



# Business Case: ICT Recurrent - Client Device Refresh

SA Power Networks 2025-2030 Regulatory Proposal

Supporting document [5.12.5]

January 2024



**Empowering** South Australia

# Contents

Glossary.....	3
<b>1. About this document.....</b>	<b>4</b>
1.1 Purpose.....	4
1.2 Expenditure category .....	4
1.3 Related documents.....	4
<b>2. Executive summary .....</b>	<b>5</b>
<b>3. Background .....</b>	<b>7</b>
3.1 The scope of this business case.....	8
3.2 Our performance to date.....	10
3.3 Drivers for change .....	12
3.4 Industry practice.....	13
<b>4. The identified need .....</b>	<b>14</b>
<b>5. Comparison of options .....</b>	<b>15</b>
5.1 The options considered .....	15
5.2 Options investigated but deemed non-credible .....	16
5.3 Analysis summary and recommended option .....	16
5.3.1 Options assessment results.....	16
5.3.2 Recommended option .....	16
5.4 Scenario and sensitivity analysis .....	17
5.5 Option 1: Do nothing different (Risk-based refresh at current refresh rates).....	18
5.5.1 Description .....	18
5.5.2 Costs.....	18
5.5.3 Risks .....	20
5.5.4 Quantified benefits .....	20
5.5.5 Unquantified benefits .....	20
5.6 Option 2: Faster device refresh for additional risk reduction.....	21
5.6.1 Description .....	21
5.6.2 Costs.....	21
5.6.3 Risks .....	22
5.6.4 Quantified benefits .....	22
5.6.5 Unquantified benefits .....	22
5.7 Option 3: 20–25 RCP allowance level.....	22
5.7.1 Description .....	22
5.7.2 Costs.....	22
5.7.3 Risks .....	24
5.7.4 Quantified benefits .....	24
5.7.5 Unquantified benefits .....	24

<b>6. Deliverability of recommended option.....</b>	<b>25</b>
<b>7. How the recommended option aligns with our engagement .....</b>	<b>26</b>
<b>8. Alignment with our vision and strategy.....</b>	<b>27</b>
<b>9. Reasonableness of cost estimates .....</b>	<b>28</b>
<b>10. Reasonableness of input assumptions.....</b>	<b>30</b>
<b>A. Appendix A – Cost models .....</b>	<b>31</b>
<b>B. Appendix B – Risk assessment .....</b>	<b>32</b>

## Glossary

<b>Acronym / term</b>	<b>Definition</b>
<b>AER</b>	Australian Energy Regulator
<b>CAD</b>	Computer-aided design
<b>Capex</b>	Capital expenditure
<b>ICT</b>	Information and communication technology
<b>IT</b>	Information technology
<b>NER</b>	National Electricity Rules
<b>NPV</b>	Net present value
<b>Opex</b>	Operating expenditure
<b>RCP</b>	Regulatory control period
<b>SP-1</b>	Security Profile 1

# 1. About this document

## 1.1 Purpose

The purpose of this document is to provide the business case and justification for the ongoing refresh of client devices for the 2025–30 Regulatory Control Period (**RCP**). Client devices include desktops, laptops, mobile devices (phones, tablets), tough devices, plotters, and video conferencing equipment that support business activities and enable the delivery of energy services to customers.

## 1.2 Expenditure category

- Non-network Information and communication technology (**ICT**) capital expenditure (**capex**): Recurrent

## 1.3 Related documents

**Table 1: Related documents**

<b>Title</b>	<b>Author</b>	<b>Version / date</b>
5.12.1 - IT Investment Plan 2025-30	SA Power Networks	Jan 2024
Digital and Data Strategy	SA Power Networks	Jan 2024
IT Asset Management Plan	SA Power Networks	Jan 2024
5.12.23 - ICT Forecasting Methodology and Business Case Structure	SA Power Networks	Jan 2024

## 2. Executive summary

This program delivers the recurrent replacement of client devices (laptops, PCs, mobile phones, tablets etc) to mitigate risks from declining reliability and performance as these devices age, become unreliable, require increased maintenance and ultimately fail. This business case recommends spending **\$32.1 million<sup>1</sup> capital** expenditure to continue to proactively refresh the oldest client devices, consistent with standard industry practice, at current and historical refresh rates.

This recommendation seeks to ensure that our client devices are fit for purpose, secure and reliable to ensure SA Power Networks can maintain our existing services and manage service risk. Devices ensure our workforce can respond to customer and network issues, receive job information in the field, access critical asset and service information, and update customers with timely information on progress. They enable a hybrid workforce, facilitate efficient collaboration between workers located at different sites and at home, and play a critical role in keeping our workforce safe in a diverse and challenging environment.

Unreliability of client devices presents a significant risk to business operations and safety and limits the effectiveness of individuals and work groups in achieving operational objectives and commitments. Aged and unreliable devices can also result in higher maintenance costs, a requirement for additional support staff, difficulty embedding work activities and processes, increased downtime, and increased vulnerability to cyber-attacks. This impacts our ability to respond to customers, maintain our network and deliver energy services. If this initiative did not proceed, our customers would experience a decline in service performance as staff within the business lose the capability to manage the electricity network and assets.

The recommended investment of \$32.1 million over the 2025–30 RCP is \$1.9 million (6%) above investment levels over the last five-year period<sup>2</sup>. The increase relates to the continued transition to hybrid working following COVID (ie, in-cycle refresh of the remaining desktop computers with portable devices), as well as a one-off purchase of new tablet docks in vehicles due to the discontinuation of our existing tablet models. This forecast is considered the most efficient amount that enables the risks associated with aged and failing client devices to be addressed.

Other options considered were:

- **Refreshing devices at a faster rate than current practice (\$35.4 million):** While this level of investment further reduces the risks associated with aged and unreliable client devices, it does so for a higher cost than the chosen option.
- **Investing at the current period regulatory allowance level (\$26.4 million):** This level of investment would require us to utilise our client device fleet past the point where the identified risks can be mitigated. Our current service levels would decrease as device failure rates increase and this would ultimately result in a higher net cost to customers.

The recommended option was selected because it:

- is the most cost-effective option for maintaining our existing systems and services at an acceptable level of risk
- provides for our continued transition to hybrid working, which has become the business norm.

Table 2 provides the options assessment summary.

<sup>1</sup> Unless otherwise specified, all financial figures in this business case are in real June 2022 dollars.

<sup>2</sup> 2018/19 – 2022/23.

**Table 2: Client Device Refresh options assessment summary, (\$m Jun 2022 real)<sup>3</sup>**

Option	2025–2030 costs			10-year estimates		Residual risk rating <sup>4</sup>
	Capex	Opex	Total	Benefits	NPV <sup>5</sup>	
<b>Option 1</b> – Current risk-based refresh	32.1	-	32.1	n/a	-51.4	Medium
<b>Option 2</b> – Faster device refresh	35.4	-	35.4	n/a	-57.8	Low
<b>Option 3</b> – Refresh at current period allowance	26.4	-	26.4	n/a	-43.3	High

<sup>3</sup> Note: Totals presented in tables throughout this document may not exactly match the sums of individual figures due to rounding.

<sup>4</sup> The overall risk level for each option after the proposed option is implemented. Refer to [Appendix B](#) – risk assessment for details.

<sup>5</sup> Net present value (NPV) of the proposal over 10-year cash flow period from 1 July 2025 to 30 June 2035, based on discount rate of 4.05%.

### 3. Background

SA Power Networks manages a large, geographically dispersed and diverse distribution network, covering 178,000 square-kilometres across 458 sites, including 42 offices and depots and over 400 substations – see Figure 1.

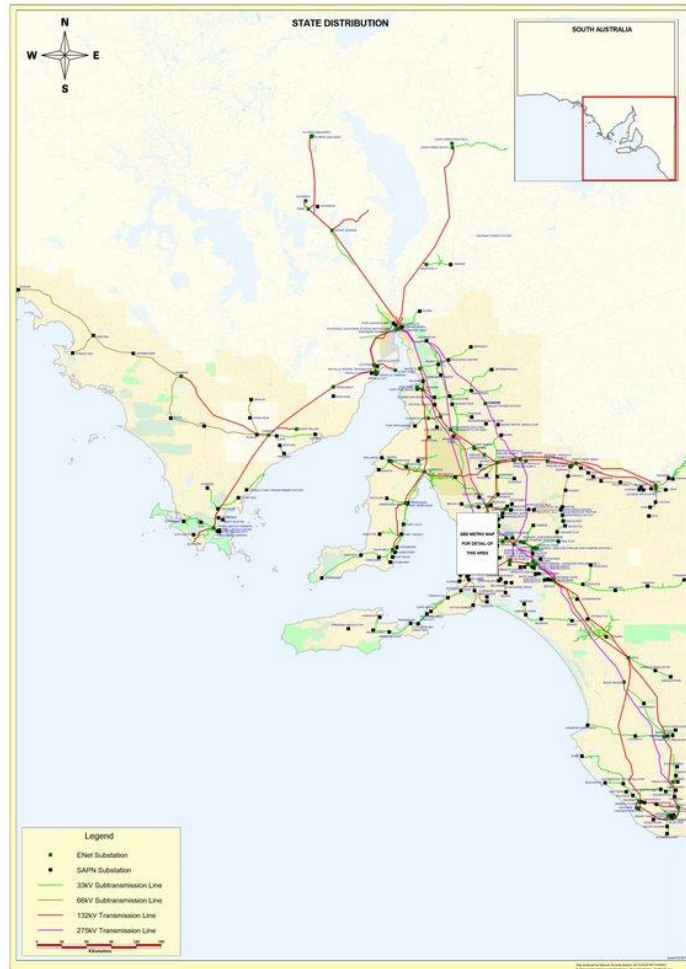


Figure 1: SA Power Networks statewide distribution network, showing offices and depots

Our workforce uses client devices (such as computers, tablets and phones) to perform their roles and manage the network effectively. These devices enable efficient delivery of customer and network services by ensuring staff can respond to customer and network issues, receive job information in the field, access critical asset and service information, and update customers with timely information on progress. They also keep our workforce safe in a diverse and challenging environment by providing access to accurate data and warnings, including under extreme conditions, such as weather-related outages and bushfires.

All devices need to be fit for purpose, secure and reliable to perform their function. As devices age, reliability and performance declines, with potential consequences of higher maintenance costs, additional support staff, increased downtime, and increased vulnerability to cyber-attacks. This impacts our ability to respond to customers, maintain our network and deliver energy services.

In addition to the risk of failure or poor performance, cyber security breaches and information loss can occur when devices are not capable of handling the latest security requirements or cannot be updated to the latest operating system or software versions.



Device failure rates systematically increase over time, such that, while there are low failure numbers in the first couple of years, these increase logarithmically in later years. This is described in a recent Gartner paper, which states that, “the goal should be to replace devices before the probability of failures increases significantly”<sup>6</sup>. This approach results in lower costs to customers over the long term and is shown in Figure 2.

**Life Cycle Based on Likelihood of Device Failure**

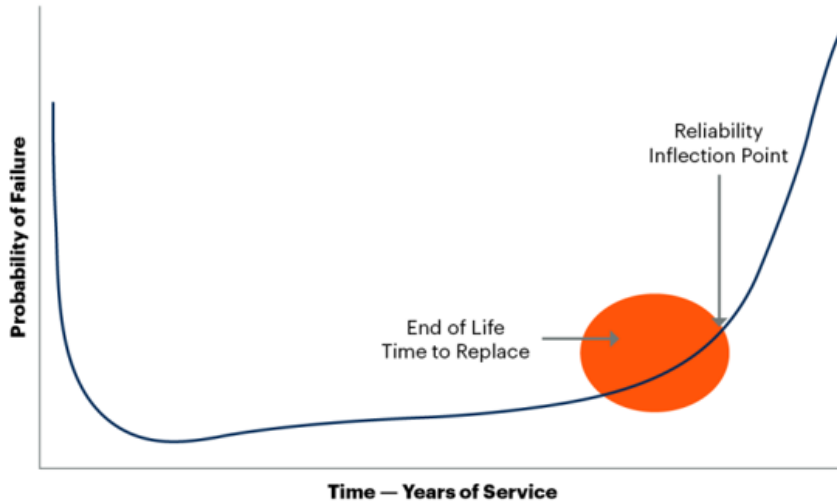




Figure 2: Gartner Life cycle based on likelihood of device failure chart








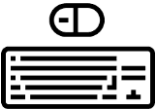

Replacing devices past this optimal point creates situations where devices fail in critical events, such as during bushfires, creating an unacceptable level of risk for our services and our people. As a result, our approach to device management is the proactive replacement of devices around this optimal point. This requires defining an appropriate standard life for each type of device. We then moderate this by stretching these lives, where prudent and reasonable to do so, and where risks can be mitigated. This approach minimises the impact of device issues on the organisation.

**3.1 The scope of this business case**

This business case covers purchasing and installing the rolling refresh program for client devices, which includes both computing and communication devices. Specifically, the program covers the following devices.

Client device type	High-level use case
 Laptops/tablets	<ul style="list-style-type: none"> <li>Provisioned to enable mobility where users need to work on the road and from multiple sites.</li> <li>Specialised Tool of Trade devices provisioned for working with monitoring and control devices on the electrical network.</li> </ul>
 Desktops	<ul style="list-style-type: none"> <li>Standard desktops are available in depots and other locations and are used for shared purposes or for users who work from a single site.</li> <li>Power desktops are used for activities heavily reliant on high data volumes and processing power (eg, computer-aided design (CAD)).</li> </ul>

<sup>6</sup> [Recommended Life Span 746332 ndx.pdf \(gartner.com\)](#).

 Phones	<ul style="list-style-type: none"> <li>• Standard provision to the majority of staff.</li> </ul>
 Tough devices	<ul style="list-style-type: none"> <li>• Provisioned for field workers due to their operating environment driving higher reliability needs. Used in the field, in-vehicle, and in workshops.</li> </ul>
 Monitors	<ul style="list-style-type: none"> <li>• Provisioned for use with laptops and desktops.</li> </ul>
 Hubs and docks	<ul style="list-style-type: none"> <li>• Docking stations used in conjunction with laptops and tablets.</li> </ul>
 Meter reading devices	<ul style="list-style-type: none"> <li>• Devices used by meter readers to collect and report electricity meter readings at customer properties.</li> </ul>
 Video conferencing devices	<ul style="list-style-type: none"> <li>• Large displays (eg, televisions) used in meeting rooms and as digital displays and signage.</li> <li>• Projectors in meeting rooms (or for mobile use).</li> <li>• Video conferencing capabilities installed in meeting rooms.</li> <li>• Large monitors for use in places such as the Network Operations Centre.</li> </ul>
 Plotters	<ul style="list-style-type: none"> <li>• Large format printers used to print design drawings.</li> </ul>
 Peripherals	<ul style="list-style-type: none"> <li>• Annual fund for replacement of any required peripherals, used in conjunction with the above devices (eg, mice, keyboards, headsets etc).</li> </ul>
 Miscellaneous IT refresh	<ul style="list-style-type: none"> <li>• Funding for device evaluation, loss or failure of devices outside of the replacement cycle.</li> </ul>

The types of costs covered by the investment includes:

- Prudent replacement of end-of-life hardware and software;
- Timely deployment/handover of new or replaced computing devices;
- Timely upgrades to device management and support tools;
- Ongoing governance on the devices

- Provision to evaluate new devices and technologies, and ensure the business is maximising long-term value in the purchase of client devices.

The following items are excluded from the scope of this business case:

- Operating expenditure related to maintaining and supporting client devices (including support costs for client devices and costs for patching and maintaining major operating system updates on devices), which are covered by base year opex.
- Device costs for enabling new business capability, which are covered within estimates for projects that deliver such new capability<sup>7</sup>.
- Refresh costs for communication capability from vehicles, which are met as part of vehicle fit out<sup>8</sup>.

### 3.2 Our performance to date

The SA Power Networks client devices business case for the current RCP was approved for the full \$25.8 million proposed, which was a reduction from the \$29.9 million spent in the 2015–20 RCP. This lower forecast spend for the current RCP was driven by an expected rationalisation in the number of devices, reflecting our proposed role-based approach.

However, the end of the 2015–20 RCP saw significant change to the business environment, which resulted in the expected reduction in devices not occurring. The global COVID-19 pandemic resulted in changes that were not considered at the time of the previous business case, in particular:

- the requirement for all staff to have individually assigned devices, rather than shared devices, to address both health and safety and cyber security risks; and
- pandemic work restrictions resulting in our whole office-based staff being required to work full-time from home for a significant period, and which will continue for many roles going forward.

#### Cyber security and safety driving an increased number of devices

The majority of our field workforce are mobile, and work in challenging – and often remote – locations and environmental conditions. Their devices are part of a worker’s essential safety equipment used for sourcing critical safety information, and for receiving and sending work and activity-related updates. For example, field workers utilise tough devices for entering timely and accurate data on restoration and close-out times, which is used to inform customers.

Following the start of the pandemic, shared devices for field staff quickly became inappropriate. This was due to two factors:

- the need for safe physical work practices driving a requirement for each staff member to have their own individual device
- operational risks associated with the potential unavailability of key staff and devices, for example, those who managed network control operations.

Additionally, cyber security requirements have increased in recent years, driven by the changing risk profile and increased legislative requirements. We now have significantly higher requirements regarding control

---

<sup>7</sup> This includes device costs expected for the Network Investment Uplift Program.

<sup>8</sup> Note that this business case does include a one-off cost for the replacement of docks in vehicles due to obsolescence of our android tablet fleet in the 25–30 period. Ongoing refresh costs for these docks will then be met as part of vehicle fit-out.

and monitoring of device access to our network, which cannot be achieved if the device is shared. The potential for malware infection also significantly increases in a shared device environment.

As a result of these combined factors, we instigated a Field Device Replacement program, delivering Panasonic Android tablets to provide each field worker with their own device. This resulted in a net increase of 246 devices, with field staff now allocated individual devices.

### **Hybrid working**

As noted above, the COVID-19 pandemic work restrictions resulted in our whole office-based staff being required to work full-time from home for a significant period. While restrictions have now eased, our office-based workforce has since adopted a hybrid operating model, with staff working from a combination of home and the office. This approach is consistent with that taken in other businesses nationally and globally. It reduces operational risks by ensuring most staff are able to continue to conduct their work with minimal interruption in the event that restrictions should again become necessary.

The hybrid working model has resulted in several significant impacts in the current period, including:

- A transition away from desktop computers and towards more expensive and lower-life portable devices (laptops or tablets), suitable for hybrid working
- Upgraded meeting rooms to support enhanced digital collaboration
- More breakages due to increasing degradation and wear on devices than would otherwise exist in a controlled environment.

These are discussed further below.

#### *Change in device profile*

With an increasingly digitally reliant, decentralised yet connected workforce, the demand for reliable devices to support access to our information assets and information technology (IT) capability systems has never been greater. The pandemic work restrictions and hybrid working model have resulted in a shift towards portable devices that can be easily moved between office and home locations, and away from fixed workstations. This has resulted in additional laptops and tablets in the current RCP, offset by reduced desktops.

#### *Digital collaboration*

The pandemic also resulted in a requirement for the installation or upgrade to technology equipment in office and depot meeting rooms, such as televisions, and video and sound equipment. In conjunction with new digital communication tools and other technology, such as Microsoft Teams and Miro<sup>9</sup>, the upgraded rooms supported hybrid working during the pandemic. With the transition to post-COVID hybrid working, the need for the digital collaboration capabilities continues as staff are still working from the office but also other locations.

#### *Wear and tear*

Fixed desktops usually sit in controlled environments and suffer little wear and tear. Devices that are more portable, such as mobile phones and laptops, are subject to day-to-day use and abuse, and have been shown to fail more frequently, potentially within two to three years of service. This has been magnified by the ongoing work from home scenario, with devices being subject to uncontrolled environments. Increased

---

<sup>9</sup> For collaborative whiteboarding during workshops.

mobility has also led to other types of failures in batteries, USB connectors, screen hinges and power cables.

The result of the new field devices and the COVID-19/hybrid working impacts is that expenditure on client devices for the current 2020–25 RCP is expected to be \$29.4 million, which is \$3.6 million above the \$25.8 million regulatory allowance.

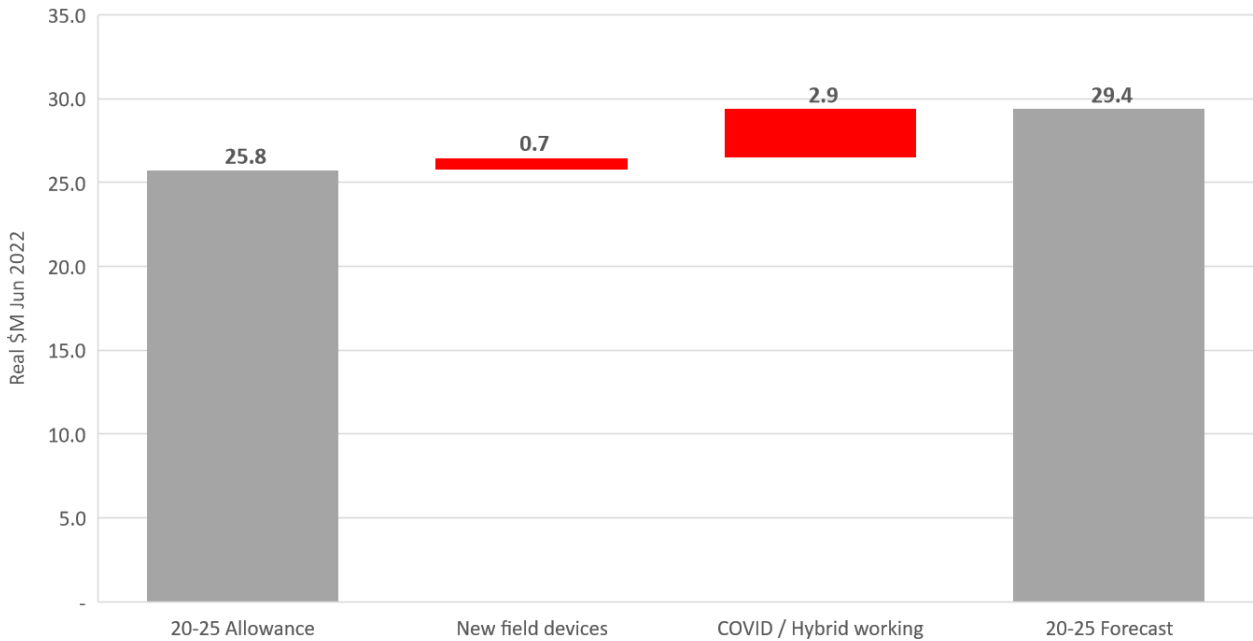


Figure 3: 2020–25 Forecast client devices investment v regulatory allowance

### 3.3 Drivers for change

The following key factors will impact on our 2025–30 funding request:

#### Hybrid working

The ongoing trend towards hybrid working, stemming from the COVID-19 pandemic discussed above, is expected to continue into future periods. This is driving a continued move towards (higher cost and lower life) laptops and tablets, and away from desktop computers. In addition, we expect to see a continued increase in peripherals (monitors, docks, headsets, etc) due to hybrid working arrangements. Wear and tear is expected to increase for all devices that are subject to increased mobility.

## Replace tablet docks in vehicles

SA Power Networks has tablet docks installed in vehicles, which allows for communication capability while operational staff are on the road to and from, and between, jobs. Docks are generally installed during vehicle fit-out and are accounted for as part of the vehicle cost. These docks typically outlast the lives of the vehicles and are transferred to the new vehicle when the existing one is replaced. All fleet vehicles are currently fitted with docks that are compatible with the Panasonic Android tough device tablets that our field staff use.

Panasonic has recently indicated that it will be moving out of the Android tablet market within the next two years. Based on discussions with the vendor, our tablet fleet is expected to become obsolete at the start of our next Reset period. It is highly unlikely that our Panasonic-compatible docks will be compatible with the replacement tablet brand, as this would require the new tablet to be the same dimensions and have all ports of the same types and in the same locations.

Since the timing of the expected dock replacement is consistent with the timing of the next refresh of our Android Tough devices, our estimate assumes the replacement of docks in all vehicles with a dock compatible with the replacement tablet brand at the same time. While the cost of the replacement docks will be funded under this business case, future refresh costs will be covered under the cost of vehicle fit-out.

## 3.4 Industry practice

Recent regulatory submissions with details available for comparable client devices refresh programs are limited, however, where publicly available, business cases describe development of expenditure forecasts using a similar approach to SA Power Networks, ie following vendor refresh cycles but then sweating the assets, where possible, before refreshing.

While small differences between businesses exist, Table 3 shows that SA Power Networks lives for the chosen option are generally comparable with those used by similar businesses, as well as with those proposed by Gartner.

**Table 3: SA Power Networks vs comparable entity refresh rates**

	SA Power Networks	Citipower, Powercor, United Energy <sup>10</sup>	Essential <sup>11</sup>	Ausgrid <sup>12</sup>	Gartner <sup>13</sup>
Standard laptop	3.5	4	4	3-4	3.5 <sup>14</sup>
Standard tablets	3.5	2	3-4	4	3
Standard desktop	5	4	4	n/a	5
Mobile phones	2.5	3	2-3	3	2.5
Video-conference units	4	3	5	5	n/a
Electronic projectors	4	4	n/a	n/a	n/a
Display screens	6	3	5	5	n/a

<sup>10</sup> CitiPower – Business Case 7.12 – Device replacement – 31 January 2020, page 7.

<sup>11</sup> Essential Energy ICT Business Plan – Jan23, Table 1, page 12.

<sup>12</sup> Ausgrid – Att. 5.9.e – ICT & infrastructure program – 31 Jan 2023 – Public, Appendix 3, page 31.

<sup>13</sup> Gartner – Recommended Life Spans to Guide PC, Mobile and Other Device Replacement Strategies, March 2021.

<sup>14</sup> Laptop life used is midpoint of Gartner ‘Aggressive’ and ‘Mainstream’ use cases, reflecting that around half of the SA Power Networks laptop fleet are either high performance machines or operational devices.

## 4. The identified need

The underlying driver for investment action to be considered in this business case is the ongoing mitigation of risks associated with the failure or performance degradation of client devices, due to devices being past their useful life, unsupported or unable to be effectively secured from cyber threats. Consequences of these risks include untimely or no detection and correction of network faults. This could cause mass and prolonged outages if large numbers of devices are impacted, as well as the potential for increased frequency and duration of network outages for customers.

In considering potential responses to this driver, we engaged with our customers on their desired service level outcomes, balanced against price outcomes, and considered our regulatory requirements under the National Electricity Rules (**NER**), National Electricity Law and jurisdictional regulations. As a result of these considerations, the identified need for our client device refresh program is as follows:

- a. To respond to customers' concerns<sup>15</sup>, identified through our consumer and stakeholder engagement process, regarding their explicit service level recommendations that we:
  - maintain reliability service performance – driven by a desire to not see outages; and
  - maintain safety service performance – driven by a desire to not see deterioration in the safety risk posed by the network.
- b. To ensure that our services are able to continue to be delivered for the lowest possible long-term cost – through prudent, systematic, and timely refresh of assets suffering breakage or degradation in performance. This includes extending useful life beyond recommended refresh cycles, where prudent and appropriate to do so.

---

<sup>15</sup> This is pursuant to Clause 6.5.7(c)(5A) of the NER, which requires regard to be had to the extent to which forecast expenditure seeks to address the concerns of distribution service end users identified by the distributor's engagement process.

## 5. Comparison of options

### 5.1 The options considered

Three options have been considered for the refresh of client devices, as summarised in Table 4.

**Table 4: Summary of options considered**

Option	Description
<b>Option 1</b> – Do nothing different (risk-based refresh at current refresh rates) (Base case)	The Base case is to maintain the current approach to client device refresh. This option continues the proactive management of the device fleet by continuing to refresh assets at current rates. Consistent with our IT Asset Management Plan, this includes sweating the assets where risk is able to be mitigated and it is possible and appropriate to do so.
<b>Option 2</b> – Faster device refresh for additional risk reduction	This option considers proactively refreshing the client device fleet at a faster rate than currently occurs, to further reduce risk associated with client devices failing while in service.
<b>Option 3</b> – 2020–25 RCP allowance level	This option entails investing an amount to refresh client devices that is consistent with the Australian Energy Regulator ( <b>AER</b> ) allowance in the current period. Refresh rates are initially set to Option 1 levels, then these refresh rates are adjusted, such that the total investment level is equivalent to the current period forecast.

The following key assumptions are consistent under all options:

- The total number of devices associated with this business case is expected to remain stable over the 2025–30 period<sup>16</sup>.
- Continued support for mobility of our staff through ongoing transition of desktop to portable devices.
- Decline in Windows tough device tablets, with less-expensive Android tablets planned to replace this over time.
- No real increase in device costs over the period.
- Devices with minimal evidence of recent use will continue to be rationalised/repurposed.
- Users with multiple devices are constrained to specific situations, such as where a user requires a specialised laptops for testing or commissioning electrical network devices and operational control equipment, or an operational technology device.
- A small set of devices is retained as spares locally, as devices can fail at any time, and at times do so under stressful outage conditions when they are needed most.
- The forecast for Miscellaneous IT refresh is based on historical trend.

<sup>16</sup> Additional devices are required for new staff proposed as part of the Network Investment Uplift business case. The costs for those additional devices are included within the cost of that business case.



## 5.2 Options investigated but deemed non-credible

### Do nothing (Reactive replacement)

This would result in the refresh of client devices only when they become unusable. A device is considered unusable if:

- it is physically broken and unable to be repaired for use;
- the vendor has stopped manufacturing the device and it is out of support;
- cyber security patches are no longer produced by the vendor (driver patching);
- cyber security patches can no longer be applied to the device (operating system patching); or
- performance/capability does not support business needs, eg, hardware can't support business applications or operating systems.

Industry standard practice, as well as our own experience in managing client devices, indicates that a proactive refresh approach results in a significant reduction in failures and performance issues compared with reactive replacement. This reduces support costs and the risk of cyber security threats, which in turn reduces risks to quality, reliability, and security of electricity supply. As such, reactive replacement of our client device fleet has not been considered.

## 5.3 Analysis summary and recommended option

### 5.3.1 Options assessment results

Table 5: Costs, benefits and risks of the alternative options (\$m Jun 2022 Real)

Option	10-year program costs			2025–30 program costs			10-year benefits <sup>17</sup>	10-year NPV <sup>18</sup>	Overall risk rating <sup>19</sup>	Ranking
	Capex	Opex	Total	Capex	Opex	Total				
<b>Option 1</b> – Do nothing different (Risk-based refresh at current refresh rates)	62.3	-	62.3	32.1	-	32.1	n/a	-51.4	Medium	1
<b>Option 2</b> – Faster device refresh for additional risk reduction	70.1	-	70.1	35.4	-	35.4	n/a	-57.8	Low	2
<b>Option 3</b> – 2020–25 RCP allowance level	52.5	-	52.5	26.4	-	26.4	n/a	-43.3	High	3

### 5.3.2 Recommended option

The recommended option is **Option 1 – Do nothing different (Risk-based refresh at current refresh rates)**.

The capital cost of this option in the 2025–2030 period is \$32.1 million.

<sup>17</sup> Represents the total capital and operating risk reduction and over the 10-year cash flow period from 1 July 2025 to 30 June 2035 expected across the organisation as a result of implementing the proposed option.

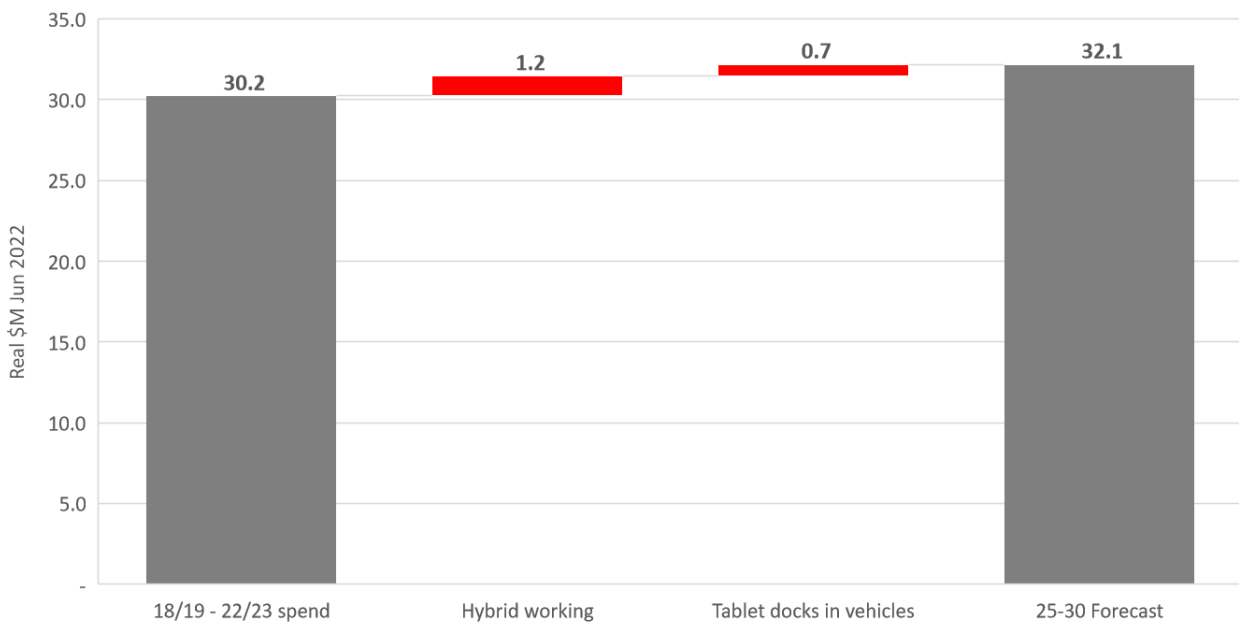
<sup>18</sup> Net present value (NPV) of the proposal over 10-year cash flow period from 1 July 2025 to 30 June 2035, based on discount rate of 4.05%.

<sup>19</sup> The overall risk level for each option after the proposed option is implemented. Refer to [Appendix B](#) – risk assessment for details.

This solution is to continue to proactively manage our client devices using the same approach that we currently take. We will refresh based on industry- and vendor-recommended lifecycles, and our own asset management experience, with assets sweated where it is considered that risks are able to be mitigated.

This option was selected because it is the most cost-effective option for reducing risks to an acceptable level. While investing at the current period regulatory allowance level would incur a lower upfront cost, the risks associated with sweating assets past the point where these assets begin to fail will result in business and customer impacts, and this option therefore does not represent the actions of a prudent service provider.

As described in Section 3.3, there are two factors that will drive an uplift in client devices capex in the 2025–30 period. Figure 4 shows how these factors impact the total expenditure, compared with the current investment level.



**Figure 4: 2020–25 forecast client devices investment vs last five years investment**

Appendix A lists the cost and benefit models for each option. Appendix B provides the detailed risk analysis for each option.

## 5.4 Scenario and sensitivity analysis

The key sensitivity between the options is the refresh rates used for each device type. These are shown in Table 6.

**Table 6: Refresh rates**

Asset type	Option 1: Current refresh rate	Option 2: Faster device refresh	Option 3: 20–25 RCP allowance level
Standard laptop/tablet	3.5	3	4
Standard desktop	5	4.5	6
Power desktop	5	4.5	6
Power laptop	5	4.5	6
Mobile phones	2.5	2	3

Asset type	Option 1: Current refresh rate	Option 2: Faster device refresh	Option 3: 20–25 RCP allowance level
Tough device (Windows)	5	4.5	5.5
Tough device (Android)	3	2.5	4
Monitor	6	5.5	7
USB docks	5	4.5	6
Meter reading	2.5	2	3.5
Conferencing unit – video	4	3.5	5
Conferencing unit – tele	4	3.5	5
Televisions (55", 65", 75", 85")	8	7.5	9
Large monitor	6	5.5	7
Plotter	5	4.5	6

Unit rates are the same under all options and are held consistent across the forecast period. While in the next RCP real dollar unit rates could either continue to increase, or potentially revert to pre-pandemic levels, there is no basis for assuming that either of these scenarios will occur. Unit rates are based on:

- competitively sourced vendor rates for the hardware component.
- a labour rate component for each device type that covers the costs associated with purchase and deployment. This rate is based on 38% of the materials cost which reflects average labour components incurred in recent periods<sup>20</sup>.

The effect of changes to the discount rate has been considered and does not affect the ranking of the options.

## 5.5 Option 1: Do nothing different (Risk-based refresh at current refresh rates)

### 5.5.1 Description

This option continues the proactive management of our device fleet by periodically refreshing assets at the current replacement intervals, but continuing to sweat assets past this point where risk is able to be mitigated and it is possible and appropriate to do so. Potential for sweating the assets is based on various factors, including risk mitigation (cyber security, risk of hardware failure, cost of unplanned break/fix replacements), support arrangements and historical reliability.

### 5.5.2 Costs

The forecast for Option 1 has been prepared on a bottom-up basis by determining refresh volumes for each device type in each period and then applying an efficient unit rate. Total costs for this option are provided in Table 7.

**Table 7: Option 1 – Costs by cost type (\$m Jun 2022 real)**

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Capex	6.3	6.2	6.8	6.7	6.2	32.1
Opex	-	-	-	-	-	-
<b>Total</b>	<b>6.3</b>	<b>6.2</b>	<b>6.8</b>	<b>6.7</b>	<b>6.2</b>	<b>32.1</b>

<sup>20</sup> Additional costs associated with short term Covid impacts have been removed

The Option 1 current refresh rates reflect asset lives for each device type that have been deemed prudent based on condition-based risk experience, suppliers’ support plans/warranties and our experience as an asset manager. These are generally consistent with standard industry practice.

Refresh volumes have been determined by:

- projecting forward the refresh dates of the existing fleet using individual asset purchase dates and the relevant device type refresh rate
- adjusting for impacts arising from expected changes to the device mix.

Table 8 shows the proposed investment by device type for the 2025–2030 RCP for Option 1. Detailed costing models are listed in Appendix A – Cost models.

**Table 8: Device refresh by device type for Option 1**

Asset type	Avg Fleet size 2025–30	Refresh rate	Total replacements	Total spend (\$m Jun 2022 real)
Standard laptop/tablet	2629	3.5	4160	10.7
Standard desktop	358	5	358	0.6
Power desktop	335	5	335	2.2
Power laptop	82	5	82	0.4
Mobile phones	1821	2.5	3642	3.7
Tough devices (Windows)	85	5	81	0.5
Tough devices (Android)	721	3	1248	3.5
Monitors	7720	6	6433	3.0
Docks	3054	5	3054	1.4
Other minor devices (meter reading, conferencing, TVs, large monitors, plotters)	460	2.5-8	494	1.9
Device evaluation	n/a	n/a	n/a	1.1
Miscellaneous IT refresh	n/a	n/a	n/a	2.4
Vehicle tablet dock replacement	507	n/a	507	0.7
<b>Total</b>	<b>17,772</b>		<b>20,393</b>	<b>32.1</b>

### 5.5.3 Risks

Table 9: Risk assessment summary

Risk consequence category	Residual risk level (Do nothing) <sup>21</sup>	Residual risk level <sup>22</sup> (Option 1)
<b>Safety</b> – Harm to a worker, contractor or member of the public	Medium	Low
<b>Performance and growth</b> – Financial impact	High	Low
<b>Network</b> – Failure to transport electricity from source to load	High	Medium
<b>Customers</b> – Failure to deliver on customer expectations	High	Low
<b>Technology</b> – Disruption of access to, or use of, systems	Medium	Low
<b>Technology</b> – Unauthorised access, modification or control of systems	High	Low
<b>Technology</b> – Unauthorised access or disclosure of information	Medium	Low
<b>Governance</b> – Non-compliance with regulatory, legislative and/or other obligations	Medium	Low
<b>Overall risk level</b>	High	Medium

### 5.5.4 Quantified benefits

There are no tangible quantifiable benefits associated with this option.

### 5.5.5 Unquantified benefits

Client devices enable efficient delivery of customer and network services by ensuring staff can respond to customer and network issues, receive job information in the field, access critical asset and service information, and update customers with timely information on progress. They also keep our workforce safe in a diverse and challenging environment, including under extreme conditions, such as weather-related outages and bushfires.

Devices that are past their useful life suffer from declining performance and unreliability and may fail at inopportune times. Mitigating this risk prevents interruptions to business operations by ensuring that individuals within the business who perform key activities on the electricity network and assets can continue to perform these activities in a timely manner. In addition, refreshing other non-operational devices ensures that these remain fit for purpose and do not restrict the effectiveness of individuals and work groups in achieving operational objectives and commitments.

Proactively upgrading older devices ensures that the whole device fleet can be updated with the latest security requirements and the latest software and operating system needs, reducing vulnerability to cyber attacks.

Stretching asset lives, where prudent and reasonable to do so, and where risks can be mitigated, minimises maintenance and refresh costs and maximises device useful life to the greatest extent possible within a prudent proactive refresh program.

<sup>21</sup> The level of risk post current controls (i.e., after considering what we currently do to mitigate the risk).

<sup>22</sup> The future level of risk once treatments proposed in this option have been implemented.

## 5.6 Option 2: Faster device refresh for additional risk reduction

### 5.6.1 Description

This option also continues the proactive management of our device fleet by periodically refreshing assets at consistent intervals. For this option we have assumed an asset life reduction of 0.5 years, compared with our current lives for every asset class.

### 5.6.2 Costs

The forecast for Option 2 has been prepared on a bottom-up basis by determining refresh volumes for each device type in each period and then applying an efficient unit rate. Total costs for this option are provided in Table 10.

**Table 10: Option 2 – Costs by cost type (\$million, Jun 2022 real)**

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Capex	7.4	5.6	7.2	9.4	5.9	35.4
Opex	-	-	-	-	-	-
<b>Total</b>	7.4	5.6	7.2	9.4	5.9	35.4

As with Option 1, refresh volumes have been determined by:

- projecting forward the refresh dates of the existing fleet using individual asset purchase dates and the relevant device type refresh rate
- adjusting for impacts arising from expected changes to the device mix.

Table 11 shows the proposed investment by device type for the 2025–30 RCP for Option 2. Detailed costing models are listed in Appendix A – Cost models.

**Table 11: Device refresh by device type for Option 2**

Asset type	Avg Fleet size 2025–30	Refresh rate	Total replacements	Total spend (\$m Jun 2022 real)
Standard Laptop/tablet	2629	3	4737	12.2
Standard desktop	358	4.5	358	0.6
Power desktop	335	4.5	335	2.2
Power laptop	82	4.5	88	0.5
Mobile phones	1821	2	4560	4.6
Tough devices (Windows)	85	4.5	81	0.5
Tough devices (Android)	721	2.5	1411	4.0
Monitors	7720	5.5	7018	3.3
Docks	3054	4.5	3393	1.6
Other minor devices (meter reading, conferencing, TVs, Large monitors, plotters)	460	2–7.5	481	1.8
Device evaluation	n/a	n/a	n/a	1.1
Miscellaneous IT refresh	n/a	n/a	n/a	2.4
Vehicle tablet dock replacement	507	n/a	507	0.7
<b>TOTAL</b>	<b>17,772</b>		<b>22,969</b>	<b>35.4</b>

### 5.6.3 Risks

**Table 12: Risk assessment summary**

Risk consequence category	Residual risk level (Do nothing) <sup>23</sup>	Residual risk level <sup>24</sup> (Option 2)
<b>Safety</b> – Harm to a worker, contractor or member of the public	Medium	Negligible
<b>Performance and growth</b> – Financial impact	High	Low
<b>Network</b> – Failure to transport electricity from source to load	High	Low
<b>Customers</b> – Failure to deliver on customer expectations	High	Low
<b>Technology</b> – Disruption of access to, or use of, systems	Medium	Negligible
<b>Technology</b> – Unauthorised access, modification or control of systems	High	Low
<b>Technology</b> – Unauthorised access or disclosure of information	Medium	Negligible
<b>Governance</b> – Non-compliance with regulatory, legislative and/or other obligations	Medium	Negligible
<b>Overall risk level</b>	High	Low

The likelihood of the risk occurring under many of the identified risk scenarios would be lower under Option 2 than Option 1. In particular, residual risks associated with the inability to transport electricity and loss of access to systems would be Low, leading to an overall reduction in residual risk to Low.

### 5.6.4 Quantified benefits

There are no tangible quantifiable benefits associated with this option.

### 5.6.5 Unquantified benefits

The benefits associated with Option 2 are similar to those described above for Option 1. However, this option results in additional investment over and above what it is considered that an efficient network operator acting prudently would incur.

## 5.7 Option 3: 20–25 RCP allowance level

### 5.7.1 Description

Option 3 also involves the proactive refresh of client devices on a periodic basis. However, expenditure under this option is constrained to the AER-approved expenditure allowance for the current 2020–25 RCP.

### 5.7.2 Costs

For this scenario, a similar modelling process has been employed as for the other two options. However, refresh rates for all items have been adjusted to reflect a total investment level that is equivalent to the current period regulatory allowance. Total costs for this option are provided in Table 13.

<sup>23</sup> The level of risk post current controls (ie after considering what we currently do to mitigate the risk).

<sup>24</sup> The future level of risk once treatments proposed in this option have been implemented.

**Table 13: Option 3 – Total cost by cost type (\$m Jun 2022 Real)**

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Capex	5.5	6.4	3.4	4.5	6.7	26.4
Opex	-	-	-	-	-	-
<b>Total</b>	<b>5.5</b>	<b>6.4</b>	<b>3.4</b>	<b>4.5</b>	<b>6.7</b>	<b>26.4</b>

Given the cost increases noted in Section 3.3, as well as the timing of when asset refreshes fall due, the constrained level of expenditure under this option results in an increase in asset refresh rates (see Table 6, above), with all refresh rates being required to increase by between 0.5 and one year.

Table 14 shows the proposed investment by device type for the 2025–30 RCP for Option 2. Detailed costing models are listed in Appendix A – Cost models.

**Table 14: Device refresh by device type for Option 3**

Asset type	Avg Fleet size 2025–30	Refresh rate	Total replacements	Total spend (\$m Jun 2022 Real)
Standard laptop/tablet	2629	4	3256	8.4
Standard desktop	358	6	355	0.6
Power desktop	335	6	190	1.2
Power laptop	82	6	54	0.3
Mobile phones	1821	3	3600	3.6
Tough devices (Windows)	85	5.5	82	0.5
Tough devices (Android)	721	4	888	2.5
Monitors	7720	7	5514	2.6
Docks	3054	6	2545	1.2
Other minor devices (meter reading, conferencing, TVs, large monitors, plotters)	460	3.5-9	290	1.2
Device evaluation	n/a	n/a	n/a	1.1
Miscellaneous IT refresh	n/a	n/a	n/a	2.4
Vehicle tablet dock replacement	507	n/a	507	0.7
<b>Total</b>	<b>17,772</b>		<b>17,281</b>	<b>26.4</b>



### 5.7.3 Risks

Table 15: Option 3 – Risk assessment summary

Risk consequence category	Residual risk level (Do nothing) <sup>25</sup>	Residual risk level <sup>26</sup> (Option 3)
<b>Safety</b> – Harm to a worker, contractor or member of the public	Medium	Low
<b>Performance and growth</b> – Financial impact	High	Medium
<b>Network</b> – Failure to transport electricity from source to load	High	High
<b>Customers</b> – Failure to deliver on customer expectations	High	Medium
<b>Technology</b> – Disruption of access to, or use of, systems	Medium	Low
<b>Technology</b> – Unauthorised access, modification or control of systems	High	Medium
<b>Technology</b> – Unauthorised access or disclosure of information	Medium	Low
<b>Governance</b> – Non-compliance with regulatory, legislative and/or other obligations	Medium	Low
<b>Overall risk level</b>	High	High

The increases in refresh lives means that under this scenario, devices would need to be sweated past the point where it is considered safe and efficient to do so. This would increase the likelihood of the risk occurring under many of the identified risk scenarios. In particular, risks associated with the inability to transport electricity and loss of access to systems would remain High, leading to an overall High residual risk under Option 3.

### 5.7.4 Quantified benefits

There are no tangible quantifiable benefits associated with this option.

### 5.7.5 Unquantified benefits

As with Options 1 and 2, this option is still technically a proactive refresh of client devices. However, the long asset lives will result in the number of devices failing in service increasing over time, effectively resulting in a significant amount of reactive replacement.

<sup>25</sup> The level of risk post current controls (ie after considering what we currently do to mitigate the risk).

<sup>26</sup> The future level of risk once treatments proposed in this option have been implemented.

## **6. Deliverability of recommended option**

The total cost of the selected option is an increase of 4% compared with the forecast current period investment. However, the proposed investment level is consistent on average with what we have been delivering over recent years and activity in each year is below what was delivered in the 2021–22 period. Additionally, more than 70% of the investment is the materials cost of the devices themselves. Given the mature client device refresh capability in place at SA Power Networks, we do not foresee any issues with our ability to deliver the proposed level of activity.

## **7. How the recommended option aligns with our engagement**

Customers expect that we will maintain our existing levels of service and risk. Maintained and fit-for-purpose devices enable SA Power Networks to achieve those requirements in a cost-effective manner and within specified key performance requirements, by ensuring our workforce can access data, respond to jobs, and manage the network to expectations.

As part of the Focused Conversation stages of customer engagement, we presented the costs for this business case as ‘for information’ at the IT workshop with the Consumer Advisory Board. These costs were included in Scenario 1 – Business as usual for all other customer workshops and pricing analysis.

## 8. Alignment with our vision and strategy

Our Digital & Data Strategy outlines the long-term strategic direction for ICT. The focus of the strategy is on the provision of efficient and reliable core systems, and a range of digitisation that ensures our workforce has appropriate skills for the technology implemented. A high-level view of our Digital & Data Strategy is depicted in Figure 5.

Reliable and secure client devices are key enablers for a number of the outcomes detailed in this strategy:

1. Client devices are a safety device for our staff. Having reliable devices that function even during extreme events, such as bushfires, are a key component of keeping our staff and community safe.
2. Enabling trusted data by facilitating the efficient collection of data at the sources, particularly when that source can be very remote.
3. Facilitating better and safer decision-making through the reliable presentation of data where our staff need it.
4. Facilitating efficient digitally-enabled work practices through the reliable provision of information on the client devices, as well as enabling the removal of paper-based information sources and forms.
5. Enabling secure, resilient systems and data through devices that can be kept up to date with required software updates.

### Digital & Data Strategy

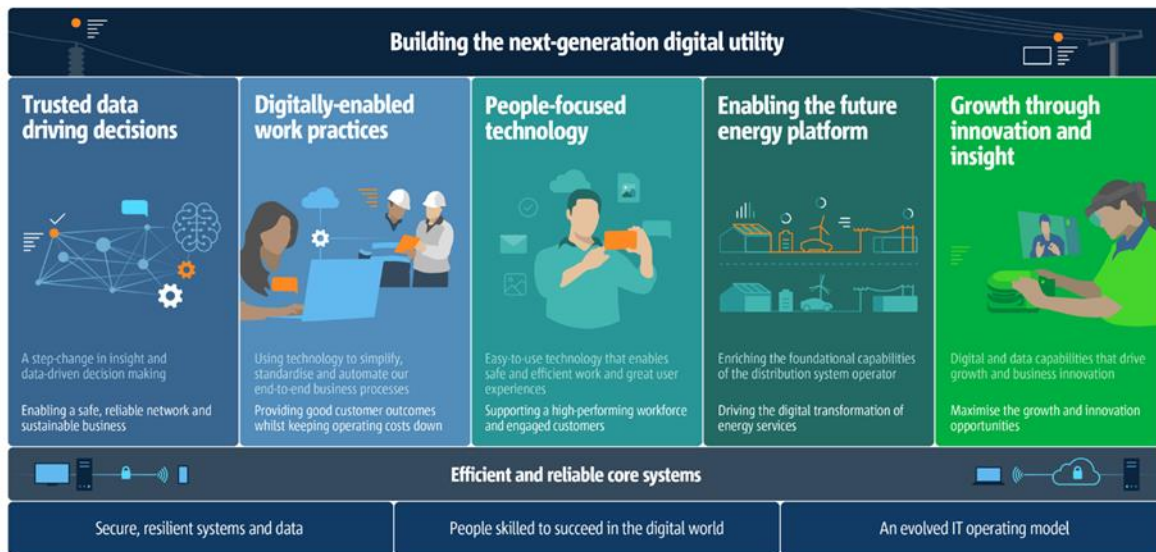


Figure 5: SA Power Networks Digital & Data Strategy

Client devices are a key enabler for the Digital & Data Strategy and the broader SA Power Networks strategic direction. Modern, reliable and secure computing and communication devices are critical tools that support core future capabilities, such as management and accessibility of data for decision-making, digital tools for optimising business processes, and the efficient provision of information to customers. They enable growth in both existing and future energy capabilities.

## 9. Reasonableness of cost estimates

The bottom-up cost estimates forecast for this business case have been validated using top-down assessment methods – trending and benchmarking.

### Trending

Figure 6 shows the client devices investment trend over time, including both actual and forecast expenditure. While this expenditure is recurrent, it is cyclical, with refresh cycles driving higher required investment levels in some years than in others.

As discussed in Section 3.2, the high level of expenditure in 2021–22 is due to COVID-19 impacts. Investment levels reduce towards the end of the current RCP to offset this, and then increase again in the next RCP due to the cost drivers noted in Section 3.3, ie:

- A change to hybrid working and the associated shift towards more mobile devices, plus an increase in total devices, with the rollout of 246 additional individual tablets to field staff.
- The replacement of tablet docks in vehicles due to the upcoming obsolescence of our Panasonic tablet fleet.

As a result, while our proposed Option 1 forecast represents a slight increase above 2020-25 RCP levels, the trend over time is materially consistent, as seen in the rolling five-year average for the chosen Option 1.

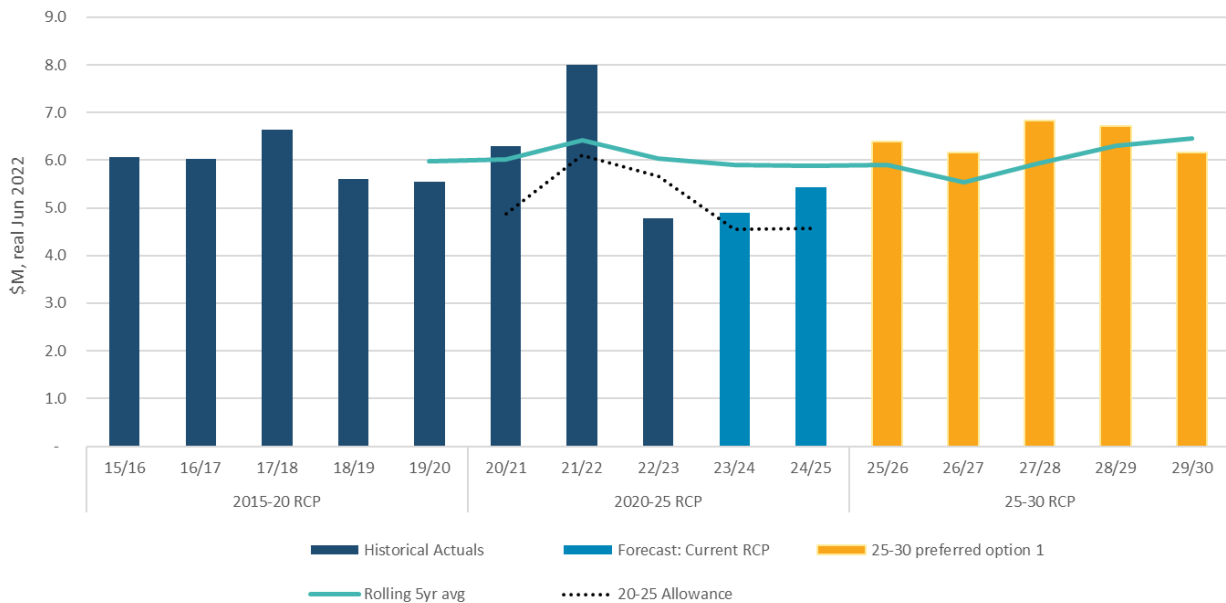


Figure 6: Client devices investment trend over time

### Benchmarking

We have also compared our expenditure to other utilities. Client devices total recurrent expenditure (capex plus opex) for SA Power Networks sits around the benchmark of all Australian electricity utilities on the basis of both customer numbers and IT users. This is shown in Figure 7 and Figure 8. We aim to maintain this position going forward – reflecting a strong balance between the need to be efficient while still responding to the rapid changes in our energy and cyber environments.

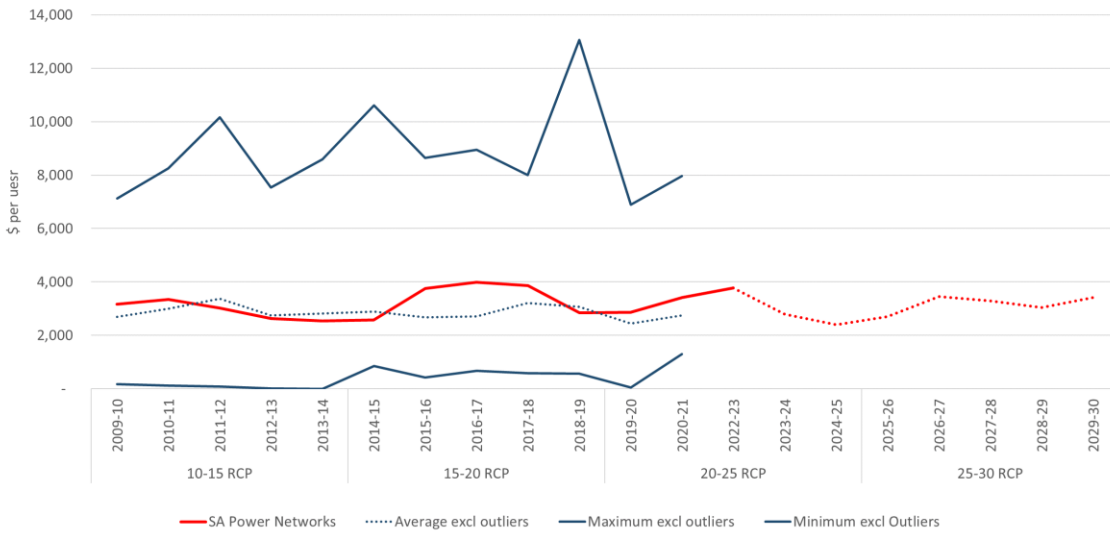


Figure 7: Client device totex per user across utilities on the NEM (\$m Jun 2022 real)

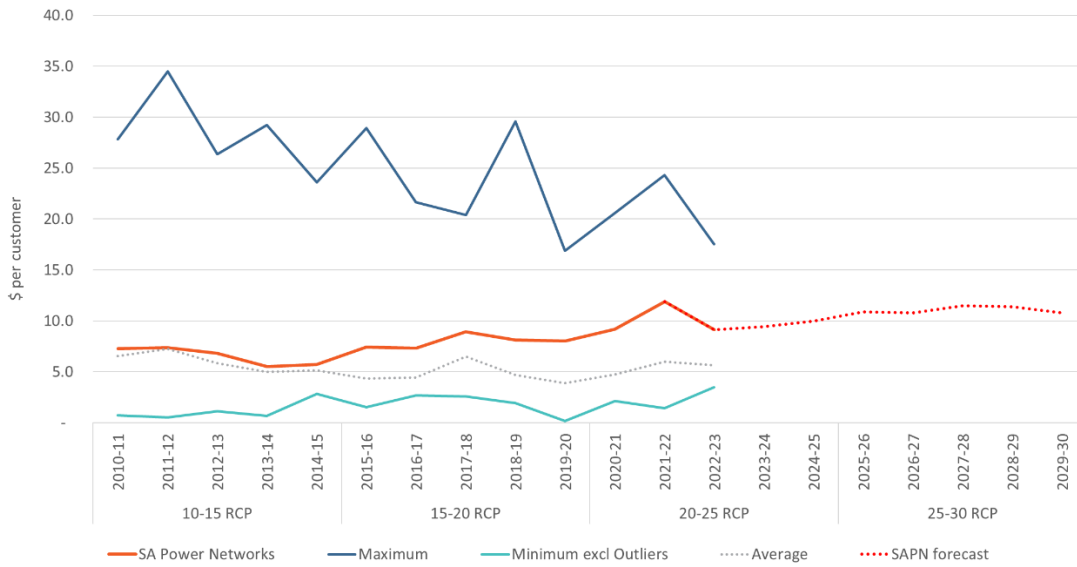


Figure 8: Client devices totex per customer across utilities on the NEM (\$m Jun 2022 real)

## 10. Reasonableness of input assumptions

The starting point for our client devices refresh forecast is the purchase dates of all assets currently existing in our device fleet. The key assumptions applied to this are:

- derivation of refresh volumes using **device lifespans**
- calculation of expenditure forecasts by multiplying derived refresh volumes by efficient **unit rates**.

### Device lifespans

The Option 1 current refresh rates reflect asset lives for each device type that has been deemed prudent, based on condition-based risk experience, suppliers' support plans/warranties, and our experience as an asset manager. These refresh rates are consistent with standard industry practice.

### Unit rates

Assumed materials unit rates reflect the most recently available purchase cost for each of the device categories. While device rates have increased significantly above inflation in the current period due to supply chain restrictions associated with the COVID-19 pandemic, we are conservatively assuming that costs will continue at 2020-25 levels (in real terms). While it is very possible that real dollar unit rates will continue to increase, there is no basis for assuming that this scenario will occur.

Labour rates are applied to each device category at a percentage of the materials rate. This reflects the expected labour costs associated with procuring and deploying devices, calculated from historical costs.

## **A. Appendix A – Cost models**

2025 – 30 Reset – Client Devices forecast template – Option 1.xlsm

2025 – 30 Reset – Client Devices forecast template – Option 2.xlsm

2025 – 30 Reset – Client Devices forecast template – Option 3.xlsm



## B. Appendix B – Risk assessment

ID	Risk scenario	Consequence description	Consequence category	Current risk Risk-based refresh (Option 1)			Residual risk – Faster refresh (Option 2)			Residual risk – Current period allowance (Option 3)			Residual risk – Do nothing (Option 0)		
				Consequence	Likelihood	Risk Level	Consequence	Likelihood	Risk level	Consequence	Likelihood	Risk level	Consequence	Likelihood	Risk level
1	Failure or performance degradation of client devices, due to devices being past their useful life or unsupported.	Untimely or no detection and correction of network faults, causing mass and prolonged outages, if large number of devices impacted.	<b>Network</b> – Failure to transport electricity from source to load	4	2	Medium	4	1	Low	4	3	High	4	4	High
		Increased frequency and duration of network outages for customers.	<b>Customer</b> – Failure to deliver on customer expectations	3	2	Low	3	1	Low	3	3	Medium	3	4	High
		Field workers unable to access safety critical and/or configuration management information before they start work on a site (eg, whether a section is energised or not, cable locations, site safety plans).	<b>Safety</b> – Harm to a worker, contractor, or member of the public	2	2	Low	2	1	Negligible	2	3	Low	2	4	Medium
		Difficulty in tracking and contacting field workers in remote locations.	<b>Performance and growth</b> – Financial impact	3	2	Low	3	1	Low	3	3	Medium	3	4	High
		Inability to operate in accordance with regulatory obligations.	<b>Governance</b> – Non-Compliance with Regulatory Obligations	2	2	Low	2	1	Negligible	2	3	Low	2	3	Low

ID	Risk scenario	Consequence description	Consequence category	Current risk Risk-based refresh (Option 1)			Residual risk – Faster refresh (Option 2)			Residual risk – Current period allowance (Option 3)			Residual risk – Do nothing (Option 0)		
				Consequence	Likelihood	Risk Level	Consequence	Likelihood	Risk level	Consequence	Likelihood	Risk level	Consequence	Likelihood	Risk level
2	Client devices become insecure or unsupported by the vendor, resulting in increased vulnerability to cyber attacks.	Cyber attackers obtain information regarding critical infrastructure, or can interfere with network and asset operations and control.  Organisational and customer private data network security being compromised.	<b>Technology</b> – Disruption of access to, or use of, systems	2	2	Low	2	1	Negligible	2	3	Low	2	4	Medium
			<b>Technology</b> – Unauthorised access, modification, or control of systems	3	2	Low	3	1	Low	3	3	Medium	3	4	High
			<b>Governance</b> – Non-Compliance with regulatory obligations	2	2	Low	2	1	Negligible	2	3	Low	2	4	Medium
			<b>Customer</b> – Failure to deliver on customer expectations	2	2	Low	2	1	Negligible	2	3	Low	2	4	Medium
			<b>Technology</b> – Unauthorised access and disclosure of information	2	2	Low	2	1	Negligible	2	3	Low	2	4	Medium
		Significant litigation/punitive damages, legal costs and major loss of management time.	<b>Performance and growth</b> – Financial impact	3	2	Low	3	1	Low	3	3	Medium	3	4	High
			<b>Overall risk level<sup>27</sup></b>			Medium			Low			High			High

<sup>27</sup> For each option, the overall risk level is the highest of the individual risk levels.