphasis added).

Developments in regulatory/compliance obligations

Our data collection and storage obligations under clause 9.2(a) of our Critical Infrastructure Licence Conditions are not static. They require us to use 'best industry practice' to ensure 'all associated ICT infrastructure can be accessed, operated and controlled only from within Australia'. This is an evolving benchmark which will require Ausgrid to expand existing market and enterprise systems in the 2019-24 regulatory period. This is to bring them into line with developments in technology and data management practices which equate with 'best industry practice'.

1.3.3 Metrology procedures

We own and operate a population of more than 2 million type 5 and 6 meters.

In accordance with metrology procedures administered by AEMO, we are required to periodically perform in-service accuracy testing of our meters. The details and auditable history of tests must be recorded in our data systems.

Developments in regulatory/compliance obligations

The AEMC's Expansion of Contestability in Metering Related Services rule change will provide our customers with more choice in the metering service they utilise.

We expect that up to half our existing customers may take advantage of this rule change in the 2019-24 regulatory period. This is by leaving our type 5 and 6 metering service in favour of a retail offering inclusive of an advanced meter.

With such a large volume of customers set to leave our metering service, there will be increased complexity in how we handle data relating to the accuracy of the meters we have installed. This creates a need to invest in better systems, as issues arise in the 2019-24 regulatory period.

1.3.4 Other regulatory obligations

We are required as an incorporated entity to put in place systems which hold data on the leave and remuneration entitlements of the 3000+ permanent staff Ausgrid employs.

Developments in regulatory/compliance obligations

We currently have a payroll system (“CHRIS21”) in place for managing our regulatory obligations with respect to employee leave and remuneration entitlements.

CHRIS21 was developed by a software company. To ensure we comply with annual ATO Tax Rate changes, there is a need to acquire a software update and patches including performance of regression testing from that company each year.

1.3.5 Need

We anticipate our regulatory obligations in terms of the creation, collection and storage of data to expand in the 2019-24 regulatory control period. These expanded obligations – which give rise to a corresponding need to expand the ICT capabilities of our existing market and enterprise systems – are summarised in Table 1.

Table 1. Summary of expanding obligations leading to the need for investment

Obligation	Existing obligations	Developments expanding existing obligations in 2019-24
Customer data	Provision of consumption data and network tariff information in accordance with sections 86 and 171 of NERR as outlined above	Commencement of AEMC’s Distribution Network Pricing Arrangements
Critical Infrastructure Licence Conditions	Audit conditions outlined above	Responding to developments in the ‘best industry practice’ benchmark for the protection of data from overseas access
Metrology procedures	Metrology procedures outlined above	Power of Choice metering reforms
Other regulatory obligations	Hold data on leave and remuneration as outlined above	Annual updates to existing systems in line with ATO tax rate changes

1.3.6 Options

Our assessment of the available options, together with an overview of what would be involved, is set out in Table 2.

Table 2. Options analysis

Program needs options	What’s involved	Assessment
1 Do nothing	Ausgrid would continue to operate our existing market enterprise systems	New developments in our regulatory obligations would not be met.

Program needs options	What's involved	Assessment
2 ICT extension ('market and enterprise system program')	The capabilities of our existing market and enterprise systems would be expanded	New developments in our regulatory and compliance obligations would be met, facilitating compliance with: section 86 and 171 of the NERR clause 9.2(a) of our Critical Infrastructure Licence Conditions AEMO metrology procedures ATO Tax Rate changes

1.3.7 Preferred option

We have selected Option 2 (implementation of market and enterprise system program) as our preferred option. It is required to meet new developments in Ausgrid's regulatory obligations, as listed in Table 1.

1.4 Stream 2 - Technology licence growth description

Ausgrid utilises a number of commercial software applications from third party vendors. Licensing for these applications is based on either the number of:

- Connections (or associated meters)
- Measurement points on the Ausgrid Network.

To ensure continued compliance with contractual software licensing agreements, it will be necessary to invest in additional licences to keep pace with predicted growth in the number of network connections and measurement points on our network during the 2019-24 regulatory period.

1.4.1 Technology licence growth background

We utilise the following software applications in the delivery of direct control services:

SAP IS-U/CCS

SAP IS-U/CCS is used to manage customer, account, tariff and billing information. It supports key business processes including network customer connections, revenue management, AEMO market interaction (customer transfers, business to business transactions, etc.) and holds key customer and site information, including supply guarantee (life support) information, which are integral to Ausgrid's compliance with market rules and NECF obligations.

Oracle Outage Management System

The Oracle Outage Management System (OMS), is used to record and track unplanned network outages based on information obtained from customer interactions or directly from Ausgrid's Distribution Network Management System (DNMS – SCADA).

GE Smallworld

The GE Smallworld is Ausgrid's solution for recording geospatial information (GIS) about Ausgrid's network assets and is used to record the electrical network connectivity model. The system supports a broad range of Ausgrid engineering and field based functions that require information about the location of assets (particularly underground) to plan and safely execute maintenance, construction projects and augmentation of the network.

This application enables our "Dial Before You Dig services" and hence key to public safety. It also holds connection information down to the individual customer's national metering identifier (NMI) which is used by Network operations teams to organise planned outages and identify customers to be notified (a NECF obligation).

PI Historian

PI historian provides key real time and historical information on operating conditions in the Ausgrid electrical network, which support network operations, engineering design and investment decision

1.4.2 Need

Ausgrid anticipates steady growth in network connections over the 2019-24 regulatory control period. Table 3 sets out our anticipated growth in NMIs.

Table 3. Growth in connections per NMI

	2019	2020	2021	2022	2023	2024
# of NMIs	1,657,621	1,675,059	1,694,628	1,716,335	1,738,520	1,759,322
NMI growth	n/a	17,438	19,569	21,707	22,185	20,802

The growth in NMIs presents a need to invest in additional licences for our GIS, OMS and SAP CSS software applications. Table 4 sets out this need in the 2019-24 regulatory control period and its timing in line with our expected NMI growth.

Table 4. Additional licence needs for GIS, OMS and SAP CCS

Current Licence (customers /connection points)		Current usage (NMIs)	Additional Licence Requirements				
			2020	2021	2022	2023	2024
GIS	1,700,000	1,657,621	-	-	100,000	-	-
OMS	1,700,000	1,657,621	-	-	60,000	-	-
SAP CCS	1,629,000	1,657,621	100,000	-	-	100,000	-

PI historian licence is based on the number of ‘PI tags’ deployed on our network. Growth in these tags is driven by SCADA growth as a result of new substation commissioning, substation replacements, SCADA remote terminal unit (RTU) refits, and recloser rollouts.

Table 5 sets out our anticipated growth in PI Tags as a result of these drivers. 0 shows the additional licences needed in response to this expected growth in the 2019-24 regulatory control period.

Table 5. Growth in PI Tags

	Current	2019	2020	2021	2022	2023	2024
SCADA Growth	150,000	173,000	199,000	229,000	263,000	302,000	347,000
Other Growth	8,000	9,200	10,600	12,200	14,000	16,100	18,500
DM&C Tags	426,000	612,500	799,500	899,000	999,000	1,099,000	1,099,000
Total Growth	**584,000**	**794,700**	**1,008,600**	**1,140,200**	**1,276,000**	**1,417,100**	**1,464,500**

Table 6. Additional licences need in response to PI Tag growth

Current Licences (tags)		Current usage (tags)	Additional Licence Requirements				
			2020	2021	2022	2023	2024
PI Historian	1,100,000	794,700	-	400,000	-	-	-

1.4.3 Options

Our assessment of the available options is set out in Table 7.

Table 7. Options analysis

Program needs options	What's involved	Assessment
1 Do nothing	Ausgrid would not renew licences	Ausgrid would be in breach of licence conditions for CSS, OMS, GIS and PI historian
2 Licence renewal	Licences would be renewed in line with growth in NMIs and measure points	Ausgrid would maintain licence compliance throughout the 2019-24 regulatory period

1.4.4 Preferred option

We are required to implement Option 2 (licence renewal) to maintain our licence compliance throughout the 2019-24 regulatory period. This option has therefore been selected.

2 PROGRAM 2 – CYBER SECURITY

2.1 Program description

We have a planned program to sustain the capabilities of our existing ICT infrastructure to reduce the risk of our critical systems being impacted by cyber-attacks, virtual or physical, in response to recent global security events and continued compliance with licence conditions.

In the 2019-24 regulatory period, we forecast that the cost of this ICT expansion program will be $19.9 million ($, real FY19).

2.2 Customer outcomes

The implementation of this program will minimise the risk of cyber-attacks, virtual or physical and maintain compliance with our DNSP licence conditions. This program will protect our people, customers and assets from cyber threats.

Stronger cyber security will also benefit our customers by preventing intrusions into our ICT infrastructure targeted at causing service interruptions. If we do not undertake this program we are at a high risk of impacts from cyber threats which could expose critical information about our supply of electricity and release personal customer information. Cyber attacks are also likely to lead to service interruptions to Sydney's CBD, defence, industry and customers. Loss of economic activity and social disruption are other potential outcomes for customers if Ausgrid does not take prudent steps to avoid cyber security intrusions

Additionally the program will assure that we remain compliant with our licence conditions enabling us to supply electricity.

2.3 Background

Cyber crime and attacks are a very real threat in the world we live in today. Ausgrid operates critical infrastructure in a high and increasing threat environment. We support 20% of the nation's GDP and 40% of the NSW population. There are rapid changes occurring in global markets making us an attractive target Ausgrid is an attractive target for cyber-attack due to our operation of critical infrastructure which, if disrupted for prolonged periods, could cause severe damage to communities, businesses and potentially Australia's national security.

We continually monitor the capabilities of our ICT infrastructure to defend and counteract cyber security attacks. This is for compliance with our regulatory obligations and Ausgrid's evolving needs in terms of the increasing level of sophistication associated with these types of threats.

2.3.1 Regulatory obligations

We are subject to regulatory obligations to manage threats to Ausgrid's cyber security.

Clause 9.2(a) of our Critical Infrastructure Licence Conditions (CILC) requires us to utilise 'best industry practice for electricity control systems [to] ensure that operation and control of [Ausgrid's] ICT infrastructure can be accessed, operated and controlled only within Australia (emphasis added)'. This is supplemented by clause 9.3(b) which specifically requires us to develop and implement strategies to 'manage cyber security and other threats affecting the network operational technology environment'.

Clause 10 of our CILC addresses data security. It provides that Ausgrid must 'ensure that all of its information (being design specifications, operating manuals and the like) as to the operational technology (such as the SCADA system) and associated ICT infrastructure… is solely held within Australia'.

Our compliance with these regulatory obligations is audited by IPART each year.

2.3.2 Evolving cyber security needs

We need to respond to our evolving cyber security needs in the 2019-24 period.

Increasing sophistication

Our cyber security needs are continually evolving as threats increase in sophistication.

Like many organisations, Ausgrid has been able to protect its ICT infrastructure by blocking threats at the perimeter using 'firewalls'. With cyber security attacks becoming increasingly more sophisticated, we are required to refocus our attention beyond these perimeter defences and prepare for a situation in which an intrusion is successful.

To do this, Ausgrid will need to expand the capabilities to embed cyber security into our people culture, strengthen key controls relating to critical systems and assets, and develop a sophisticated cyber threat management capability providing greater agility in responding to cyber threats and predicting possible threats. In the 2019-24 regulatory period, this will be an ongoing process with continual requirements to expand our ICT capabilities in response to evolving levels in the complexity of threats to our cyber security.

Internet connectivity

Advancements in technology has led to our network increasingly enter the 'digital age'.

We have over 6,000 modems installed in distribution substations and field devices. These modems are needed to send and receive information about the health of our network, and to allow Ausgrid to manage and respond to faults.

The emergence of such internet connectivity allows to Ausgrid improve the safety, reliability and the resiliency of our assets. But as with anything connected to the internet, there are risks of cyber-attack.

2.3.3 Consequences

In its February 2017 discussion paper Strengthening the National Security of Australia's Critical Infrastructure the Commonwealth government identified the following consequences of an operator of critical infrastructure failing to manage its cyber security risks:

- Espionage: attacks that target Ausgrid's ICT infrastructure for the collection of information about our customers – including large corporations and government organisations – which is not publicly available.
- Sabotage: attacks that target Ausgrid's ICT infrastructure to cause deliberate interruption or destruction to our operations that lead to economic damage.
- Coercion: attacks that target Ausgrid ICT infrastructure to apply coercive power against Ausgrid or to influence decision-making or policy of Australian governments.

2.3.4 Our current position

We have conducted a cyber security maturity assessment which evaluated our cyber security and resilience controls, existing mitigation strategies and produced a tangible costed and executable roadmap of cyber improvement activities including ongoing continuous improvement. The assessment evaluated control maturity using the US Department of Energy developed, Cybersecurity Capability Maturity Model (C2M2) framework. This identified that we are displaying a low maturity on this measure compared to our industry peers.

The review concluded that Ausgrid operates in a high threat environment being an attractive target for “Nation State” adversaries seeking to cause widespread impact to the Australian economy and as a result necessitates a “Low” risk appetite.

This demonstrates that Ausgrid requires increased spending not just to meet existing regulatory compliance obligations, but to catch-up with the current benchmarks for cyber security protection.

The resulting three year program of work will significantly reduce the risk profile for Ausgrid within the first year, set a foundation for future cyber investments, and move toward industry best practice cyber security and resilience at Ausgrid. In addition, our technologies, systems and telecommunication networks have been subject to, and will continue to be subject to cyberattacks, computer viruses, malicious code, phishing attacks or information security breaches that could result in the unauthorized release, gathering, monitoring, misuse, loss or destruction of confidential, proprietary and other information of us and of our suppliers, employees or customers, or otherwise disrupt customers’ or other third parties’ business operations. Although to date we have not experienced any material losses relating to cyberattacks or other information security breaches, there can be no assurance that we will not suffer such losses in the future and so we have included funding to continually maintain the cyber program after the initial three year program is complete (Dec 2020).

Ausgrid further engaged an industry expert (Hakluyt) to assist Ausgrid with a strategic review of its cyber security strategy and program. The review found the Ausgrid cyber security strategy and program as “sound” and identified a number of recommendations incorporated into the Ausgrid cyber security strategy and program.

In addition, the Ausgrid cyber security strategy and program has been reviewed and endorsed by the Critical Infrastructure Centre and Australian Signals Directorate (ASD) within Federal Government.

2.4 Need

We will need to expand our ICT capabilities in the 2019-24 regulatory period to maintain compliance with our regulatory obligations relating to cyber security threats. The drivers behind this need are summarised in Table 8 below.

Table 8. Summary of cyber security needs in the 2019-24 period

Need	Overview
Regulatory obligations	ICT expansion programs is needed to maintain compliance with Critical Infrastructure Licence Conditions
Evolving cyber security needs	Increasing sophistication in cyber security attacks and the connection of our assets to the internet present cyber security risks which are in need of mitigation by expanding the capabilities of existing ICT infrastructure
Consequences	The consequences of a cyber security attack are severe. The Commonwealth government has recognised that they include espionage, sabotage and coercion. To avoid these severe consequences, we need to expand our ICT capabilities as cyber security threats become more sophisticated.
Current position	We are not spending enough on cyber security relative to other businesses in our industry

2.5 Options

In Table 9 below, we consider each of the available options we have in response to our increasing cyber security threats. Our preferred option is selected in the next section.

Table 9. Options analysis

Program needs options	What's involved	Assessment
1 Do nothing	We would rely on our existing capabilities to defend and counteract cyber security threats	Ausgrid would be vulnerable to increasingly sophisticated cyber security threats. This could lead to a breach of our ICT infrastructure which leads to severe disruption to communities, businesses, and potentially Australia's national security.
2 ICT extension ('cyber security')	Our existing ICT capabilities would be expanded in line with the increasing sophistication of cyber security threats.	The risk of a serious breach of our ICT infrastructure would be mitigated. Our cyber security protections would be expanded in capabilities to a level which meets the increasing sophistication of intruders. We would also catch-up on historical under-investment in our cyber security protections and be in a position where Ausgrid would be able to continue to meet our regulatory obligations.

2.6 Preferred option

We are required to strengthen our existing ICT defences against cyber security threats. This is in response to the increasing level of sophistication of these threats and to maintain our compliance with our regulatory obligations. Option 2, an ICT extension program targeted at strengthening our cyber security protections, has therefore been selected as our preferred option for the 2019-24 period.

3 PROGRAM 3 – APPLICATION MAINTENANCE

3.1 Program description

Ausgrid's business processes are supported by 104 critical systems, of which thirty are mission critical and seventy four are business critical. IT applications have an expected useful life of between four and seven years, meaning that there will be a need to 'refresh' systems every one to two regulatory periods so that systems remain supportable and continue to underpin the processes supporting the Ausgrid business. This is in line with accepted industry practice and is necessary so that Ausgrid can operate the network in a manner consistent with the NER and be able to meet those licence requirements and corporate obligations in the most efficient way. Retaining systems without upgrading or replacing beyond this point will result in additional maintenance costs and reliability risks, impacting on efficiency and resilience.

The Application maintenance program consists of these major streams.

- End of Life Application Upgrades
- Mandatory patch and release management
- SAP core maintenance
- Field Services enablement.

The process of updating to later versions of an IT application which is covered by technical support is called 'application maintenance'. The maintenance program is to keep the applications on current supported versions, to protect against failure of IT systems. In the 2019-24 regulatory period, we forecast this to cost $80.9 million ($, real FY19). This is a 'business as usual' program in line with our IT application policy and standards.

3.2 Customer outcomes

This program will allow Ausgrid to continue to deliver safe, reliable and affordable customer service and business operations. If we do not undertake this program, then the business operations will be significantly disrupted. This includes an increased risk of non-compliance with licence conditions, laws and regulatory obligations; our systems will be out of line with normal IT industry changes; and there would be an increased risk of a significant cyber security breach. This would also introduce inefficient ways of working, increased operational spend with people doing manual processes, and non-compliance to regulatory requirements.

There are safety impacts for all customers, including life support customers, hospitals, schools and transport if services are impacted.

The following are some specific examples of how these applications support the customers:

- Customer Outage. A customer rings our contact centre to report an outage. The call is directed through the Telstra avalanche mass call platform and Ausgrid contact centre systems (capable of receiving and processing 60,000 - 30 secs messages per hour). The technology determines whether we are already aware of an outage and if so, informs the customer and the approximate time to restore. The customer can hang up or be directed to an operator (in Australia) using intelligent call routing. The operator searches and logs (if not already) an outage for the customer within our outage management system. Based on the number of calls, the Outage Management System predicts timing and scale of outage.
- SAP Mobile Workforce Manager is used to send work orders to the field and also to capture data from field service staff on iPAD devices. These devices are used to remit

work orders for services to maintain our electrical network and integrate into SAP asset management system without manual intervention, includes job costing and time entry. This eliminates the need to go to the depot to get a schedule of which site to visit and removes paper handling and data input. In the event of failure, the ability to appropriately deploy field service staff and perform the right work is impacted, resulting in unproductive time for field staff.

- Asset planning and maintenance scheduling. Customers reference the Dial Before you dig system which links to Ausgrid systems to get information from GIS systems and provides it back to customers from safety and supply of electricity to the surrounding environment.
- Metering and Market Systems. These systems contain all the metering related assets, consumption data, B2B transactions and service orders for Ausgrid. Loss of systems could impact disconnect and reconnection of customers supply, updates of critical information such as life support customer data and reading of meters including move in / move out readings. As a network provider if we fail to disconnect a site for a retailer in the requested period Network are not entitled to charge the NUOS fees for that service resulting in a loss of revenue. In addition if our systems have not updated Life Support information and the customer is disconnected during a planned outage without notification this can result in a type 1 NECF breach.

3.3 Stream 1 – End of Life applications upgrades background

ICT systems have an expected useful life, which generally coincides with when the vendor reduces or withdraws support. Retaining systems beyond this point will result in additional maintenance costs and reliability risks, impacting on efficiency and resilience. Complex and integrated ICT environments are a mandatory investment for businesses such as Ausgrid that are required to make informed technical and economic decisions about their assets and operations.

Based on the size and maturity, software vendor will normally provide “Extended” or “Sustaining support” (where available) for up to one to two versions less the current version of the application. However, continuing to operating the business on applications older than this will result in the following risks:

- Core applications no longer being supported by ICT vendors
- Security exposures increase
- ICT applications becoming increasingly unstable
- Being unable to address strategic imperatives and architectural weaknesses
- An increased rate of failure in older IT applications, resulting in unplanned production outages
- Unable to adequately meet the quality, reliability and security of standard control services.

Ausgrid assesses its portfolio of applications based on the application classification shown in Table 10 below.

Table 10. Ausgrid’s application classification

Class	Description	Description
1	Mission critical 0 – 4 hours	Business Applications vital to the safe support and restoration of energy. The loss of the application will create unacceptable impacts to Ausgrid.

Class	Description	Description
2	Business critical 4 – 24 hours	Business applications which support the day to day viability of Ausgrid.
3	Business important 1 – 3 days	Business important applications used by multiple business areas within or across a division.
4	Non-critical > 3 days	Applications supporting key functions or activities of a workgroup.

A program of work to maintain end of life applications has been established to ensure current versions of Mission Critical, Business Critical and Business Important rated IT applications continue to be vendor supported and their technical currency is maintained reducing the risk of potential failure and/or unplanned production outages.

IT application policy and standards

Ausgrid has a set of IT Applications and Software Version compliance guidelines.

Under these guidelines, we aim to have continuous vendor support for our IT applications.

To do this, we monitor 'end of life' (EOL) notifications released by vendors. They inform users when the life cycle of an IT application is about to end. Typically, an EOL notification will set out a period of extended technical support.

Our goal is to use the extended technical support offered by vendors for as long as possible before replacing or updating an IT application. This minimises our costs by deferring the investment in a new or updated version of an IT application until all technical support is about to end.

3.3.1 Need

We have identified a suite of IT applications which are likely to have their technical support being withdrawn in the 2019-24 regulatory period.

To mitigate the risk of running software platforms without any technical support, we plan to update these IT applications. This will lead to continued stability in our software platforms over the forthcoming period.

Table 11 lists the IT applications which we anticipate will have their technical support withdrawn. Their role in the management of our business and regulatory obligations is also shown.

Table 11. IT applications expected to have technical support withdrawn

Project Name	BIA rating	Brief summary description of application(s)	Proposed scope – EOL Need
Asset Lifecycle Management			
SAS Enterprise	Business Critical	SAS Enterprise – is an application from which staff can access the following applications: General Load System (i.e. Genload): reporting of feeder and transformer loads at sub-transmission, zone and distribution levels. Loadcycle: load cycles and peak loads for sub-transmission and zone transformers. Protection Grading (i.e. Grade): analysis of system protection to achieve safe fault clearing times. TIS Query & Reporting: legacy reports against the Network Reporting Database.	Ensure the SAS Enterprise and its components continue to be vendor supported and their technical currency is maintained reducing any risk of potential failure and/or unplanned production outages.
Geographical Information System (GIS) EOL Maintenance	Mission critical	GE Smallworld GIS – is the database of records for spatial and connectivity data related to Ausgrid's network. It is used for Dial Before You Dig, planning and analysis along with providing data for key business systems such as SAP, Outage Management System (OMS), Electric Thinking Program (ETP) and Ratings and Impedance Calculator (RIC).	Investment will be required during the 2019-24 regulatory period to ensure that the GIS environment does not become unsupported and support for this Mission Critical system continues to be provided by the Vendor, General Electric (GE).
Engineering Applications	Business critical	AutoCAD / VAULT – used by Ausgrid that supports 2D and 3D Computer-Aided Design (CAD), drafting, modelling, architectural drawing, and engineering CAD. MicroStation – Information modelling environment.	Investment will be required during the 2019-24 regulatory to maintain the technology currency of these engineering applications and maintain the ability to send and receive compatible files with relevant contractors/partners and external third parties.
Physical Network Inventory (PNI) Maintenance	Mission critical	GE Smallworld PNI – is the authoritative source of telecommunications network spatial data. The PNI database is used by Ausgrid to manage the fibre optic network for teleprotection communication and signalling. The high integrity of PNI data provides the ability to build, manipulate and display a total, connected model of Ausgrid's telecommunications network which supports the management and operation of Ausgrid's electrical distribution network.	Investment will be required during the 2019-24 regulatory period to ensure that the PNI environment does not become unsupported and support for this Mission Critical system continues to be provided by the Vendor, General Electric (GE).

3.3.2 Options

Our assessment of the available options is set out in Table 12.

Table 12. Options analysis

Program needs options	What's involved	Assessment
1 Do nothing	IT application would not be updated or replaced when an EOL notification is released.	The applications listed in Table 11 would not be covered by technical support in the 2019-24 regulatory period. The stability of these programs is likely to suffer. If a bug arises, then we have no recourse to a vendor for any technical support. This is not considered a prudent approach as a loss of stability in our IT applications could put at risk our ability to continue to provide safe and reliable electricity network services, and to comply with our regulatory obligations.
2 Continue IT application maintenance	IT applications updated in line with IT application and software guidelines	The risks identified in the 'do nothing' scenario would be mitigated. In line with internal guidelines, we would use the extended technical support offered by vendors for as long as possible. This would minimise our costs by deferring the investment in a new or updated version of an IT application until all technical support is about to end. This is a 'business as usual' option which is necessary for the stability of our IT applications.

3.3.3 Preferred option

The adoption of a 'do nothing' (Option 1) approach would carry substantial risks. A large volume of application which Ausgrid uses to operate our business and support the delivery of network services would lose technical support, with the stability of these programs likely to suffer. The continuation of IT application maintenance (Option 2) is thus required to mitigate against the risk of this occurring.

3.4 Stream 2 – Mandatory patch and release management background

To maintain our IT security and the stability of our software, we implement small IT applications known as patches. This practice, referred to as 'patch and release management', is a 'business as usual' activity which will continue in the 2019-24 regulatory period.

Ausgrid uses a number of software programs to operate our business, store data and to meet our legislative and regulatory obligations.

Each of our software programs is subjected to 'patch management' and 'release management'. Both patch and release management are processes of acquiring, testing and installing 'patches' or new 'releases', which expand the capabilities of an existing program or which have been developed to correct an error in functionality.

Information security

A feature of both patch and release management is becoming more important is information security.

The Australian Cyber Security Centre (ACSC) notes that 'there are thousands of [cyber security] adversaries around the world willing to steal information, illegally make profits and undermine their targets'.[1] These threats are continually evolving, with adversaries constantly developing innovative approaches to gain access to IT systems.

To address these risks, an effective strategy is to manage the releases of changes to the software of patches. This is in line with advice from the ACSC which has found that 'implementing timely patching and system-hardening regimes and upgrading unsupported operating systems will mitigate most of the risk [of intrusion].[2]

A recent example which demonstrates this is the 'WannaCry' ransomware attack. In May 2017, it infected 250,000 computers in 150 countries. From a patch management perspective, this attack is significant because the virus exploited a known vulnerability in a widely used software program which had been 'patched' months earlier.

Malicious attacks such as WannaCry are likely to become more frequent over the 2019-24 regulatory period as cyber threats become more sophisticated. As a prudent electricity distributor, we will need to continually update our software programs with newly released patches that mitigate known vulnerabilities.

Ausgrid programs

We have acquired software programs to suit the needs of each of the divisions in Ausgrid. Table 13 sets out these divisions and summaries how they use software programs to deliver reliable and safe network services, and support the operation of our business.

Table 13. Software programs by Ausgrid division

Division	Software programs
Asset Operations	The programs supporting our Asset Operations are used to monitor our assets and to manage network outages. Assets which are managed using these programs include plant, components of our network, communications infrastructure, meters and modems. The applications supporting this domain hold key network information that must be kept secure from outside vulnerability to continue to provide safe and reliable network services.
Market Management	Our Market Management programs collect and store metering and market data. The data which we manage via these programs is essential for customer billing and our interaction with other energy providers in the national electricity market. Personal information about our customers is stored in our Market Management programs. This gives rise to regulatory obligations under the Privacy Act.
Customer Management	We hold data about Ausgrid customers in our Customer Management programs. Any vulnerability in these applications may be a target of cyber-attack. The data which in collected and stored within our Customer Management programs includes personal information subject to regulatory obligations in the Privacy Act.
Enterprise Management	Enterprise Management provides core 'back office' functions. These functions are not directly involved with the supply electricity distribution services, but provide core support capabilities relating to: Financial control and reporting Effective management of human resources Compliance with work, health and safety regulatory obligations Procurement.

3.4.1 Need

We use software programs to operate critical infrastructure, manage our business and to collect and store data – including personal information – about our customers.

[1] Australian Cyber Security Centre, *2017 Threat Report*, 2017, p. 2.
[2] Australian Cyber Security Centre, *2017 Threat Report*, 2017, p. 38.

As patches or small changes are released for these software programs, Ausgrid is faced with a need to manage them. This is by acquiring, installing and testing new software that correct errors and which remedy vulnerabilities that have been identified in our information security.

In the 2019-24 regulatory period, our patch and release management needs are likely to expand. Cyber security threats are increasing in sophistication and, in response to this, software developers are continually increasing the frequency and volume of the patches and versions they release.

3.4.2 Options

Our assessment of the available options is set out in Table 14.

Table 14. Options analysis

Program needs options	What's involved	Assessment
1 Do nothing	We would not download the new releases or patches for our existing suite of IT applications when they are released	Our IT security would be put at risk. Potential adversaries seeking to target vulnerabilities in 'un-patched' software would have a higher likelihood of succeeding.
2 Continue patch and release management	Ausgrid would continue to acquire patches and releases when they become available	The risks identified in a 'do nothing' scenario would be mitigated. This is a 'business as usual' program which is required to respond to our existing cyber-security threats and the expected uplift in the volume of releases and patches being released by vendors.

3.4.3 Preferred option

Option 1 (do nothing) would carry too much risk as it could expose Ausgrid to potential adversaries seeking to exploit 'un-patched' or out of date software. Option 2 (continue patch and release management) is therefore the preferred option. It will allow us to respond to our existing cyber-security threats and the expected uplift in the volume of patches and releases being distributed by vendors.

3.5 Stream 3 – SAP core maintenance background

We plan to migrate our SAP core management systems to a next generation platform. This is in response to an announcement that the version of SAP we presently operate will have its mainstream maintenance withdrawn.

After our SAP transformation program, our systems will be managed in the cloud under a software subscription contract rather than currently as it is on premise.

SAP is a suite of business software. It includes SAP 'Enterprise Resource Planning' (ERP) and SAP 'Business Warehouse' (BW), along with other associated products.

The ERP version of SAP provides an integrated and continuously updated view of core business processes. It provides this by integrating the collection, storage, management and interpretation of data produced by an organisation.

To achieve this, SAP ERP comprises of various IT applications called 'modules'. Each module is developed for specific areas of a business. The role of SAP ERP is to connect these modules so that data can be shared across all areas of a business. Among other things, SAP has developed modules specifically for plant (asset) maintenance, procurement, financial and management accounting, inventory planning, and human resources.

SAP BW performs a different, but related, function to SAP ERP. Whereas SAP ERP provides for an integrated view of the processes needed by an organisation to run its business, the role of SAP BW is to store and consolidate that data for reporting. Each SAP product therefore works together to manage the information requirements of a business.

How Ausgrid uses SAP

We use both SAP ERP and SAP BW as the core enterprise system platform for most areas of our business. This includes:

- Asset life management and operations
- Works management
- Customer management
- Finance management
- Network billing
- Human resources
- Procurement
- Planning and scheduling
- Enterprise functions, including IT management.

Product life cycle

The version of SAP ERP which we use to run our business is called 'SAP ECC6'.

In FY2025, 'mainstream maintenance' for SAP ECC6 will end. Mainstream maintenance provides SAP customers, including Ausgrid, access to regular support packs and patches. These contain critical system fixes and country specific system changes related to regulatory and legal compliance obligations.

The withdrawal of mainstream maintenance would put Ausgrid at risk. The stability of SAP ECC6 is likely to suffer as regular system fixes would no longer be offered. Our ability to comply with our regulatory and legal compliance obligations could also be put at risk, as we would no longer receive updates to SAP ECC6 in line with changes to those obligations.

New platforms

The latest version of SAP which has been released is called 'SAP S/4 HANA'.

SAP S/4 HANA is different to the version of SAP we currently operate in two main respects. It is, first, 'cloud' based and, second, procured via a 'Software-as-a-Service' (SaaS) contract.

Being cloud based means that SAP S/4 HANA utilises remote server infrastructure, not owned and managed by Ausgrid to store, manage and process data. This is different to how our current version of SAP works, which performs its data functions independent of the internet, via servers owned and managed in Ausgrid data centres.

SaaS, the other major difference between our current version of SAP, is a subscription based approach to delivering software. With SaaS, cloud providers combine the cost of hosting and managing software applications and underlying infrastructure, and handle any maintenance such as updates and security patching. Users connect to the application over the internet and pay a subscription fee.

The adoption of SAP S/4 HANA would reduce ICT capex and total cost of operation (TCO) over the long run through the SaaS delivery model. However, to perform this transition, capex would be required in the implementation phase during the 2019-24 regulatory period.

3.5.1 Need

The version of SAP ERP we currently operate (SAP ECC6) will have its mainstream maintenance withdrawn in 2024/25. To provide continuity in technical support, this creates a need to consider migrating to a new platform within the 2019-24 regulatory period.

3.5.2 Options

We have assessed the options we have available to address the impending withdrawal of mainstream maintenance for our current version of SAP ERP. Table 15 summarises this assessment.

Table 15. Options analysis

Program needs options	What's involved	Assessment
1 Do nothing	Continue with the existing version of SAP ECC6 as currently deployed on Ausgrid's own hardware infrastructure hosted in our on-premise data centres.	This option is not consistent with the vendor (SAP) recommendation to migrate to next generation technology platforms. The withdrawal of mainstream maintenance for our existing version of SAP (SAP ECC6) would result in our systems going into 'extended' maintenance support in the short term and to be un-supported by the vendor soon after that. The loss of technical support would put the stability of our data management systems at risk and our ability to continue to provide safe and reliable energy network services to our customers.
2 Migrate to a SAP S/4 HANA	Ausgrid would migrate from its existing arrangements to a cloud based system delivered via a SaaS model Both our existing versions of SAP ERP and BW would be replaced with SAP S/4 HANA.	We have selected this option as it addresses the risks involved with losing mainstream maintenance for our existing SAP platform in 2023/24. This option will result in reduced Capital expenditure and an optimum TCO in the long run, however significant business process re-engineering project activities need to be conducted which would incur CAPEX cost during the implementation phase.

3.5.3 Preferred option

Based on our analysis, Option 2 was considered the most prudent and efficient to enable Ausgrid to receive the full benefits of this project and ensure continued delivery of standard control services.

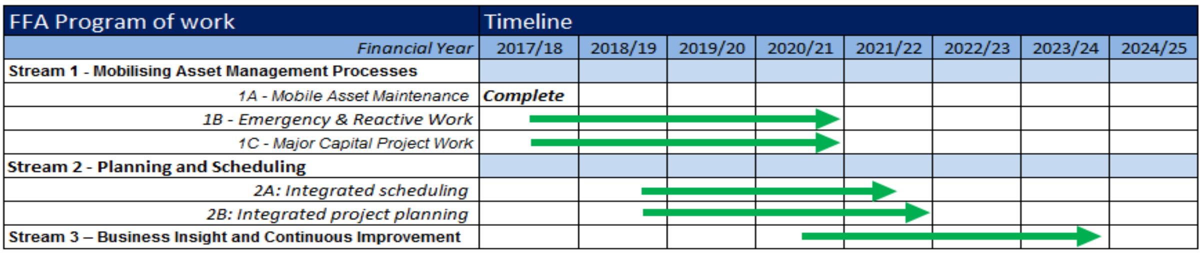
3.6 Stream 4 – Field services enablement background

Our field services workforce is critical to the delivery of a safe and reliable electricity service to our customers. Along with the construction and installation of new assets, the field services workforce is responsible for responding to emergencies, conducting proactive maintenance of our assets, and managing vegetation growth around our electrical equipment.

The existing systems in place for managing field services activities are in need of modernisation. At present, scheduling and resource allocation is principally managed through paper based ‘job packs’. This leads to delays in the provision of information to and from the field. The paper based system causes a lack of visibility across the field services regarding how resources could increase productivity.

The implementation of the Field Services program has commenced in 2014-19 regulatory control periods by modernise some of these processes through the introducing a mobile IT platform for our field workforce. This has enabled real, or near real, time maintenance updates for 26 maintenance types both to and from the field without the need for manual processes. Further implementation of field processes with SAP will increase automation and accuracy of information on work performed on our assets.

Figure 1. Indicative timing for the FIELD SERVICES program



FFA Program of work	Timeline							
Financial Year	2017/18	2018/19	2019/20	2020/21	2021/22	2022/23	2023/24	2024/25
Stream 1 - Mobilising Asset Management Processes								
1A - Mobile Asset Maintenance	***Complete***							
1B - Emergency & Reactive Work	→	→	→	→				
1C - Major Capital Project Work	→	→	→	→				
Stream 2 - Planning and Scheduling								
2A: Integrated scheduling		→	→	→	→			
2B: Integrated project planning		→	→	→	→			
Stream 3 – Business Insight and Continuous Improvement				→	→	→	→	

As shown in Figure 1 above, the Field Services program is to be delivered via three streams staggered across both the 2014-19 and 2019-24 regulatory control periods. The first stream involves the deployment of a mobile IT platform to the asset maintenance, emergency and reactive works and major capital project divisions of our field workforce. Some of this has completed and has begun to phase-out the requirement to issue paper based job packs.

The second stream builds on the first by introducing scheduling capabilities. Along with a consolidated view of maintenance and capital work, this scheduling tool will provide Ausgrid with the ability allocate resources using a mobile IT platform and reallocate them during emergencies. The third stream is a business improvement phase which will provide real-time visibility of fieldwork and a dashboard solution for managers displaying performance metrics, ratios and trends.

3.6.1 Need

The planned Field Services program is an “ICT Asset Replacement” project primarily driven by a need to broaden the functionality of our existing ICT assets.

We currently have a SAP asset management system which is capable of enterprise workforce scheduling and resource allocation. The Field Services program has enhanced these existing ICT capabilities by implementing a mobile IT platform that automates current processes and provides greater visibility, and control, over the scheduling of our field workforce and the allocation of resources. The program will continue to build on the mobile IT platform and integrate additional functions to support the field delivery initiatives.

3.6.2 Options

Our assessment of the available options is set out in Table 16. It shows that the completion of the final streams of the program has been selected for the 2019-24 regulatory period.

Table 16. Options analysis

Program needs options	What's involved	Assessment
1 Do nothing	Continue to leverage solutions delivered in the 2014-19 regulatory period (see stream 1A in Figure 1 above) without completing the remaining streams.	This option is not consistent with the Network submission requirements. No further ICT capital expenditure would be incurred on the Field Services program. The full benefits of the initial rollout of stream 1A of the Field Services program would not be realised, with the current paper based resource allocation and scheduling still relied on.
2 ICT extension ('Field Services program')	Implementation of the remaining Field Services improvements to realise further business benefits.	We have selected this option as it addresses the requirements to support the Network submission. This option will result in current paper based systems being replaced with automated processes capable of enterprise wide resource allocation and scheduling. Real (or near real) time project updates would become available and manual updates into SAP would no longer be required. Managers would have access to dashboard analytics and end to end reporting.

3.6.3 Preferred option

The preferred option is to implement the remaining components of the field services program to automate functionality to assist the Network business achieve the targeted results for the 2019-24 regulatory period (Option 2).

4 PROGRAM 4 – INFRASTRUCTURE AND TELECOMMUNICATIONS MAINTENANCE

4.1 Program description

The program seeks to complete, in the 2019-24 period, the migration of Ausgrid's core IT infrastructure services to cloud based offerings and maintain or refresh elements of Ausgrid's telecommunications infrastructure that are reaching the end of their technical life.

The Infrastructure and Telecommunications maintenance program consists of two major streams.

1. Infrastructure maintenance
2. Telecommunications maintenance and capacity upgrades.

This is an ongoing program which commenced in the 2014-19 period. The forecast value of the program in 2019-24 is $24.1 million ($, real FY19), resulting in a reduction of $11.9 million ($, real FY19) from the previous period.

4.2 Customer outcomes

The Application Maintenance Program relies on the Infrastructure and Telecommunications maintenance program to deliver safe, reliable and affordable customer service and business operations. If we do not undertake this program, then the business operations will be significantly disrupted. This includes an increased risk of non-compliance with licence conditions, laws and regulatory obligations; our systems will be out of line with normal IT industry changes; and there would be an increased risk of a significant cyber security breach as the majority of the applications run on the Infrastructure and "connect" to each other via the telecommunications. This would also introduce increased operational spend with errors and corrections required to be processed manually.

As a consequence of the applications relying on the infrastructure and telecommunications, the same customer impacts exist as those included in Program 3.

4.3 Stream 1 – Infrastructure maintenance background

Our core IT infrastructure is currently made up of servers and storage architecture located "on-premise" at data centres where Ausgrid leases space.

The proposed works will complete an ongoing program targeted at transitioning to a cloud based support model for IT infrastructure by FY2024. This will involve the migration of on-premise servers and connectivity to cloud based technologies.

The decision to begin transitioning to cloud based technologies in the 2014-19 period was based on an assessment that our existing on-premise IT infrastructure model was too costly and time consuming to refresh. This will simplify our core IT infrastructure requirements by moving to 'Infrastructure as a Service' (IaaS) and 'Platform as a Service' (PaaS) arrangements.

4.3.1 Need

The program is primarily driven by a need to manage our existing IT infrastructure costs and align to industry standards.

In response to our growing digital needs, the cost of operating our existing on-premise IT infrastructure is forecast to exponentially increase. Our existing infrastructure is also aging and is becoming more expensive to maintain if it is kept in service beyond the 2014-19 period due to changes in the industry.

This is a simpler approach to IT infrastructure delivery as it shifts responsibility for security, technical upgrades and other updates from Ausgrid to our Cloud Service Providers. It will therefore allow for a leaner IT team as some current activities will be provided by the cloud service providers once the transition is complete.

By migrating to cloud based technologies we will be able to manage our rising IT operating costs, and reduce the total cost of ownership. Other needs which the program will deliver are outlined in Table 16.

Table 17. Overview of drivers

Drivers	Overview
Increased flexibility of operations	Cloud based technologies enable rapid scaling of data and storage and accelerated delivery of new applications and services to meet changing business needs.
Future proofs against risk and compliance	Moving to the cloud keeps Ausgrid compliant with industry and regulatory requirements, and provides for a more future proof architecture.
Currency and compliance	Patches and server maintenance is performed by the Cloud Service Provider as part of their maintenance as opposed to internally managed lifecycle management activities.
Enhanced security maintenance	Moving to the cloud will enable increased proactive monitoring, identification and response to threats.

4.3.2 Options

We have already commenced migrating to cloud based technologies for the delivery of our core IT infrastructure. The options for how we proceed in the 2019-24 are set out in Table 18 below.

Table 18. Options analysis

Program needs options	What's involved	Assessment
1 Do nothing	The migration of services to the cloud would stop, leaving a number of infrastructure components in a semi-migrated state	Additional capex would be required to maintain and upgrade the remaining on-premise infrastructure. In addition, there would be higher support costs to manage a hybrid environment with both cloud and on-premise solutions. The potential benefits from capex already spent on this program would, as a result, never be realised.
2 Do the minimum	Ausgrid would re-prioritise the migration to pursue the inflight infrastructure/platform as a service and leave all remaining infrastructure components maintained on-premises	Some benefits from capex already incurred would be realised under this option. It would, however, lead to Ausgrid operating both on- and off-premises infrastructure. In addition, there would be higher support costs to manage a hybrid environment with both cloud and on-premise solutions.
3 Do the optimum	We would continue the transitioning to a cloud based support model for the management of all infrastructure ("Infrastructure as a Service" / "Platform as a Service").	The full benefits of capex already incurred on this program would be realised. This option would also come at a lower on-going operating cost than if a 'do the minimum' or 'do nothing' options were pursued.

4.3.3 Preferred option

Based on our analysis, Option 3 was considered the most prudent and efficient to enable Ausgrid to receive the full benefits of this program.

4.4 Stream 2 – Telecommunication maintenance and capacity upgrades background

Telecommunications are vital for monitoring and controlling the electricity network, connectivity of applications and infrastructure, and connectivity to the market providers. They are also critical to our corporate functions by enabling communications between our staff across our network.

The telecommunications infrastructure provides network connectivity across about 50 corporate sites through routers and switches, allowing access to data centres and cloud based resources for critical applications, data storage and telephony.

4.4.1 Need

Ausgrid has invested in deploying and maintaining its own telecommunications infrastructure. In the 2014-19 period, we invested in higher capacity communications and connectivity infrastructure. These will support proposed investments in technology such as our Advanced Distribution Management System (ADMS) and the migration of our applications and infrastructure to cloud based offerings.

Our telecommunications infrastructure reaching the end of life is required to be maintained through installation of more recent software or replaced with newer hardware. This scope includes the communications network, corporate environment, operating support systems, and voice and video maintenance.

The program will ensure we maintain the performance of our telecommunications infrastructure which in turn will support reliable and secure electricity service to our customers, and ensure that no critical business functions are endangered.

The drivers for the program investment are to ensure the communications network has connectivity to transfer data between applications as we transition to cloud services. We propose to maintain the existing hardware and software until the end of agreed support period. At the end of the support period, we will have transitioned to cloud based platforms outside of our data centres.

The telecommunications infrastructure includes tools which provide end to end management, including monitor and reporting on Ausgrid's network management systems. These tools also provide secure access to data centre and cloud based resources. These tools are needed to ensure notification of communication failures on the network; this visibility provides warnings vital to maintaining the network.

In addition, there is a need for voice and video communications to maintain the normal operation of the network and for critical event management by enabling the control room to communicate and co-ordinate activities.

4.4.2 Options

We have already commenced migrating to cloud based services for the delivery of our corporate telecommunications infrastructure. The options for how we proceed in the 2019-24 are set out in Table 19 below.

Table 19. Options analysis

Program needs options	What's involved	Assessment
1 Do nothing	The migration of services to the cloud would stop, leaving a number of telecommunications components in a semi-migrated state. The services required to stay on premise that reach end of life would be unsupported.	This approach would expose Ausgrid to the risk of service unavailability. Reliability would decline a result of higher failure rates of ageing equipment, unsupported software and limited network capacity.
2 Upgrade the telecommunication infrastructure	Replace the asset with a "like for like" solution or migrate to a Cloud/Hosted solution or maintain the asset software under the vendors support agreement where required to remain on premise.	This is the preferred option to evaluate each item so that when infrastructure has reached the end of its technical life or a vendor has withdrawn technical support, determine if the solution can be migrated to the cloud/hosted solution.

4.4.3 Preferred option

Based on our analysis, Option 2 was considered the most prudent and efficient to enable Ausgrid to receive the full benefits of this program.

5 PROGRAM 5 – WORKPLACE TECHNOLOGY

5.1 Program description

We have a planned program to sustain the capabilities of our existing ICT workplace technology which supports Ausgrid employees and contractors to perform their day to day activities. This includes email systems, desktop standard operating environments (SOE), and mobile devices.

In the 2019-24 regulatory period, we forecast that the cost of this program will be $4.7 million ($, real FY19).

5.2 Customer outcomes

This program enables Ausgrid to maintain productivity, mobility and quality of collaboration for the workforce.

A mobile enabled workforce can lead to opportunities to rationalise office floor space and facilities costs as employees are freed from reliance on fixed work spaces. The implementation of this program is likely to lead to lower operating costs which, in the longer term, will be passed on to the customers through lower prices.

ICT Program 3 provides examples of the customer outcomes which rely on reliable workplace technology. The use of iPAD devices across the field in particular is important for achieving an efficient outcome for customers.

5.3 Background

In response to our growing digital needs and the need for a mobile enabled workforce, we transitioned our field employees to iPAD devices in the 2014-19 period. We also aligned our workplace technology tools with industry standard for modern work practices. We commenced the transition from Lotus notes to Office 365, by moving to Outlook, Skype for Business and online access to the Microsoft office suite of tools allowing for streamlined integration across the workforce.

5.4 Need

The program is primarily driven by a need to maintain our workplace technology to enable continued delivery of the business outcomes. There is a need to continue this modernisation program by fully transitioning away from Lotus Notes databases and aging content management platforms to enable shared content across the organisation for safety documentation and project communications.

We need to implement additional functionality included in Office 365 to reduce overall cost of ownership for workplace technology tools. This includes upgrading the Windows SOE to mitigate software defects that can occur if operating systems are not supported which would impact on our workforce ability to deliver to the end customer.

We need to maintain and refresh mobile devices to prevent failures of the device which would impact on performance of field delivery productivity.

5.5 Options

We have already commenced migrating to modern workplace technologies across Ausgrid. The options for how we proceed in the 2019-24 are set out in Table 20 below.

Table 20. Options analysis

Program needs options	What's involved	Assessment
1 Do nothing	Ausgrid would not invest in any maintenance to support and enhance the components of workplace technology. This would result in stopping “as-a-service” capabilities that have been transitioned to date, not maintaining the desktop SOE and continuing to use existing mobile devices with no replacement plan.	This option exposes Ausgrid to unacceptable risk associated with unsupported software and ageing devices supporting critical business processes. This would result in potential security breaches and increased costs associated with both desktop support and information security. These costs would eventuate due to the increased number of support and security incidents which would result from not having desktops and mobiles on supported software.
2 Maintain currency of workplace technology components	We would complete the transition to and maintain support and enhancement processes for modern ‘as-a-service’ tools; maintain new desktop SOE as required; and maintain the currency of the mobile device fleet by conducting an on-going maintenance and refresh program.	The full benefits of past expenditure incurred on this program would be realised by completing the migration to new tools. The stability of this workplace technology would also be maintained through enabling secure and reliable tools to support critical business processes.

5.6 Preferred option

Option 2 (Maintain the currency of workplace technology components) is the preferred option. This option maintains the core platform required by users to access Ausgrid's key business applications and corporate data.

6 PROGRAM 6 – DATA AND DIGITAL ENABLEMENT

6.1 Program description

The way in which customers expect to interact with service delivery providers has evolved. The Data and Digital Enablement program is an ongoing program to provide the data and digital technologies required to support the efficiencies already built into the proposal and meet changing customer expectations.

The data and digital enablement program consists of two streams.

1. Digital transformation
2. Information management

This is an ongoing program which commenced in the 2014-19 period. The forecast value of the program in 2019-24 is $23.5 million ($, real FY19).

6.2 Customer outcomes

Customer expectations are changing demanding faster response times, real time and up to date information which is readily accessible for outages and consumption data pushed out to mobile devices and information portals.

If we do not undertake this program, our costs will increase as we will continue to manage using old technologies creating manual processes for both our customers and our employees.

These programs enable the use of digital technologies to improve safety, response times and better predictive decision making for investments.

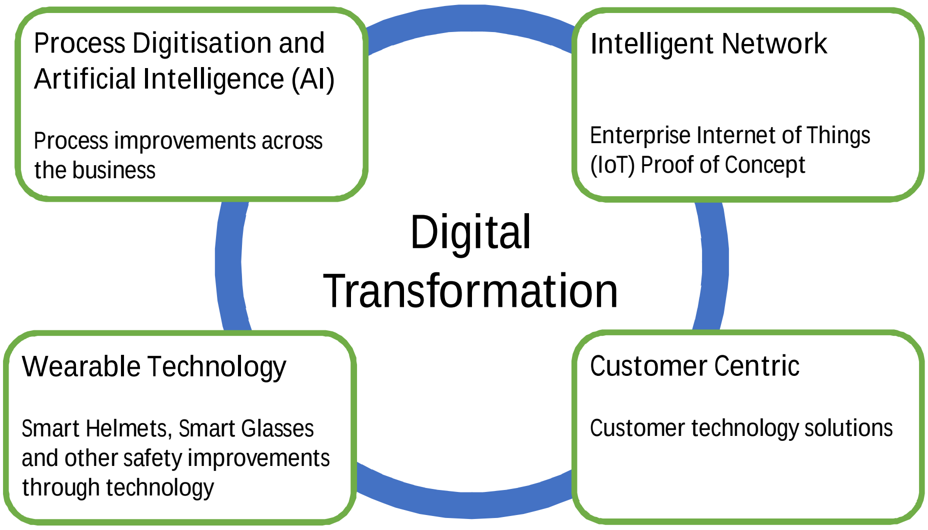
This program responds to the evolution in customer preferences by replacing older technologies and manual process with digital based platforms that will provide information to customer when and how they want it.

6.3 Stream 1 - Digital transformation background

Digitisation is changing the way organisations do business. In the 2019-24 regulatory period, Ausgrid will be required to respond to these changes by transforming our practices to digital processes.

This will involve taking advantage of developments in digital technology that provide for greater automation of our internal processes and expand the capabilities of our existing IT systems. In particular, we have four streams of work planned for the next period, as illustrated in Figure 2 below.

Figure 2. Digital transformation streams of work


Process Digitisation and Artificial Intelligence (AI)
Process improvements across the business
Intelligent Network
Enterprise Internet of Things (IoT) Proof of Concept
Digital Transformation
Wearable Technology
Smart Helmets, Smart Glasses and other safety improvements through technology
Customer Centric
Customer technology solutions

Process Digitisation

The implementation of Robotic Process Automation (RPA) involves automating processes which are currently handled manually. RPA in back office, shared services and contact centres will enable Ausgrid to improve reliability of our systems and the quality of the data we produce.

Intelligent network

The Intelligent Network stream involves investing in programs as input into the strategy, costs, benefits and process of implementing an Enterprise Internet of Things (IoT).

The IoT comprises of a network of devices which are able to connect and exchange data via the internet. The establishment of an Enterprise IOT by Ausgrid would involve expanding the existing internet connectivity of our electricity network assets and devices. This would facilitate data capture from all IoT devices and allow for assets and devices to be managed within our network securely.

Wearable technology

There is opportunity for Ausgrid fieldworkers to utilise wearable technology, i.e. a smart helmet or smart glasses. The wearable technology can improve productivity by using voice recognition to automate the raising of service orders and to undertake other administrative tasks.

Customer centricity

Ausgrid will continue to develop its customer management platform to expand the capabilities to facilitate and automate (where appropriate) two-way communication with our customers and partners; and adds a preference centre that enables customers to register with Ausgrid to receive alerts (through their preferred method of real time communication) on information relevant to them. Additional capabilities will be provided enable personalised self service capabilities for customers and invest in eliminating manual processes.

6.3.1 Need

We have an ongoing need to respond to align to industry standards and advancements in digital technology which enable us to improve our processes through greater automation or expanded IT capabilities.

This ongoing need is corroborated by The Electricity Network Transformation Roadmap developed by Energy Networks Australia and the CSIRO. Digital transformation is required to meet the following items identified in the roadmap:

- Improves trust with customers through better engagement and customised services
- Facilitates an ‘intelligent grid’ which defers or negates the need for capital expenditure by better managing peak demand
- Leverages flexible, efficient and agile ways of delivering electricity network services to customers.

6.3.2 Options

Our assessment of the available options, together with an overview of what would be involved, is set out in Table 21.

Table 21. Options analysis

Program needs options	What’s involved	Assessment
1 Do nothing	Do not develop the current digital platforms further.	We will fall behind the industry and be unable to reduce costs which are required to undertake the Ausgrid regulatory program. We will continue to develop older technologies at a higher price.
2 Planned digital transformation program	Continue to develop and test digital technologies to improve interaction with customers, safety of the workforce and automate processes.	We will align to IT industry standards, provide our customers a streamlined, lower cost experience and improve the safety of our workforce.

6.3.3 Preferred option

We have selected Option 2 (implementation of planned digital transformation program) as our preferred option.

6.4 Stream 2 - Information management background

Our information management needs are guided by our compliance obligations and an internal audit of our current capabilities. To gauge our needs in the 2019-24 regulatory period, we also took into account the Energy Network Association’s (ENA) roadmap.

Compliance obligations

Since our last regulatory determination, we have had additional compliance obligations imposed on us. Among these additional obligations are new requirements relating to information management.

Our Ministerially imposed Licence Conditions for Ausgrid Operator Partnership to operate a distribution system came into effect on 1 December 2016. Under clause 9.2(a), they require Ausgrid to put in place data management systems which are consistent with the following:

> [Ausgrid] must, by using **best industry practice** for electricity network control systems, ensure that operation and control of its distribution system, including **all associated ICT infrastructure, can be accessed, operated and controlled only from within Australia**, and that its distribution is not connected to any other infrastructure or network which could enable it to be controlled or operated by persons outside Australia (emphasis added).

Internal audit

Ausgrid recently conducted an internal audit of our existing data management capabilities.

It revealed a perception that Ausgrid is behind our peers in the industry and is largely reactive to business demands and regulatory challenges. The audit also observed that data management systems tended to be developed in silos and that there was a need to standardise approaches across the business.

Transformation

The industry in which Ausgrid operates is moving towards the direction described in the roadmap released by ENA in April 2017. It identified a need to "address the management and exchange of information between networks and distributed energy resources participants and allow effective coordination of the system in real time".[3]

In the 2019-24 regulatory period, we will need to develop our data management systems in line with this vision from the ENA. This may include, among other things, the establishment of a registry for small scale battery storage, as outlined by a recent COAG Energy Council Consultation Paper.[4]

6.4.1 Need

Ausgrid continues to face challenges with its current information management capabilities due to the pain points below:

- **Information Delivery:** In most areas of the business, processes have been designed to accept a significant delay in gathering insights from data. This limits the ability for Ausgrid to be proactive, agile and effective.
- **Data Quality:** Although usability and quality are improving, outcomes vary by business area. Challenges stem from information still sitting in physical form, priorities of business areas, and high effort in preparing data from multiple data stores. There is a lack of alignment and reconciliation between various data sources which results in difference between insights and reports.
- **Accessibility:** Areas of the Business have indicated challenges in having to access data and reports from multiple interfaces and source systems, requesting a consolidated view of reports and a single point of truth. There are limited capabilities around cross-functional analysis of data as reporting capabilities are siloed. As such, business are not in a proactive, forward facing position; but rather struggle to optimise daily tasks.
- **Business Empowerment:** Business areas suffer from a lack of agility due to a limited awareness, access, skills and tool capabilities. This restricts them from achieving significant value from current information systems and investments.
- **Skills and Training:** There is a general consensus that people are not receiving adequate formal training in information technologies. People are not skilled enough to use standardised tools and information systems. The level of analytics capabilities across the business is below peers and the wider industry levels.

6.4.2 Options

Our assessment of the available options, together with a description of what would be involved if they were implemented, is set out in Table 22 below.

[3] ENA, *Electricity network transformation roadmap: Final report*, April 2017, p. 72

[4] COAG Energy Council, *Consultation Paper: Cost benefit analysis of options to collect and share information about small scale battery storage*, 22 May 2017.

Table 22. Options analysis

Program needs options	What's involved	Assessment
1 Do nothing	Maintain existing data management systems	We will remain reactive to business demand and market challenges.
2 Planned data management program	Enhance information management systems across the business	This will expand our existing information management capabilities. Undertaking this option, will allow Ausgrid to continue to meet our regulatory obligations and put us in a position where we can respond to our changing data management requirements.

6.4.3 Preferred option

The preferred option is to complete the planned data management program (Option 2). It is required to meet our regulatory obligations and, unlike if we did nothing (Option 1), will provide Ausgrid with the necessary level of flexibility to respond to our changing data management requirements.