



31 January 2023

# **Attachment 5.9.e: ICT & infrastructure program**

## **Ausgrid's 2024-29 Regulatory Proposal**

Empowering communities for a resilient,  
affordable and net-zero future.



## Table of Contents

1. Document governance .....	4
1.1. Purpose of this document .....	4
Related documents .....	4
Document history .....	4
Approval(s) .....	4
2. Executive summary .....	5
3. CONTEXT .....	7
3.1. Background .....	7
3.1.1. Introduction .....	7
3.1.2. Current capability .....	7
3.1.3. Key drivers of change .....	8
3.1.4. How we manage risk associated with aging ICT infrastructure assets.....	8
3.1.5. ICT Risk Appetite .....	9
3.1.6. Cyber Risk Appetite .....	9
3.2. Problem / opportunity .....	10
3.3. Investment objectives .....	10
3.4. Customer outcomes .....	11
3.5. Business drivers .....	12
3.6. Compliance requirements.....	12
4. OPTIONS.....	14
4.1. OVERVIEW OF OPTIONS .....	14
4.2. OPTION 1: BASE CASE (Maintain current assets).....	15
4.2.1. Description.....	15
4.2.2. Option 1 assumptions .....	15
4.2.3. Option 1 costs.....	16
4.2.4. NPV analysis .....	17
4.3. OPTION 2: Renewal and upgrades of ICT infrastructure .....	17
4.3.1. Option 2 assumptions .....	17
4.3.2. Option 2 costs.....	17
4.3.3. NPV analysis .....	18
4.4. Alternative Options .....	19
4.4.1. Infrastructure Services .....	19
4.4.2. End-user computing.....	20
4.5. Approach to Costing.....	20

5. RECOMMENDATION .....	21
5.1. Recommended solution.....	21
5.2. Program delivery risks .....	21
5.3. Program assumptions.....	22
5.4. Program dependencies .....	22
5.5. Business area impacts .....	23
6. GLOSSARY .....	24
7. APPENDICES.....	26
Appendix 1 Risk assessment – Option 1 .....	26
Appendix 2 Risk assessment – Option 2.....	29
Appendix 3 Infrastructure asset lifecycle management guidelines.....	31
Appendix 4 Overview of infrastructure lifecycle –end of life (EOL) dates .....	33
Appendix 5 2024-29 Major ICT infrastructure initiatives .....	34

## 1. Document governance

### 1.1. Purpose of this document

The purpose of this document is to outline a program brief for the proposed Information, Communications and Technology (ICT) and Infrastructure program of work that will form part of our 2024-29 regulatory proposal.

### Related documents

Document	Version	Author
Attachment 5.9 - Technology Plan	V2.1	ICT Manager
Attachment 5.9.k - ICT & Infrastructure - CBA model	V1.0	ICT Manager
Consolidated Cost Model	V18.0	ICT Manager
2022-35 Corporate Strategy	V1.0	Head Of Strategy
2022-29 Technology Strategy	V1.0	CIO
2022-25 Cyber Security Strategy	V1.0	CISO
ICT Asset Lifecycle Management Guidelines	V3.0	ICT Manager
ICT Digital Risk Management Branch Procedure	V1.0	ICT Manager

### Document history

Date	Version	Comment	Person
28/02/2022	V1.0	Initial Draft	ICT Manager
15/03/2022	V1.1	ICT Leadership Team Feedback	ICT Manager
18/03/2022	V1.2	CIO Feedback	ICT Manager
11/05/2022	V1.3-5	Independent Review	ICT Manager
31/10/2022	V1.6	CIO Final Review	CIO

### Approval(s)

Name	Position	Date
CIO	Chief Information Officer	31/10/2022
CFO	Chief Financial Officer	30/11/2022

## 2. Executive summary

The table below provides a summary of the ICT and Infrastructure program discussed in this program brief. It shows that the program of work, if approved, will require a total investment of \$70.3 million and would reduce our overall risk exposure to Group Risks (specifically 11.1 – Failure of Internal ICT Services and 4.1 - Significant Protective Security Incident). It would also deliver probabilistic benefits of \$113.7 million over 5 years and net present value (**NPV**) of \$49.9 million, based on our NPV modelling.

Executive summary	
<b>Key Objective(s) of the program</b>	<p>Key objectives of our ICT Infrastructure program for FY25-29 regulatory control period are:</p> <ul style="list-style-type: none"> <li>• Maintain prudent and efficient ICT Asset Lifecycle Management of our core ICT Infrastructure in support of delivering efficient, reliable, and secure energy services to customers;</li> <li>• Provide fit-for-purpose ICT Infrastructure to support business and customer platforms and services, enabling consistent reliability and availability without disruption;</li> <li>• Provide fit-for-purpose end user devices (laptops, PCs, and tablets), telephony and mobile telecommunications so that our field and office workers can efficiently deliver energy services and communicate with customers and stakeholders;</li> <li>• Optimise performance and cost-to-serve<sup>1</sup> across the ICT Infrastructure portfolio; and</li> <li>• Utilise modern Infrastructure-as-a-Service (<b>IaaS</b>), Platform-as-a-Service (<b>PaaS</b>) and Software-as-a-Service (<b>SaaS</b>) offerings, which are 'pay per use' and scalable in support of growing data and storage needs.</li> </ul>
<b>Customer benefits</b>	<ul style="list-style-type: none"> <li>• Enables continued delivery of safe and reliable electrical services to customers with the least possible disruption, also meeting regulatory compliance and strategic business objectives.</li> <li>• Prudent mitigation of key operational risks by enabling systems to be up to date and supported by vendors.</li> <li>• Value for customers through controlled capex through effective asset lifecycle management</li> <li>• Appropriate risk management over the life of assets to enable costs of delivering technology services to be managed</li> <li>• Removes potential security vulnerabilities through ongoing security patching, thereby reducing the risk of unauthorised access leading to data loss or loss of service to customers.</li> <li>• By moving to IaaS, PaaS, and SaaS offerings, we will be able to have demand-driven services which are 'pay per use'. This drives more efficient value for money for supporting ICT infrastructure.</li> <li>• Implementing flexible cloud services that can scale up and down as required, will enable us to accommodate increased data volumes and</li> </ul>

<sup>1</sup> This is the total amount of all technology and business costs required to provide these services.

	storage levels prudently and efficiently. This will enable network and business driven data and analytics and growing consumer energy resources ( <b>CER</b> ) related data.						
<b>Compliance requirements</b>	<ul style="list-style-type: none"><li>Security of Critical Infrastructure Act 2018 (<b>SOCI</b>), Security Legislation Amendment (Critical Infrastructure) Act 2021 (<b>SLACI</b>) and Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (<b>SLACIP</b>) – Requires ICT infrastructure to be kept up to date, supported and secured as a key enabler to comply with this Act.</li><li>Privacy Act 1988, Information Privacy Act 2014 - Having up-to-date and supported infrastructure as a key enabler to appropriately securing information and reducing the risk of a data breach.</li><li>Electricity Supply Act 1995 New South Wales (<b>NSW</b>) – Requires supporting ICT infrastructure and end user devices to be highly available and secure enables our critical business services to meet obligations in this Act.</li><li>National Electricity Law (<b>NEL</b>) and National Electricity Rules (<b>NER</b>) - Requires supporting ICT infrastructure and end user devices to be highly available and secure enables our critical business services to meet these Rules.</li></ul>						
<b>NPV calculations</b>	<b>Customer:</b> \$49.4 million		<b>Shareholder:</b> \$0.5 million		<b>Total:</b> \$49.9 million		
<b>Program timings</b>	<b>Program duration</b>		<b>5 years (ongoing deployments)</b>				
	<b>Program start year</b>		2025	Q1 <input checked="" type="checkbox"/>	Q2 <input type="checkbox"/>	Q3 <input type="checkbox"/>	Q4 <input type="checkbox"/>
<b>Expenditure forecast</b>	<b>\$ million</b>	<b>FY25</b>	<b>FY26</b>	<b>FY27</b>	<b>FY28</b>	<b>FY29</b>	<b>Total<sup>2</sup></b>
	<b>CAPEX</b>	(12.6)	(18.0)	(12.8)	(9.2)	(12.8)	<b>(65.3)</b>
	<b>OPEX</b>	(1.4)	(0.6)	(1.4)	(0.4)	(1.1)	<b>(5.0)</b>
	<b>Total SCS<sup>3</sup></b>	(14.0)	(18.6)	(14.2)	(9.6)	(13.9)	<b>(70.3)</b>
<b>Program type</b>	<b>ICT investment</b>		<input checked="" type="checkbox"/> Yes				<input type="checkbox"/> No
	<b>Recurrent ICT</b>		<input checked="" type="checkbox"/> Yes (various investments)				<input type="checkbox"/> No or n/a
	<b>Non-recurrent ICT</b>		<input checked="" type="checkbox"/> Yes (various investments)				<input type="checkbox"/> No or n/a
	<b>One-off SaaS opex</b>		<input checked="" type="checkbox"/> Yes (some investments)				<input type="checkbox"/> No or n/a

Table 1 Executive summary

<sup>2</sup> Due to rounding, some totals may not correspond with the sum of the separate figures.

<sup>3</sup> Cost Allocation Method (**CAM**) allocated standard control services component. Indirects are excluded.

### 3. CONTEXT

#### 3.1. Background

##### 3.1.1. Introduction

ICT infrastructure assets provide a critical technology foundation to enable the delivery of reliable, secure, and safe electricity to customers. The performance, quality and availability of these critical assets supports our day-to-day operations both in the field and in our back-office services. As our business environment, regulatory requirements, the energy market, and customer needs change, so do the requirements of the underlying ICT infrastructure supporting these.

Our ICT and infrastructure program is entirely purposed around maintaining existing capability and the routine renewal of the aging ICT infrastructure assets and associated support systems on which all of our information services run. It is “recurrent expenditure” in terms of the AER’s Guidelines on ICT expenditure assessment.

The lifecycle management of these assets is in alignment with our *ICT Asset Lifecycle Management Guidelines*, and as per vendor recommendations and industry standards for ICT infrastructure, all of these have an asset lifecycle of five years or less, and therefore are classified as mostly recurrent ICT expenditure that occurs in every regulatory control period (and in some cases multiple times throughout the period).

##### 3.1.2. Current capability

Our ICT infrastructure assets include:

- Servers;
- Storage;
- Databases;
- Backup and restoration systems;
- End user devices (laptops, PCs, and tablets);
- Telecommunications (fixed line telephony and mobile);
- ICT network infrastructure;
- Collaboration tools, and
- Supporting IT service and infrastructure management software.

Most of these assets (apart from end user devices, telecommunications, and some network infrastructure) have traditionally been physical on-premises assets, however since FY20 we have actively transitioned more of these to the cloud. This transition has been done in alignment with our *2022-29 Technology Strategy* and *Cloud Hosting Strategies* to achieve the following strategic objectives:

- Consolidate: Remove duplication and legacy systems;
- Cost Effective: With the right commercial model and best fit solutions;
- Scalable: Can readily increase capacity in line with increased demand and growth;
- Automation: Streamlined IT service management processes; and
- Quality Data: Modernised integration platforms enables consistent and reliable data sourced from core systems of record.

Timing of investments whilst considering ICT asset lifecycle management, have also been planned prudently in coordination with our cloud transition activities to enable economies of

scale and mitigate duplication across the ICT program. This approach will continue into the 2024-29 regulatory control period.

### 3.1.3. Key drivers of change

- Several ICT infrastructure assets within the current landscape will reach their end of useful asset life over the next five years;
- Increased targeted cyber threat on critical infrastructure and utilities in recent years requires active management and controls. The SOCI Act (including amendments) requires cyber security controls to be designed and operating effectively for managing cyber risk. Efficient ICT infrastructure asset lifecycle management and removing legacy ICT infrastructure, is a key enabler to successfully meeting these requirements;
- Increased data management, storage and integration requirements driven by market changes such as 5-minute settlements, and increased Internet of Things (IoT) and CER integration to the network. Core ICT infrastructure will need to be scalable to manage performance loads relative to these business, customer and data needs; and
- The trend towards a more flexible and mobile workforce at Ausgrid has increased the demand for mobility and remote user access solutions in all facets of business operations including for our staff, contractors, partners, and customers. It is anticipated that this trend will continue throughout the 2024-29 regulatory control period.

### 3.1.4. How we manage risk associated with aging ICT infrastructure assets

We currently manage the following Group Risks *11.1 – Failure of Internal ICT Services* and *4.1 - Significant Protective Security Incident*, both of which have an increased likelihood of occurring if investments to replace aging ICT infrastructure do not proceed and sufficient controls are not put in place.

For all ICT infrastructure assets approaching their end of useful asset life, the following actions are taken:

- Review options regarding extending the use of the asset beyond its useful life, and the risks and benefits of doing so;
- Review options to extend or adopt alternate support arrangements; and
- Adopt an ICT Risk Management approach as per the *ICT Digital Risk Management Branch Procedure* which, and in alignment to our Risk Appetite position.

Risk responses include:

- **End of Life Risk** - Management must ensure that all assets that become end of life have sufficient compensating controls to ensure ongoing reliability and security of the affected asset for the safe supply and restoration of power so far as is reasonably practicable.
  - Sufficient compensating controls include purchasing extended support, extended warranty, and hardware maintenance subscriptions with third parties.
- **End of Support Risk** - Management must ensure that all assets that become end of support have sufficient compensating controls to ensure ongoing reliability and security of the affected asset for the safe supply and restoration of power so far as is reasonably practicable.

The below summarises our ICT and Cyber Risk Appetite that informs the cost-efficient method that we apply to prudently manage aging ICT infrastructure assets.

### 3.1.5. ICT Risk Appetite

- The organisation will maintain ICT assets to support the safe supply and restoration of energy and to support day-to-day operations.
- The organisation is **risk neutral** in the way it:
  - Invests appropriately to facilitate the continuity of business systems that support the day-to-day operations of the organisation; and
  - Implements transformational change by embracing innovation and change (especially new technologies) that could improve the way we operate.
- However, the organisation is **risk sensitive** in the way it, so far as is reasonably practicable (**SFAIRP**), manages the availability of network control systems and manages other mission critical systems to prevent any interruptions that impact on the safe supply and restoration of energy.
- All Group Risks are required to be remediated as per Ausgrid's risk appetite statement.

### 3.1.6. Cyber Risk Appetite

The organisation will restrict unauthorised access (physical and cyber) that could result in interruptions to the availability of mission critical network control systems through the adoption of industry best practice for energy network control systems, SFAIRP.

- The organisation is **risk averse** in the way it:
  - SFAIRP, aims to achieve best industry practice to prevent unauthorised access to mission critical network control systems or critical infrastructure sites (such as the control rooms), that results in unauthorised control of the Network;
  - SFAIRP, aims to minimise instances of unauthorised or inappropriate access to its other mission critical or business systems including those resulting in loss of corporate knowledge, privacy breach, minor interruptions to continuity or significant financial loss;
  - Consistently tests our physical and cyber security effectiveness;
  - Simulate and practice effective response plans in preparation for a cyber-attack; and
  - Strives to meet appropriate maturity levels within the Australian Energy Sector Cyber Security Framework (**AESCSF**) and those proposed amendments to the SOCI, SLACI and SLACIP.
- All Group Risks are required to be remediated as per Ausgrid's risk appetite statement.

### 3.2. Problem / opportunity

With several ICT infrastructure assets reaching the end of their useful asset life over the 2024-29 regulatory control period, this increases the risk of failure of internal ICT services if proactive asset lifecycle management of these assets is not undertaken. This is impacted by:

- System failures that directly affect the continuity of supply of electricity to customers;
- Delays to asset maintenance and asset replacement programs of work;
- Degraded service level performance and/or customer satisfaction (e.g., increased incident response times and/or an inability to keep customers informed);
- Inability to satisfy regulatory reporting requirements in a timely manner;
- Penalties associated with compliance breaches (e.g., new customer connections);
- Increased vulnerability to security threats and intrusions;
- Increased reliance upon customised systems to support business operations and the resultant increase in support costs;
- Loss of vendor support and system specific expertise;
- Heightened risk that ICT infrastructure is unable to accommodate increased or new data and storage loads in support of changing market, network, and customer needs; and
- Exposure to future step function cost increases for system refreshes and replacements.

A more detailed assessment of risks associated with ICT infrastructure assets are detailed in **Appendix 1 Risk assessment**.

We take a prudent approach when renewing or upgrading ICT Infrastructure assets by assessing and recognising the enhancement opportunities available in renewing these assets as technology improvements and new releases occur in the market. We plan renewals and upgrades based on an assessment of both risks and benefits to best optimise the value from the investment. This provides us and our customers with added value for money. These enhancement opportunities include:

- Improving ICT self-service and service management capabilities through orchestration, automation, and increased business productivity;
- Increasing our defense profile against cyber threats, as new cloud offerings come with the latest security controls;
- Improving internal and external user experience with faster, more resilient, and reliable devices, data, and functionality; and
- Cost efficiencies and opportunities to save on ICT spend, including the adoption of more flexible cloud infrastructure services that enable us to pay per use. Including the ability to adopt flexible commercial models that best meet fixed and variable usage forecasts.

### 3.3. Investment objectives

Under the proposed program of work, we are aiming to:

- Maintain prudent and efficient ICT Asset Lifecycle Management of our core ICT infrastructure in support of delivering efficient, reliable, and secure energy services to customers;
- Provide fit-for-purpose ICT infrastructure to support business and customer platforms and services enabling consistent reliability, security, and availability without disruption;

- Provide fit-for-purpose end user devices (laptops, PCs, and tablets), mobile and fixed line telecommunications so our field and office workers can efficiently deliver energy services and communicating with customers and stakeholders;
- Optimise performance and cost-to-serve across the ICT infrastructure portfolio; and
- Utilise modern IaaS, PaaS and SaaS offerings which are 'pay per use' and scalable in support of growing data and storage needs.

### 3.4. Customer outcomes

Our 2022-35 Corporate Strategy has identified four key topics that will define our business into the future. Of these, the ICT Infrastructure Program is aligned to the following themes Optimised Asset and Operations and Delivering Net Zero as detailed below.



Objectives	Actions	Measures
<b>Optimised Assets &amp; Operations</b> <i>Excel at operations to deliver safe and affordable services</i> 	<ul style="list-style-type: none"> <li>• Improve operational efficiency</li> <li>• Lift our digital and data capabilities to make fast, evidence-based decisions</li> <li>• Enhance effectiveness of internal services</li> <li>• Grow revenue by leasing our assets</li> </ul>	<ul style="list-style-type: none"> <li>• Standard Control Services (<b>SCS</b>) opex</li> <li>• Delivery of network CAPEX program</li> </ul>
<b>Delivering Net Zero</b> <i>Innovate and grow our business to support a net zero future</i> 	<ul style="list-style-type: none"> <li>• Demonstrate leadership and facilitate an equitable and affordable transition to net zero</li> <li>• Enable flexibility and support a resilient and secure energy system</li> <li>• Embrace the energy transition to create revenue opportunities</li> <li>• Reduce Ausgrid's carbon footprint</li> </ul>	<ul style="list-style-type: none"> <li>• Unregulated Earnings before Interest, Tax, Depreciation and Amortization (<b>EBITDA</b>).</li> <li>• Carbon equivalent emissions</li> </ul>

Table 2 Summary of Customer Outcomes

#### • Optimised Assets & Operations:

- Allows prudent ICT Asset Lifecycle Management of our core ICT infrastructure to be maintained, in support of resiliency of our core business and network services. This will assist in mitigating degradation of performance, potential disruption/outages, and emerging security vulnerabilities linked to legacy infrastructure.

Furthermore, moving to cloud services increases asset resilience in comparison to services based within on-premises infrastructure, this enables consistent level of availability of infrastructure in supporting us to deliver energy services to our customers.

- By consolidating on-premises infrastructure and moving to more IaaS and PaaS offerings, we will be able to have demand-driven services where only service volumes

which are consumed will be charged for. This drives more efficient value for money for supporting ICT infrastructure and reduces incremental price impacts to customers.

- Implementing flexible cloud services that can scale up and down as required, will enable us to accommodate increased data volume and storage levels prudently and efficiently. This will support network and business driven data and analytics, and growing CER related data.

- **Delivering Net Zero:**

- Adoption of cloud services will also reduce our overall carbon footprint through reduced energy use.

### 3.5. Business drivers

At the end of the 2029 period, we anticipate that we will need to be able to adequately respond to the following changes within our network and business without negatively impacting cost, reliability or safety of managing our network and supporting business services:

1. Forecasted growth in data and storage needs;
2. Changing mobility and connectivity needs across our workforce, stakeholders and customers;
3. Maintain or increase defences against new and emerging cyber security threats on our ICT infrastructure; and
4. Enables value for money for our customers.

### 3.6. Compliance requirements

The proposed program of work is also required to meet regulatory obligations. The obligations are set out below.

Obligation	Description of Requirement
<b>Security of Critical Infrastructure Act</b>	<p>The <i>Security of Critical Infrastructure Act 2018 (SOCI)</i> applies in managing national security risks relating to critical infrastructure. The <i>Security Legislation Amendment (Critical Infrastructure) Bill (SLACI) 2021</i> and <i>Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP)</i> introduces new requirements:</p> <ul style="list-style-type: none"> <li>• additional security obligations for critical infrastructure assets, including a risk management program, to be delivered through sector-specific requirements, and mandatory cyber incident reporting;</li> <li>• enhanced cyber security obligations for those assets most important to the nation, described as assets of national significance; and</li> <li>• government assistance to relevant entities for critical infrastructure sector assets in response to significant cyber-attacks that impact on Australia's critical infrastructure assets.<sup>4</sup></li> </ul> <p>Enables ICT infrastructure to be kept up to date, supported and secured is a key enabler of complying with this act.</p>

<sup>4</sup> Security Legislation Amendment (Critical Infrastructure) Bill 2021 Explanatory Memorandum:

[JC000738.pdf;fileType=application/pdf \(aph.gov.au\)](#)

Security Legislation Amendment (Critical Infrastructure) Bill 2022 Explanatory Memorandum:

[JC004947.pdf;fileType=application/pdf \(aph.gov.au\)](#)

Obligation	Description of Requirement
<b>Australian Energy Sector Cyber Security Framework (AESCSF)</b>	<p>Protecting Australia's energy sector from cyber threats is of national importance. These protections maintain secure and reliable energy supplies thereby supporting our economic stability and national security. We are obligated to participate annually in an assessment within this framework.</p> <p>Requires ICT infrastructure to be kept up to date, supported and secured is a key enabler to meet our AESCSF maturity targets.</p>
<b>Record Keeping</b>	<p>The State Records Act 1998 (NSW) directs that all organisation records are stored in a way that makes sure the organisation meets its legislative and regulatory requirements. Under Section 11(1) of the State Records Act "each public office must ensure the safe custody and proper preservation of the State records that it has control of".</p> <p>Having appropriate back-up and disaster recovery infrastructure is one of the enablers for meeting this obligation.</p>
<b>Privacy Act 1988 &amp; Information Privacy Act 2014</b>	<p>The State Records Act 1998 (NSW) directs that all organisation records are stored in a way that makes sure the organisation meets its legislative and regulatory requirements. Under Section 11(1) of the State Records Act "each public office must ensure the safe custody and proper preservation of the State records that it has control of".</p> <p>Having appropriate back-up and disaster recovery infrastructure is one of the enablers for meeting this obligation.</p>
<b>Electrical (Consumer Safety) Act and the Codes of Practice</b>	<p>Obligations for the safe operation of the energy distribution network.</p> <p>Requires supporting ICT infrastructure and end user devices to be highly available and secure enables our critical business services to meet this Act.</p>
<b>National Electricity Rules (NER)</b>	<p>The operating and capital expenditure objectives<sup>5</sup> set out in the NER require us to maintain both the quality, reliability, and security of supply of standard control services and the reliability and security of the distribution network.</p> <p>Requires supporting ICT infrastructure and end user devices to be highly available and secure enables our critical business services to meet these rules.</p>

*Table 3 Summary of compliance requirements*

<sup>5</sup> See clauses 6.5.6(a) and 6.5.7(a) of the National Electricity Rules. <https://energy-rules.aemc.gov.au/ner/390>

## 4. OPTIONS

This section provides an overview of the options to address the investment need. The NPV associated with each option is also noted.

### 4.1. OVERVIEW OF OPTIONS

Two options have been considered for this investment program, which are detailed in the table below. The preferred option is Option 2: Renewal and Upgrades of ICT Infrastructure 2024-29 control regulatory period as it presents the most efficient NPV result, and acceptable level of risk required for ICT infrastructure availability, performance and security. Further information is provided within this section.

Option	Description	NPV
<b>Option 1: Base Case: (Retain current assets)</b>	<p>This option considers extending the use of existing ICT infrastructure assets beyond their useful asset life during the 2024-29 regulatory control period. Extending the use of these assets, this will require us to:</p> <ul style="list-style-type: none"> <li>• Extend existing support for legacy infrastructure;</li> <li>• Invest in and apply custom fixes and workarounds for unsupported infrastructure and supporting systems; and</li> <li>• Heightened monitoring services of legacy infrastructure – because of increased vulnerabilities.</li> </ul> <p>This option does not comply with our <i>ICT Asset Lifecycle Management Framework</i>, nor does it comply with the Group Risk appetite, and exposes us to significant risks to business operations and customers, further detailed in <b>Appendix 1</b>. Over time it will also put at risk our ability to meet our compliance obligations detailed in <b>Section 3.6 - Compliance requirements</b>.</p>	<b>(52.2) million</b>
<b>Option 2: Renewal and Upgrades of ICT Infrastructure</b>	<p>This option includes the delivery of recurrent and non-recurrent investments for renewals and upgrades of ICT infrastructure assets in alignment with our <i>ICT Asset Lifecycle Management Framework</i> detailed in</p> <p>Key initiatives include:</p> <ul style="list-style-type: none"> <li>• Renewal and upgrades of existing servers, storage, backup and restoration services, end user devices, telecommunications, ICT network infrastructure, collaboration tools, and supporting IT service management software;</li> <li>• Migration of on-premises systems to the cloud;</li> <li>• Enhancements to cloud infrastructure management capabilities; and</li> <li>• Expansion of cloud services.</li> </ul> <p>Refer to the detailed list of major ICT infrastructure investments in <b>Appendix 5</b> for further information.</p>	<b>49.9 million</b>

Table 4 Summary of options

A summary of the key differences in impact between the two options considered is detailed below.

Key Objective	Option 1	Option 2
Alignment to SOCI Act	partial	✓
Achievement of AESCSF Target State Maturity	partial	✓
Reduces risk profile of Group Risks 4.1(Cyber) and 11.1 (ICT)	X	✓
Alignment to our Risk Appetite Statement	X	✓
Alignment to our Technology Strategy	X	✓
Alignment to our Cyber Security Strategy	X	✓
Flexibility and elasticity to scale in support of increasing data and storage needs	X	✓

*Table 5 Summary of key differences between the two options*

## 4.2. OPTION 1: BASE CASE (Maintain current assets)

### 4.2.1. Description

This option considers extending the use of all our existing ICT infrastructure assets beyond their useful asset life during the 2024-29 regulatory control period.

### 4.2.2. Option 1 assumptions

The base case assumes the following:

#### Benefits:

- Reduced asset restoration times (on failure) – Third party support can assist in the restoration of an infrastructure asset in the event of a failure or significant availability, or performance issues as legacy assets continue to age; and
- Improved security posture – through the application of custom compensating controls for unsupported infrastructure (if available) and heightened Security Operations Centre (**SOC**) monitoring over known vulnerabilities.

**Risks:**

This option does not comply with our *ICT Asset Lifecycle Management Framework*, nor does it comply with the Group Risk Appetite Statement. Whilst it is prudent in applying some controls, it still exposes significant risks to our business operations and customers detailed in **Appendix 1**.

During the 2024-29 regulatory control period, this option will create:

- Escalating risk of failure as foundational ICT infrastructure and supporting services are stretched beyond their useful asset life (which negatively impacts our Group Risk 11.1 – *Failure of Internal ICT Services*);
- Heightened cyber security risks as services become end of life and patches/support are no longer available (which negatively impacts our Group Risk 4.1 - *Significant Physical or Cyber Security Incident*);
- Escalating risk of asset failure causing unplanned outages, as infrastructure services are stretched beyond their useful asset life; and
- Servers, storage, and integration services at risk of reaching capacity, and unable to handle new processing and storage loads. This negatively impacts our Group Risk 11.1 – *Failure of Internal ICT Services*, and our ability to meet changing customer and market needs.

As the impacted Group Risks will not be remediated within 6 months of being identified, this option will not meet *our Risk Appetite Statement*.

**4.2.3. Option 1 costs**

For this option the estimated operating expenditure is \$58.3 million, capital expenditure is \$0 and the market NPV of \$(52.2) million. This is made up of the following operating expenditure costs:

- Extended support costs for legacy infrastructure;
- Custom workarounds and compensating controls for unsupported servers and supporting systems; and
- Heightened SOC monitoring.

**Option 1: Capital Expenditure Cost and Scope Assumptions**

There are no capital expenditures in this option.

**Option 1: Operating Cost Assumptions**

\$ million	FY25	FY26	FY27	FY28	FY29	Total (FY25-29)
<b>Contractor services</b>	(8.8)	(10.0)	(11.4)	(13.0)	(15.1)	<b>(58.3)</b>
<b>TOTAL OPEX</b>	<b>(8.8)</b>	<b>(10.0)</b>	<b>(11.4)</b>	<b>(13.0)</b>	<b>(15.1)</b>	<b>(58.3)</b>

Table 6 Option 1 – Operating expenditure

#### 4.2.4. NPV analysis

The NPV analysis is primarily driven by the benefits of a reduced risk profile (see **Appendix 1**). The key risks impacted are business operational risks (due to infrastructure failure or disruption) and cyber security risks.

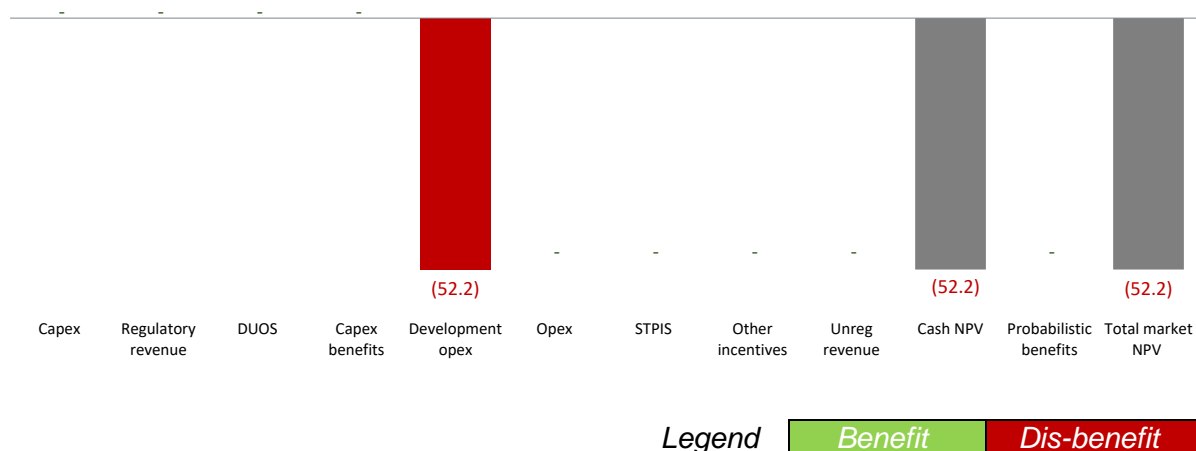


Figure 1 Option 1 - Market NPV (\$' millions, real FY24)

### 4.3. OPTION 2: Renewal and upgrades of ICT infrastructure

#### 4.3.1. Option 2 assumptions

Option 2 assumes the following:

##### Benefits:

The following probabilistic benefits have been identified:

- Patches and bug fixes resulting in ongoing vendor support and fewer planned outages;
- Avoided restoration costs associated with technology related outages;
- Reduction in the need for customisation and greater support costs for out of support systems;
- Avoided costs associated with infrastructure failure that extends the length of network outages/restoration times; and
- Critical ICT infrastructure remains up to date, supported and patched to remain secure. This is a key enabler to meeting items detailed in **Section 3.6 - Compliance requirements**.

#### 4.3.2. Option 2 costs

The estimated capital cost of Option is \$65.3 million, of which \$6.9 is non-recurrent expenditure. There is also operating expenditure of \$5.0 million, of which \$0 million is non-recurrent, over the 2024-29 regulatory control period. Further information on the costs of Option 2 is provided in the following tables. A detailed breakdown of initiatives is in **Appendix 5 2024-29 Major ICT infrastructure initiatives**.

**Option 2: Capital Expenditure Cost and Scope Assumptions**

\$ million	FY25	FY26	FY27	FY28	FY29	Total (FY25-29)
<b>Direct labour</b>	(0.8)	(1.2)	(0.8)	(0.6)	(0.8)	<b>(4.3)</b>
<b>Materials</b>	(1.7)	(2.5)	(1.8)	(1.3)	(1.8)	<b>(9.0)</b>
<b>Contractor services</b>	(10.0)	(14.3)	(10.2)	(7.3)	(10.2)	<b>(52.0)</b>
<b>Indirect cost</b>	-	-	-	-	-	-
<b>Contingency</b>	-	-	-	-	-	-
<b>TOTAL CAPEX</b>	(12.6)	(18.0)	(12.8)	(9.2)	(12.8)	<b>(65.3)</b>
<b>Non-recurrent</b>	(0.2)	(3.4)	(0.2)	-	(3.1)	<b>(6.9)</b>
<b>Recurrent</b>	<b>(12.4)</b>	<b>(14.6)</b>	<b>(12.6)</b>	<b>(9.2)</b>	<b>(9.6)</b>	<b>(58.4)</b>

*Table 7 Option 2 – Capital expenditure*

\$ million	FY25	FY26	FY27	FY28	FY29	Total
<b>Direct Labour</b>	-	-	-	-	-	-
<b>Materials</b>	-	-	-	-	-	-
<b>Contractor Services</b>	(1.4)	(0.6)	(1.4)	(0.4)	(1.1)	<b>(5.0)</b>
<b>TOTAL INVESTMENT OPEX</b>	(1.4)	(0.6)	(1.4)	(0.4)	(1.1)	<b>(5.0)</b>
<b>Non-recurrent</b>	-	-	-	-	-	-
<b>Recurrent</b>	(1.4)	(0.6)	(1.4)	(0.4)	(1.1)	<b>(5.0)</b>
<b>Ongoing new opex</b>	-	-	-	-	-	-

*Table 8 Option 2 – Operating Cost Assumptions***4.3.3. NPV analysis**

This NPV of \$49.9 million is primarily driven by the probabilistic benefits of avoided risks (see **Appendix 1**).

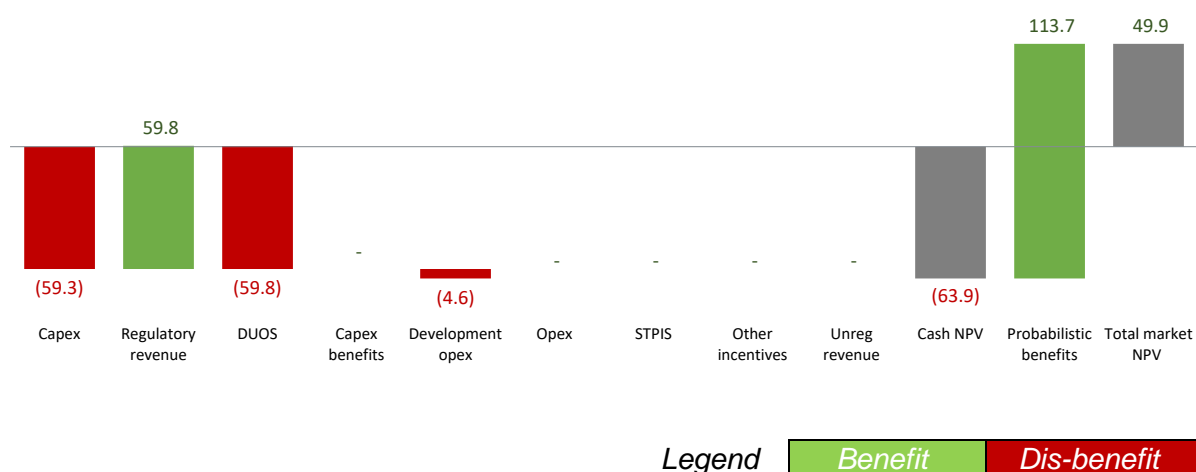


Figure 2 Option 2 - Market NPV (\$' millions, real FY24)

## 4.4. Alternative Options

We are mindful of the AER's Guidelines on ICT expenditure assessment in particular the *development of detailed options analysis of all credible options including options of various scopes and timings and identification and quantification of all relevant benefits and residual risks for each option*<sup>6</sup>.

Section 4.2 of our Technology Plan sets out how Ausgrid uses its Architectural Principles to drive customer benefits in our use of and expenditure on technology and how this is enforced through formal Governance processes. We have explored alternative options for ICT Infrastructure Management by separately considering:

- Infrastructure Services and
- End-user computing.

### 4.4.1. Infrastructure Services

In the context of this regulatory proposal, the strategies, core vendor solutions and architectural frameworks for infrastructure services (centralised data processing and storage) reflect the results of detailed options evaluation carried out as part of this governance process in 2017.

This initiative was part of our regulatory proposal for the period 2015-19 and the results of a detailed investigation into technical options presented to the Enterprise Architecture Reference Board (**EARB**), the peak architecture governance forum at the time<sup>7</sup>.

This analysis considered business needs, architectural requirements and a detailed functional and technical assessment of five ICT infrastructure service options: Current State, Bridge to Cloud, Hybrid Cloud by Operating System, Hybrid Cloud by Business Function and Hybrid Cloud by Workload - shortlisting two solutions (Bridge to Cloud and Hybrid Cloud by Workload).

Evaluating these two solutions against risk, cost, benefit and performance using our architectural principles in 2022, the Technology Review Group (which now replaces the EARB) endorsed an exit from Fujitsu Data Centres in FY26 and migration to a single third party cloud provided by Microsoft (Azure) for Ausgrid based on a comparative assessment five hosting options against cyber risk, access to new technology, complexity, scalability, resilience,

<sup>6</sup> Italics quoted from *Assessing the prudence and efficiency of the project in Consultation paper - ICT Expenditure Assessment*, AER, May 2019 p.20

<sup>7</sup> *Ausgrid Cloud Strategy*, Ausgrid, May 2017

opportunities for experimentation alignment with Ausgrid's architectural principles and a comparison of their like-for-like costs<sup>8</sup>.

Ausgrid has independently selected Microsoft's Azure cloud solutions as a target state platform for data & analytics and CRM by applying the same assessment against risk, cost, benefit, performance and user experience using our architectural principles. This is the same Microsoft solution framework that supports Azure: Ausgrid's target state platform for infrastructure services in this brief.

Microsoft Azure cloud is a contemporary solution and fit for purpose in Ausgrid's context. Migrating to an alternative solution would incur costs of data and application migration and technical integration to the rest of Ausgrid's ICT environment.

Alternative cloud solutions in the market would not meet customers' needs any better than Microsoft Azure but the cost of transitioning to them would be between 50 and 100% more than our proposed "Option 2" given the additional migration and integration costs of moving to an alternative solution.

The detailed analysis supporting EARB 2017 selection of Microsoft remains current. Given that alternative customer management options would all be more expensive than Microsoft's with no additional customer benefit, we have rejected all alternative options as part of this project brief.

#### **4.4.2. End-user computing**

End-user computing services (laptops, tablets, phones, PCs, printers, virtual desktops and audio-visual equipment) are also covered by this brief.

This brief reflects the strategy endorsed by Ausgrid's Enterprise Architecture Board in 2021 to manage risk, cost, benefit and performance using our architectural principles.<sup>9</sup> The strategy identifies a target state of Device and Print "as a Service" where the end-to-end device life cycle and print services are sourced from and managed by a single external party.

#### **4.5. Approach to Costing**

We have used revealed costs, market testing and peer review to ensure that costs for each option are efficient.

A bottom-up methodology was used to estimate the costs for each option and considered typical delivery team resource requirements, delivery partner costs and licence/subscription fees. Previous actual costs from similar projects within the ICT Infrastructure Management area were also used to estimate costs, which we have tested against industry peers directly, liaison with software vendors and through consultants' independent cost benchmarks.

Consultants and peers within Ausgrid have reviewed project labour estimates.

As outlined in section 4.2 of the Technology Strategy, a final business case development process will be used to refine scope, costs and impacts for the proposed investment. A competitive procurement activity will also be undertaken to inform costs and solution options and ensure activities undertaken represent value of money.

---

<sup>8</sup> *Cloud Hosting Strategy*, Ausgrid, June 2022

<sup>9</sup> *Digital Workplace Strategy & Roadmap*, Ausgrid, November 2021

## 5. RECOMMENDATION

### 5.1. Recommended solution

The recommended option for the 2024-29 regulatory control period is **Option 2 - Renew ICT Infrastructure**. This is the preferred option as it:

- Has the most favourable NPV of the two options at \$49.9 million;
- Demonstrates prudent and efficient management of ICT infrastructure assets in alignment with our *ICT Asset Lifecycle Management Guidelines* to enable reliable and high availability infrastructure to support us in delivering energy services to our customer;
- Reduces our exposure to Group Risks 11.1 (ICT Risk) and 4.1 (Cyber Risk), therefore reducing overall risk of disruptions in delivering energy services to customers, and/or impacts to customer data.
- Maintains compliance with SOCI and AESCSF; and
- Provides flexibility of storage and performance of ICT infrastructure to support future energy needs and enabling value for money for our customers.

### 5.2. Program delivery risks

Risk #	Risk Category	Description	Inherent Risk Level	Mitigation Plan	Residual Risk level
01	<b>New Technology Support Skills</b>	If new technology is being introduced as part of this program, there may be insufficient skills to support the new technology after the program of work has been completed.	Medium	Put plans in place to develop the required skillset is developed to enable technology to be supported in the future.	Low
02	<b>Scope Expansion</b>	Requests for additional features or capabilities not captured in the originally scope, may extend the timeline of the project.	Medium	Set scope expectations early on and define boundaries.	Low
03	<b>Costs</b>	Project Costs are estimated based upon market knowledge in FY22, and costs could increase as the project is executed in 2024-29 regulatory control period.	Medium	Develop a Gate 3 Business Case prior to executing the program and revise costs accordingly.	Low

Risk #	Risk Category	Description	Inherent Risk Level	Mitigation Plan	Residual Risk level
04	Key Program Resources	Availability of suitable cloud and ICT infrastructure resources within the local market to deliver the program of work.	Medium	Define resource requirements early and leverage existing relationships with strategic partners.	Low

Table 9 Summary of program delivery risks

### 5.3. Program assumptions

#	Type	Description
01	Resourcing	Cloud and ICT infrastructure resources will be available as required during the delivery of the ICT infrastructure program and for ongoing operations.
02	Prioritisation	Given the nature of the risks and the potential consequences of failures to business operations, this program will be prioritised accordingly (Refer to <b>Appendix 1 and 2</b> – Risk Assessments).
03	Scope	Refer to <b>Appendix 5</b> .
04	Supply Chain	Delayed delivery of equipment from suppliers is possible and contingency has been incorporated into project scheduling.

Table 10 Summary of program assumptions

### 5.4. Program dependencies

#	Program Name	Description
01	ERP Program	Timing of the ERP program may cause delays to retiring related infrastructure and may require an extension to additional support and monitoring of infrastructure. This is being managed by prioritising end of life components earlier (i.e., Metering).
02	Cyber Security Program	Inability to deliver on the renewal and upgrades of ICT infrastructure (detailed in <b>Appendix 3 - Infrastructure asset lifecycle management guidelines</b> ) within acceptable asset lifecycle periods may cause exposures to cyber security risks. This includes vulnerabilities within legacy and unsupported technologies, and this may have a direct impact on the goals and targets of the Cyber Security Program. This may require elevated cyber security monitoring and services to manage these risks.
03	Data to Intelligence	This program will help establish the cloud storage and integration capabilities required to support scaling data needs.

Table 11 Summary of program dependencies

**5.5. Business area impacts**

#	Impacted Group	Description
<b>01</b>	All Ausgrid	The rollout of the End user devices refresh will impact all teams across the business. This will be done in a logical order to avoid business disruptions.
<b>02</b>	All Ausgrid	Where possible the program initiatives will be managed with go-lives that minimise the amount of (or any) disruption to business operations due to technology transition downtimes (e.g., planned out of hours etc.)
<b>03</b>	Specific Groups / Functions	Any asset upgrade or change requires appropriate ICT Change Management processes to be followed. Impact to customer facing services or employees will be scheduled optimally to minimise impact and risk of unplanned outages.

*Table 12 Summary of program dependencies*

## 6. GLOSSARY

Shortened Form	Extended Form
<b>ADMS</b>	Advanced Distribution Management System
<b>AESCSF</b>	Australian Energy Sector Cyber Security Framework
<b>CAM</b>	Cost Allocation Methodology
<b>Capex</b>	Capital Expenditure
<b>CER</b>	Consumer Energy Resources
<b>CCPs</b>	Cloud Connection Points
<b>CMDB</b>	Configuration Management Database
<b>DNSP</b>	Distribution Network Service Provider
<b>EARB</b>	Enterprise Architecture Review Board
<b>EBITDA</b>	Earnings before Interest, Tax, Depreciation and Amortization
<b>EOL</b>	End-of-Life
<b>FY25-29</b>	Financial Year 2025 to Financial Year 2029
<b>ICT</b>	Information, Communications and Technology
<b>IoT</b>	Internet of Things
<b>IaaS</b>	Infrastructure-as-a-Service
<b>JRE</b>	Java Runtime Environment
<b>LAN</b>	Local Area Network
<b>NEL</b>	National Electricity Law
<b>NER</b>	National Electricity Rules
<b>NPV</b>	Net Present Value
<b>Opex</b>	Operating Expenditure
<b>OS</b>	Operating System
<b>OT</b>	Operational Technology
<b>PaaS</b>	Platform-as-a-Service
<b>RPO</b>	Recovery Point Objective

Shortened Form	Extended Form
<b>RTO</b>	Recovery Time Objective
<b>SaaS</b>	Software-as-a-Service
<b>SAN</b>	Storage Area Network
<b>SCS</b>	Standard Control Services
<b>SFAIRP</b>	So Far as Is Reasonably Practicable
<b>SLA</b>	Service Level Agreement
<b>SLACI</b>	Security Legislation Amendment of Critical Infrastructure Act 2021
<b>SLACIP</b>	Security Legislation Amendment of Critical Infrastructure Protection Act 2022
<b>SOC</b>	Security Operations Centre
<b>SOCI</b>	Security of Critical Infrastructure Act 2018
<b>SOE</b>	Standard Operating Environment
<b>SVC</b>	Storage Volume Controller
<b>TSM</b>	Tableaus Services Manager
<b>VM</b>	Virtual Machine
<b>VOIP</b>	Voice Over Internet Protocol
<b>WAN</b>	Wide Area Network

*Table 13 Glossary definitions in extended form*

## 7. APPENDICES

### Appendix 1 Risk assessment – Option 1

**Table 14 - Option 1 - Key risks and residual risk position by 2029** summarises the inherent risks which could be experienced by the end of the coming regulatory control period of (2029) if the base case (counterfactual) option is selected.

Option 1 does not reduce the likelihood or impact of risks R1 and R2 materialising. By 2029, it is **Likely** both risks will materialise causing **Major** impact to the organisation.

The equivalent risk analyses provided with the recommended option (Option 2) have been conducted with respect to effectiveness of mitigating the below base case risks. This assessment has been undertaken in alignment with the Ausgrid Groups Risk Management Framework.

Risk Description	Inherent Risk 2029	Nature of Mitigation	Residual Risk 2029
<b>R1 – Cyber Security</b> With the inability to progress major system release upgrades, which can include access control and security updates, coupled with the growing sophistication of cybersecurity attacks, there is increasing potential for: <ul style="list-style-type: none"> <li>• Undetected data corruption or manipulation;</li> <li>• Disclosure of personal or sensitive information;</li> <li>• Loss of control of Mission and Business Critical ICT Services;</li> <li>• Threat of hostile takeover; and</li> <li>• Malicious access to Operational Technology (OT) networks and Advanced Distribution Management System (ADMS)</li> </ul>	<b>High</b>	Cyclic renewal of technology components with modern capability and application of cyclic updates reduces threat vulnerability.	<b>High</b>

<p><b>R2 – Business Operational Impact</b></p> <p>Inability to restore corporate data and systems from backup in the event of requiring disaster recovery.</p> <p>Information backup and system restores can be hampered by numerous factors such as backup type, link speed, data corruption and backup/restore time.</p> <p>A failure to meet Recovery Time Objective (<b>RTO</b>) and Recovery Point Objective (<b>RPO</b>) times can be very disruptive to a business, but failure to restore at all can be catastrophic, affecting all of business and customers.</p>	<p><b>High</b></p>	<p>Cyclic renewal of storage, server infrastructure and disaster recovery solutions with modern capability will enable contemporary methods in data protection, integrity checking, security and throughput are utilised reduces the likelihood and consequences if this risk materialised.</p>	<p><b>High</b></p>
--	--------------------	---	--------------------

*Table 14 Option 1 - Key risks and residual risk position by 2029*

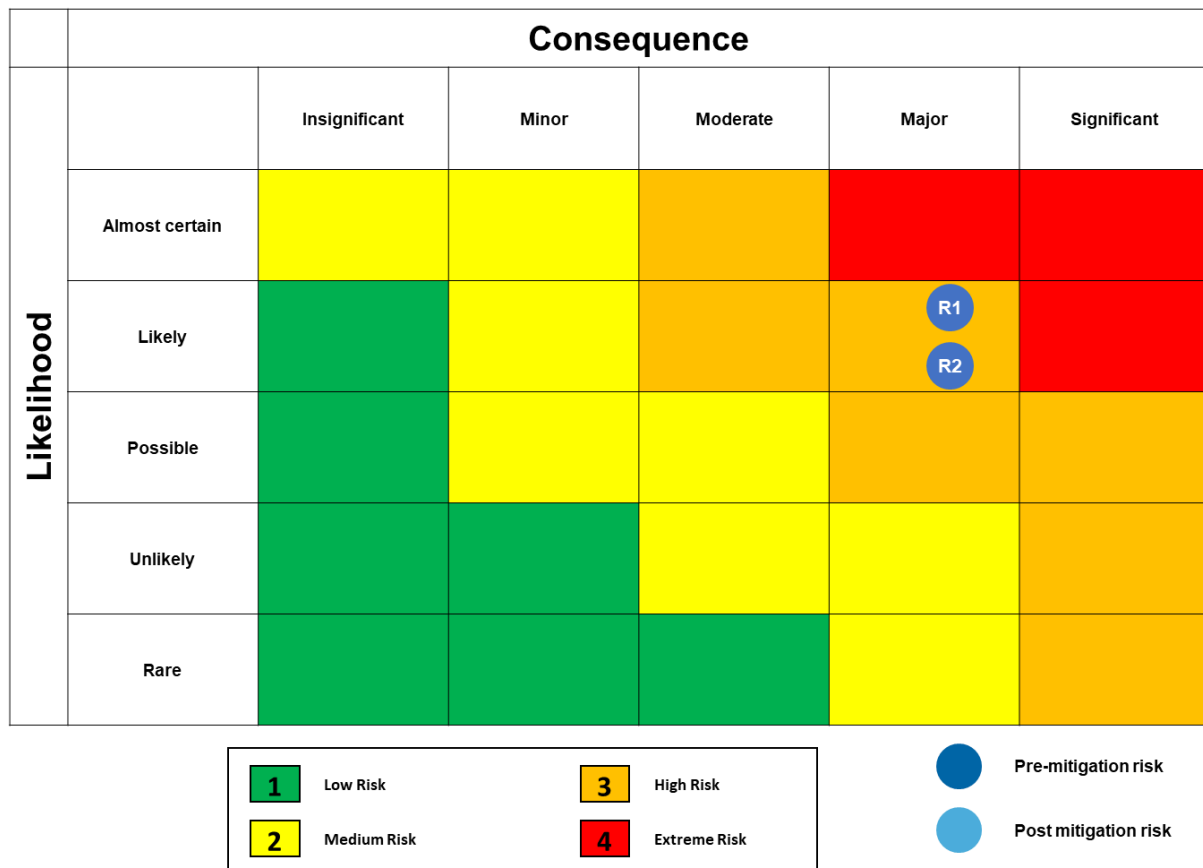


Figure 3 Change in risk position with Option 1 by 2029

## Appendix 2 Risk assessment – Option 2

**Table 15 - Option 2 - Key risks and residual risk position by 2029** summaries the inherent risks which are reduced by the end of the coming regulatory control period of (2029) if option 2 is selected. This assessment has been undertaken in alignment with the Ausgrid Group's Risk Management Framework.

Option 2 reduces the likelihood / impact of risks R1 and R2 materialising. By 2029, it is **Possible** both risks will materialise causing **Moderate** impact to the organisation.

The primary benefit of undertaking the proposed ICT infrastructure investment program is the reduced risk of a successful cyber-attack or failure/disruption of our ICT infrastructure.

Risk Description	Inherent Risk 2029	Nature of Mitigation	Residual Risk 2029
<b>R1 – Cyber Security</b> With the inability to progress major system release upgrades, which can include access control and security updates, coupled with the growing sophistication of cybersecurity attacks, there is increasing potential for: <ul style="list-style-type: none"> <li>• Undetected data corruption or manipulation;</li> <li>• Disclosure of personal or sensitive information;</li> <li>• Loss of control of Mission and Business Critical ICT Services;</li> <li>• Threat of hostile takeover; and</li> <li>• Malicious access to Operational Technology (OT) networks and Advanced Distribution Management System (ADMS)</li> </ul>	<b>High</b>	Cyclic renewal of technology components with modern capability and application of cyclic updates reduces threat vulnerability.	<b>Medium</b>

<b>R2 – Business Operational Impact</b> Inability to restore corporate data and systems from backup in the event of requiring disaster recovery. Information backup and system restores can be hampered by numerous factors such as backup type, link speed, data corruption and backup/restore time. A failure to meet <b>RTO</b> and <b>RPO</b> times can be very disruptive to a business, but failure to restore at all can be catastrophic, affecting all of business and customers.	<b>High</b>	Cyclic renewal of storage, server infrastructure and disaster recovery solutions with modern capability will enable contemporary methods in data protection, integrity checking, security and throughput are utilised reduces the likelihood and consequences if this risk materialised.	<b>Medium</b>
--	-------------	--	---------------

Table 15 Option 2 - Key risks and residual risk position by 2029.

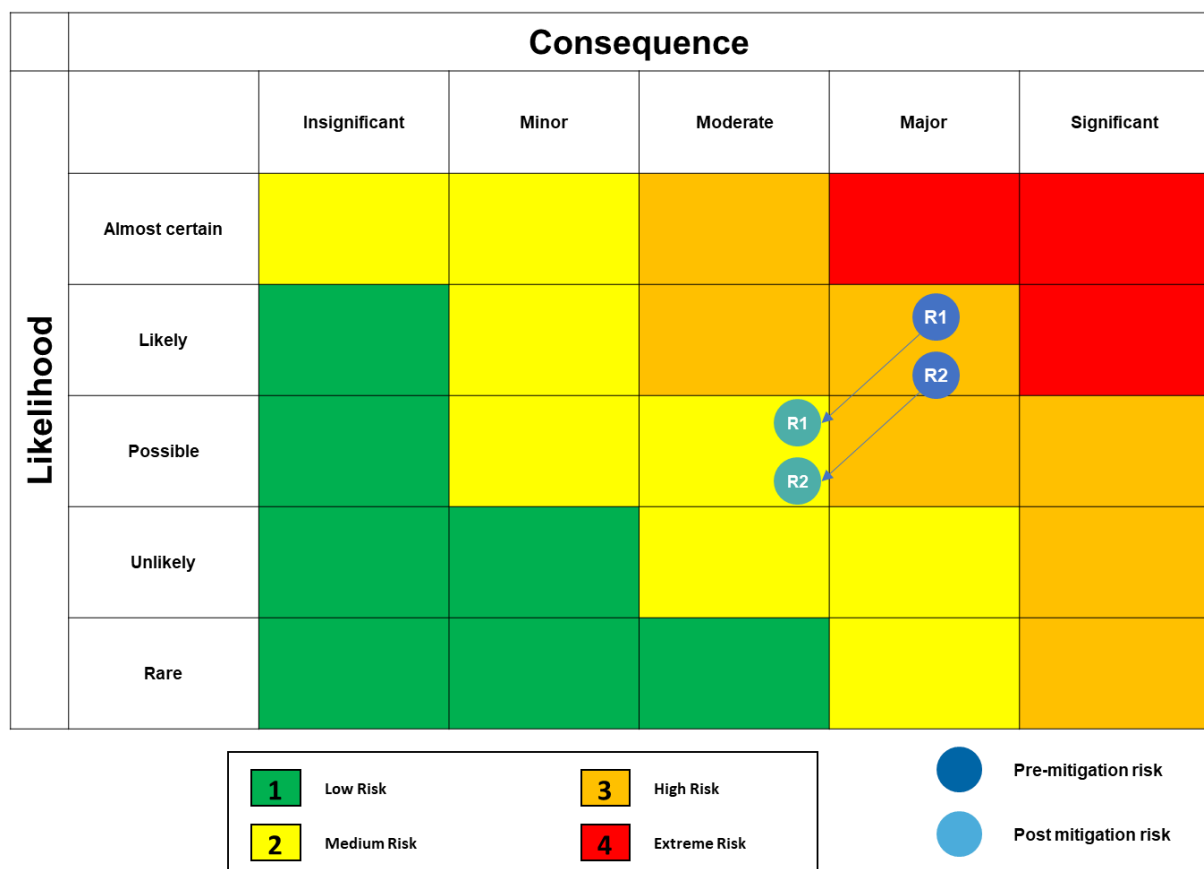


Figure 4 Change in risk position with Option 2 by 2029

### Appendix 3 Infrastructure asset lifecycle management guidelines

The following table provides an overview of the asset lifecycles adopted by us in the management of our ICT infrastructure assets.

Asset Category	Asset Class	Asset Lifecycle Management Guideline	Forecast Replacement Age
<b>Endpoint Devices</b>	Laptop (Standard)	4-year warranty / maintenance agreement. Devices are replaced through a cyclic renewal program or on failure	4 years
	Laptop (High Performance)	3-year warranty / maintenance agreement. Devices are replaced through a cyclic renewal program or on failure	3 years
	Printer	Managed service	Service Level Agreement (SLA)
	Desk Phone	Voice Over Internet Protocol (VOIP) handsets <sup>10</sup>	5 years
	Mobile Phone	Corporate data plan and outright ownership	3 years
	iPads	4-year warranty / maintenance agreement. Devices are replaced through a cyclic renewal program or on failure	4 years
<b>Collaboration Technology</b>	Video Conferencing Units	Devices are replaced through a cyclic renewal program or on failure	5 years
	Meeting Room Displays	Devices are replaced through a cyclic renewal program or on failure	5 years
<b>Server Technology</b>	Physical Servers	Devices are to be replaced prior to the vendor announced End of Life or End of Primary Support. Devices should no longer be in use if there are no more firmware updates available due to Security risks	5 years
	Virtual Machine (VM) Elastic Sky X Integrated (ESXi) Hardware	Devices are replaced with virtualised server infrastructure (where possible) upon identified obsolescence following extended warranty period which is typically 5 years	5 years
<b>High-Capacity Storage Facilities</b>	High-Performance Solid-State Storage	Devices are replaced following warranty expiry	5 years
	Storage Area Network (SAN) Storage	Devices are replaced following warranty expiry	5 years
	Backup Facilities	Backup appliances on-premises are replaced following warranty expiry	5 years
<b>Infrastructure Operating Software</b>	Server Operating Systems	Software is periodically upgraded to vendor supported levels to ensure availability of patching, security updates and compatibility with corporate systems.	4 years
	Database Management Systems		4 years
	Server Virtualisation Software		4 years

<sup>10</sup> Note these may be discontinued dependant on demand and convergence to alternate voice services.

Asset Category	Asset Class	Asset Lifecycle Management Guideline	Forecast Replacement Age
	Application Virtualisation Software	Software is periodically upgraded to vendor supported levels to ensure availability of patching, security updates and compatibility with corporate systems.	4 years
	IT Monitoring Systems	updates and compatibility with corporate systems.	4 years
<b>Corporate Networking Infrastructure</b>	Local Area Network ( <b>LAN</b> ) Devices	Devices are replaced in line with vendor end of support / end of life designations, to ensure vendor support is available (i.e., availability of active patching and security updates).	5 years
	Data Centre, Wide Area Network ( <b>WAN</b> ) and Perimeter Devices	Devices are replaced in line with vendor end of support / end of life designations, to ensure vendor support is available (i.e., availability of active patching and security updates).	5 years

*Table 16 Infrastructure asset lifecycle management guidelines*

## Appendix 4 Overview of infrastructure lifecycle – end of life (EOL) dates

Investment	Implemented Date	EOL Date	2024-29 Start Date
iPhones	2021	2025	FY25
iPads	2021	2025	FY25
5 min Metering storage and VM expansion	2017	2023	FY26
Configuration Management Database ( <b>CMDB</b> ) Automation Update	2023	SaaS	FY25
Service catalogue enhancement	2018	SaaS	FY25
Decommission of shared network drives	2012	2022	FY26
DR automation	2023	2026	FY25
Java Runtime Environment ( <b>JRE</b> ) mitigate exposure	2019	2024	FY25
NetScout Azure deployment	2023	2027	FY27
Alemba Service Manager	2017	2022	FY26
PC refresh	2017	2022	FY25
V7000 storage used for Tableaus Services Manager ( <b>TSM</b> ) refresh	2015	2024	FY25
Storage capacity upgrade V7200	2019	2024	FY25
pSeries equipment upgrade EOL FY23	2017	2023	FY25
Operating System ( <b>OS</b> ) Network landscape upgrades	2022	2027	FY25
Windows server upgrades	2012	2023	FY27
Windows 10 upgrade to 11	2017	2025	FY25
Cloud remote access services	2023	PaaS	FY26
High availability of Cloud Connection Points ( <b>CCPs</b> )	2023	2028	FY26
Linux 7 EOL upgrades	2018	2024	FY25
Remediate Window Applications from Windows 10 for Windows 11	2017	2025	FY25
SAN Volume Controller ( <b>SVC</b> ) EOL Hardware upgrade	2017	2025	FY25
Business Insights Platform ( <b>BIP</b> ) Improvements	2017	NA	FY25
Data Centre Core Network Refresh phase 2	2023	2028	FY27
Wi-Fi refresh and Optimisation	2023	2028	FY25
Infoblox upgrade	2023	2028	FY25

Table 17 Overview of infrastructure lifecycle –end of life (EOL) dates

## Appendix 5 2024-29 Major ICT infrastructure initiatives

Investment	Description	ICT Investment FY25-29 (FY24 Real \$m) <sup>11</sup>	Recurrent / Non-Recurrent Classification
Azure Infrastructure Enhancements	Various enhancements to the current Azure footprint.	2.4	Recurrent
Cloud Remote Access Services	Upgrade to existing cloud remote access services	1.9	Recurrent
Future of Fixed Telephony	Take the approved strategy thorough tender and delivery of the replacement of the end of life / end of support Alcatel System with new cloud-based technology.	1.1	Recurrent
IT Mobility Solution Refresh-iPads	Recurrent replacements of our iPad fleet	1.7	Recurrent
IT Mobility Solution Refresh -iPhones	Recurrent replacement of our mobile (iPhone) fleet	2.3	Recurrent
High Availability within the CCPs	Install Redundant Fibre between the cloud providers and data centers. Implement High Availability (HA) for Palo Alto firewalls, Juniper routers and Nokia Switches. Deploy a secure management network.	1.6	Recurrent
Windows Upgrade (next version)	This will be recurrent bi-annual upgrades of our core standard operating environment (SOE)	1.9	Recurrent
PC Refresh (Annual)	Recurrent replacement of our PC Fleet as key tools of trade for our employees.	11.2	Recurrent
ESX Host Upgrade Part 2	Recurrent upgrade of our existing ESX Host	1.6	Recurrent
Data Centre Decommissioning	decommissioning as part of the data centre exit strategy	3.0	Non-Recurrent – Maintain Services
pSeries Equipment Upgrade	Replace pSeries equipment that has reached the end of its useful life.	2.9	Recurrent
Remediate Windows Applications Next version	Remediation activities for Windows Applications Next.	1.6	Recurrent
Storage Capacity Upgrade V7200-	Upgrade V7200 storage capacity to meet forecasts.	1.7	Recurrent
Windows Server Upgrades	Replace servers that have reached the end of their useful life.	2.0	Recurrent
Linux 7 End of Life Upgrades – (Non-S/4HANA)	Replace servers that have reached the end of their useful life.	1.6	Recurrent
V7000 Storage Refresh	Replace storage that is at the end of its useful life.	3.5	Recurrent
OS Network landscape upgrades	Upgrade OS network services to enable scaling.	2.8	Recurrent
5-minute metering storage and VM expansion	Expansion to allow for additional data volumes	2.4	Non-recurrent
Minor ICT Infrastructure Investments	This includes 5 Minute Metering Additional Central Processing Unit (CPU), Active Directory Schema Upgrade, Central Logging and Automation, Data Centre Firewall, Data Centre Core Network Refresh, End User Computing Peripherals, Infoblox, Java Runtime Environment, Message hub Upgrade, VMware Hypervisor, P-305 Decommission Shared Network Drives, Printer Refresh, SAN	23.1	Recurrent and Non-recurrent

<sup>11</sup> SCS only.

	Switch Refresh, SVC Hardware Upgrade, WIFI Refresh and Optimisation and Window Servers Upgrades		
	<b>TOTAL FORECASTED INVESTMENT</b>	<b>70.3</b>	

*Table 18 Major ICT infrastructure initiatives*