Business case: ICT Recurrent - Cyber Security Refresh

2025-30 Regulatory Proposal

Supporting document 5.12.6

January 2024

SA Power Networks

Empowering South Australia

Contents

Glossary

Acronym / term	Definition
ACSC	Australian Cyber Security Centre
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCSF	Australian Energy Sector Cyber Security Framework
Capex	Capital expenditure
CISC	Cyber and Infrastructure Security Centre
ICT	Information and communication technology
IT	Information technology
NEM	National Electricity Market
NPV	Net present value
Opex	Operating expenditure
OT	Operational technology
P1	Priority one
RCP	Regulatory Control Period
SaaS	Software as a service
SCADA	Supervisory control and data acquisition
SLACIP	Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
SOCI	Security of critical infrastructure
SP	Security profile
UX	User Experience

1. About this document

1.1 Purpose

The purpose of this document is to provide the business case and justification for the recurrent refresh of cyber security systems, which are fundamental to the security and reliability of the electricity distribution network.

1.2 Expenditure category

- Non-network Information and communication technology (ICT) – Recurrent
- Non-network ICT – Step change: Capital expenditure (Capex) to Operating expenditure (Opex) shift

1.3 Related documents

Table 1: Related documents

Title	Author	Version / date
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
5.12.9 - ICT Non-Recurrent – Cyber Security Uplift Business Case	SA Power Networks	Jan 2024
5.12.23 - ICT Forecasting Methodology and Business Case Structure	SA Power Networks	Jan 2024
5.12.24 - External review of Cyber Expenditure Treatment	BDO Australia	Jan 2024

2. Executive summary

This business case recommends a recurrent investment of $18.2 million[1] to maintain our existing cyber security and Information Technology (**IT**) resilience capabilities. By safeguarding the security and reliability of the SA Power Networks' electricity distribution network, cyber security practices enable the benefits of a customer-centred and increasingly interconnected world. A strong cyber security capability will keep our customers and organisation safe and secure, underpin our future network, reduce cyber security risk, increase IT resilience, and secure our digital identity.

As part of the 2020–25 Reset, the Australian Energy Regulator (**AER**) approved $5.7 million non-recurrent capital investment for SA Power Networks to uplift our capability to begin to address an increasing cyber security threat level. Over the current period, there has been a significant escalation in the number and seriousness of threats faced by SA Power Networks, with utilities garnering increasing attention. This is evidenced by sophisticated cyber-attacks [redacted] in several global jurisdictions.

With an ever-increasing business reliance on technology, the severity of consequences from a cyber security failure at SA Power Networks continues to grow. [redacted]

It is therefore prudent to continue to maintain the health of our cyber security systems, processes, practices and tools that are critical in preventing, detecting, reporting, and remediating threats. This business case proposes maintaining our current level of cyber security risk management, in relation to the existing threat level, for our IT and operational technology (**OT**) systems and data. Given the high level of cyber security risk currently present in the business (and all businesses), the residual risk associated with all options in this business case is Extreme. This indicates that this business case alone will do little to address the massive risk associated with the ever-evolving cyber security threats. However, it is the best of the available options.

The **$18.2 million forecast for the preferred option comprises $2.9 million of capex and $15.3 million of opex**. The proposed expenditure for the program reflects the average of the current Regulatory Control Period (**RCP**) investment level, with a small uplift to cater for the material increase in the volume of activity covered within the teams supporting our operational cyber security capability. The expectation is that this increase in activity will continue to grow throughout the next RCP.

These changes have necessitated an increase in capability to ensure we can effectively triage and investigate incidents in a timely manner and avoid a potential disruption to services. It is expected that the volume of activity covered within the teams supporting our operational cyber security capability will continue to grow into the next period as the current capability uplift is embedded into operations.

As part of this business case, we considered an alternative option of investing at only the average 2020-25 RCP level of $17.7 million ($3.5 million average per annum). However, this option would result in an increased likelihood of many identified risk events and their associated consequences. It therefore does not

[1] Unless otherwise specified, all financial figures in this business case are in real June 2022 dollars

represent the actions of a provider of [redacted] energy infrastructure. Options to invest a lower amount in cyber security, or not investing at all, were considered but discounted. These options would result in a rapid degradation in cyber security capability at the existing risk and threat level and therefore an Extreme residual cyber risk well before the end of the RCP.

[redacted]

Despite the significant activity undertaken to date, the residual risk rating remains Extreme, given the growing levels of cyber risk. To address this Extreme risk rating, we have also developed a separate business case for the 2025–30 RCP that proposes an increase in cyber security capabilities to address the increase in risks and threats that will emerge in coming years. Together with that investment, the continuation of existing cyber security practices ensured by this business case will minimise and manage the substantial current risks, ensuring that services to our customers remain secure, reliable, available and for the lowest possible cost.

Table 2: Options assessment summary, $m, June 2022.[2]

	2025-2030 costs			10-year estimates		Residual risk rating[3]
Option	**Capex**	**Opex**	**Total**	**Benefits**	**NPV[4]**	
1. Maintain existing levels of expenditure	4.1	13.5	17.7	n/a	-29.2	**Extreme**
2. Maintain existing levels of service with a prudent level of expenditure (preferred)	2.9	15.3	18.2	n/a	-29.9	**Extreme**

[2] Note: Totals presented in tables throughout this document may not exactly match the sums of individual figures due to rounding
[3] The overall risk level for each option after the proposed option implemented. Refer to Appendix B – risk assessment for details.
[4] 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%.

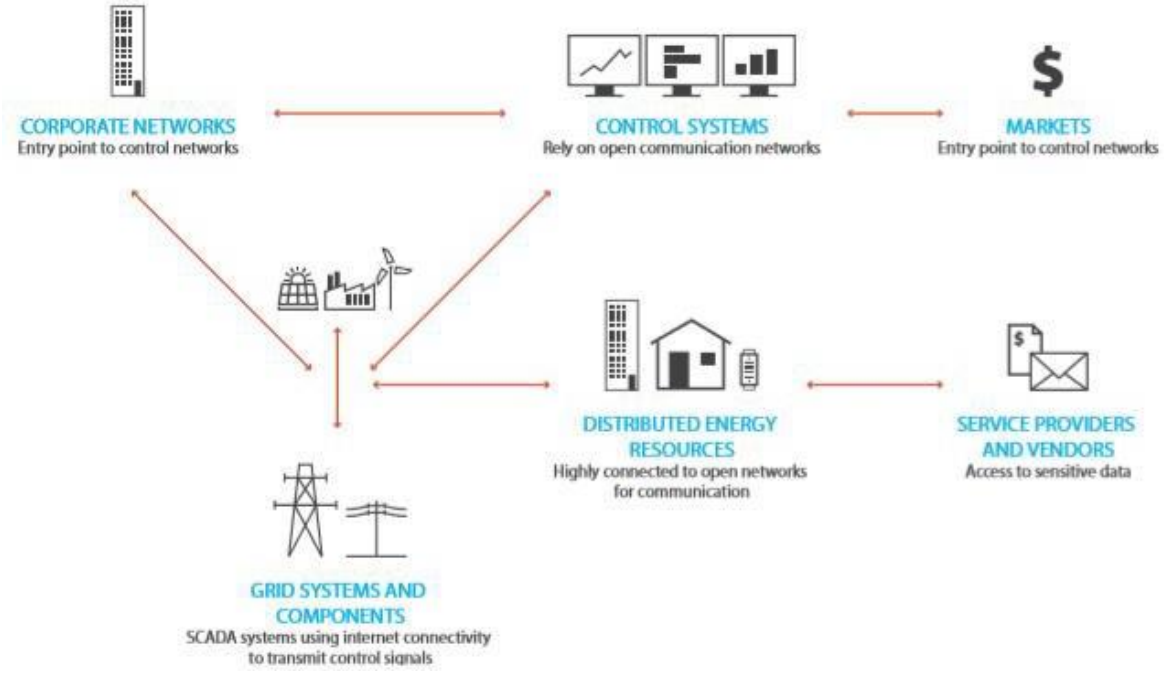
3. Background

Around the globe, energy infrastructure supports the effective operation of most modern economies and societies. Australia's reliable, safe, and efficient energy sector underpins the sustainable delivery of all essential services that we rely on as a country.

[redacted], SA Power Networks has a duty to maintain the reliability, availability, and safety of its electricity networks. [redacted]

Figure 1 below outlines the key components of electricity networks and systems that are subject to potential cyber security threats.

Figure 1: Electricity Network components subject to cyber security threats



[redacted]

Over the last 10 years, SA Power Networks has developed security and resilience safeguards to protect our systems, processes and people from vulnerabilities that can, purposefully or accidentally, cause disruption or failure. Specifically, these safeguards allow us to respond to:

- the increasing complexity, prevalence and targeted nature of threats;
- a changing electricity distribution industry and regulatory obligations; and
- technology opportunities and changes, such as cloud services.

Most of the effort in the current RCP (approximately two thirds) has focused on developing systems and processes to support these safeguards. This was therefore proposed, and is currently treated, as capex and is the subject of this business case. The remaining one third of the cost of these activities is currently treated as opex and is therefore funded through roll-forward of the efficient base year.

[redacted]

3.1 The scope of this business case

The key objectives for the SA Power Networks Cyber Security program are to develop and then maintain, enhance and adapt the capabilities and supporting tools and processes required for the following activities:

- **Identify** cyber security risks to systems, assets, data and business operations.
- **Protect** the delivery of services through appropriate safeguards and resiliency.
- **Detect** the occurrence of cyber security events that have bypassed protection controls.
- **Respond** to a detected cyber security event to minimise its impact or harm through timely execution of appropriate actions.
- **Recover** any capabilities or services that may be impaired due to a cyber security event.

This business case encompasses the capex portion of these activities across the organisation. Specifically, it covers our operations, digital identity and risk and resilience recurrent cyber security activities, for both our IT and OT operations. These are discussed further below.

Operations

Our cyber security operations function provides SA Power Networks with an in-depth understanding of our cyber threats, and then supports this with proactive threat management and enhanced response and recovery strategies. The core activities that are involved in this are:

Security logging, monitoring and detection

Logging is the collection of the technical data automatically produced by information/digital assets (eg, IT, OT and Supervisory control and data acquisition (**SCADA**) assets) that identifies the asset's low-level processes, tasks, actions and changes. Logging is the foundation that cyber security monitoring is built on.

Monitoring is the activity that collects and analyses technical security data (such as logs) and presents it in a meaningful way to facilitate detection.

Detection is the activity that correlates, analyses, contextualises, evaluates, identifies, alerts and escalates security information in response to detected cyber security occurrences, events and incidents.

Incident response

Containing, mitigating, and remediating cyber security incidents in collaboration with internal stakeholders.

Vulnerability management

This is the proactive identification, assessment, prioritisation, remediation, and ongoing monitoring of cyber security vulnerabilities. This activity helps us understand our weaknesses and plan mitigation activities accordingly.

Threat intelligence and threat hunting

Threat intelligence is the activity of collecting, processing and analysing data to understand a threat actor's motives, targets and attack behaviours. Threat intelligence enables us to make faster, more-informed, data-backed security decisions.

Threat hunting is a proactive activity that seeks out threat patterns that are not usually identified by cyber security technologies. This approach allows us to detect and mitigate cyber threats before they can cause disruption to our assets.

Digital Identity

[redacted] The core activities involved in this are:

- Internal and external platform enhancement – developing and enhancing all our current digital identity repositories located internally and in Software as a service (**SaaS**) solutions.
- Risk reduction – continuing to apply and enhance risk-reduction controls to multi-factor authentication, our conditional access policy, risky users and password policies.
- Role-based access – maintaining a secure role-based access control mechanism, and providing a framework for requestable and automatic role deployment, as well as supporting precise access for each individual.
- Identity lifecycle monitoring – monitoring and protecting digital identities, including continuing to develop access and provisioning, and ensuring lifecycle management (creation and separation) of the user identity cube and its subordinate accounts. Our goal is to build fluid and frictionless fit-for-purpose access as the user account changes over time.
- User experience (**UX**) collaboration – continued collaboration to increase the useability and user experience of the identity management system, which delivers efficiencies by allowing the customer to self-service.

Cyber Risk and IT Resilience

Cyber Risk and IT Resilience is responsible for documenting, mitigating and overseeing cyber security risk. A core function of this team moving forward is developing enhanced cyber security capabilities to mitigate evolving cyber security threats. Those activities are the subject of a separate business case (see **5.12.9 - Cyber Security Uplift business case**). However, the following operational risk and resilience activities are covered within this business case:

- managing the cyber security architectural resources for business projects
- overseeing the IT resilience function
- providing a security awareness program.

Operational Technology

Cyber Security architecture provides a high level of visibility of operational technology assets, with thorough monitoring and tightly managed network controls.

The architecture ensures that the system provides authorised users with access to services while protecting the availability, integrity and confidentiality of our OT infrastructure. The security architecture is scalable and flexible and supports additional services without compromising the level of security in the network. It is built in line with SA Power Networks' cyber security standards.

This business case covers the refresh of this cyber security architecture (infrastructure purchases and software updates) for the 2025–30 RCP.

Exclusions

This business case excludes:

- business application security patching, which is included in our IT Applications Refresh recurrent business case (refer Supporting Document 5.12.4);
- infrastructure security patching, which is covered by our IT Infrastructure Refresh recurrent business case (refer Supporting Document 5.12.7);
- the proportion of the recurrent cyber security investment (approximately one third) that is currently funded under operating expenditure and will be covered by the base year roll-forward; and
- enhancing cyber security capabilities to mitigate new and evolving threats, which is covered by our Cyber Security Uplift non-recurrent business case (refer Supporting Document 5.12.9).

3.2 Our performance to date

The 2020–25 recurrent cyber security business case proposed continued maintenance and updating of our cyber security capabilities and maintaining our risk exposure at current levels. Key achievements during the 2020–25 period to date include:

- developing an around-the-clock hybrid cyber security operations capability, aligning with the non-stop, 24x7 nature of our critical business operations, and allowing us to respond to all cyber threats in a timely manner;
- adopting a cyber threat-led approach to ensure we are focused on mitigating cyber-attacks from threat groups targeting energy organisations, both in Australia and globally;
- creating a Digital Identity Management capability;
- developing and building an external Customer Identity Access Management solution to provide a single identity store for all of our external identities; and

- avoiding any priority one (P1) cyber security incidents or notifiable data breaches[5].

Table 3 shows that our expenditure is tracking closely to the allowance for the RCP to date. While there has been a consistent level of activity over the period, there are some fluctuations in expenditure from year to year. This simply reflects a slight shift in emphasis on uplift activities, ie higher or lower levels of work performed on the non-recurrent program at different times, and therefore an offsetting change in the level of recurrent activities. The full RCP expenditure is expected to be very close to allowance.

Table 3: 2020–25 performance to date, $m real June 2022

Cost type	2020–21	2021–22	2022–23	2023–24	2024–25	Total 2020–25
Allowance	**2.9**	**3.9**	**4.1**	**3.4**	**3.5**	**17.8**
Actual/forecast	**3.4**	**2.7**	**2.7**	**4.7**	**4.0**	**17.5**

We are also undertaking an uplift program of work in the current RCP in response to increasing risk as well as additional regulatory requirements. The expenditure was allowed under SA Power Networks 2020-25 'Utilities Cyber Security uplift' business case. This program is also proceeding in line with expectations, [redacted] This is a testament to our commitment to cyber security and our efforts to ensure the reliability and security of our network. Further detail on the current period cyber security uplift program is provided in the 'Utilities Cyber Security uplift' business case[7].

3.3 Drivers for change

The increasing complexity, prevalence and targeted nature of cyber security threats

The threats against critical infrastructure are increasing rapidly within Australia. The Australian Cyber Security Centre's (**ACSC**) 2022 Cyber Threat Report[8] stated that 95 cyber security incidents occurred against critical infrastructure within the 2021–22 financial year. This threat is expected to continue to increase, with Gartner predicting that by 2025, 30% of critical infrastructure worldwide will experience a breach that will result in the halting of either operations or mission-critical cyber-physical systems. Within SA Power Networks, we have seen an escalating number of cyber events that have resulted in an incident over the last three years, as shown in Figure 2.

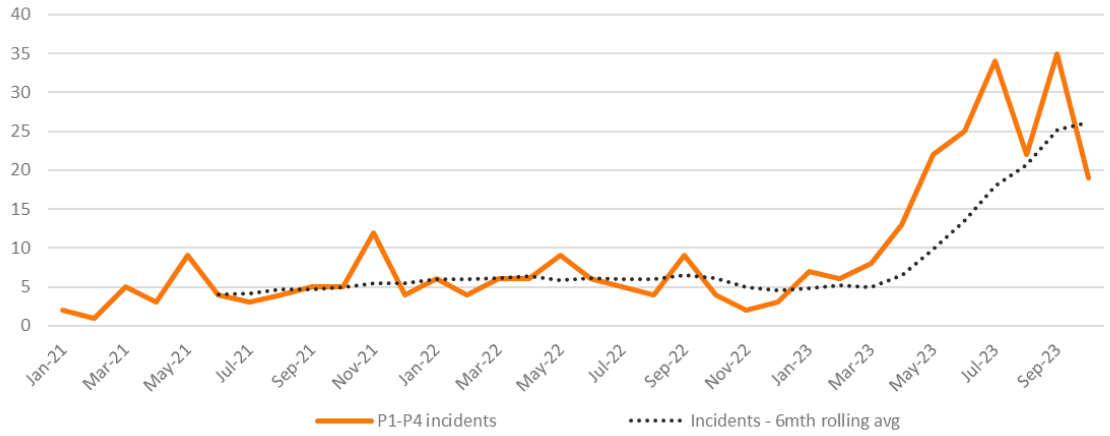
[5] Cyber security incidents are classified as to severity on a scale of P1 (most severe) to P4 (least severe).

[6] [redacted]

[7] Document 5.12.9

[8] ACSC-Annual-Cyber-Threat-Report-2022_0.pdf

Figure 2: SA Power Networks cyber incidents over last three years



A changing electricity distribution industry

Coupled with this, customer expectations of SA Power Networks are growing rapidly, as is the demand for new energy services. The network of the future[9] will continue to leverage a wider use of technology and will include more integration and data sharing between corporate IT and OT systems and devices, and a range of new market participants with varying cyber security practices and maturity levels. There is an overall greater connectivity and interaction with the energy market, a greater number of participants, and increased data collection and exchange in real time or near real time format. Greater trust will be placed in the data supporting decisions made within these environments. This has and will continue to create new challenges for maintaining a safe, secure and reliable distribution network. Our cyber security capabilities will be constantly challenged and we will need to consider new and emerging risks resulting from these industry changes.

Increased scale of operational cyber security activities

The outcome of these ongoing changes is continued growth in the cyber security user base across many operational activities, leading to a materially increased workload within these teams. Examples of this are:

- External user access to our systems
  We have upgraded several customer portals within the current RCP, including the Registered Electricians portal and Public Lighting portal. This has resulted in a significant increase in the number of external accounts, with large increases in the number of external users accessing our systems:
  - Between June and November 2023, there was an active user increase of the Registered Electricians portal of 523 users, equating to a 30% per annum increase.
- Number of incident volumes
  With SA Power Networks continuing to digitise processes and provide more digital capability into the hands of its users, there has been a significant increase in our cyber security incident volumes:
  - As described above and shown in Figure 2, the number of cyber security incidents that our team are dealing with has increased materially over the current period.
  - [redacted]

[9] SA Power Networks Future Operating Model 2016-2031 describes a multi-dimensional electricity system with more participants in the storage and generation of electricity.

These changes have necessitated an increase in capability to ensure we can effectively triage and investigate incidents in a timely manner and avoid a potential disruption to services. It is expected that the volume of activity covered within the teams supporting our operational cyber security capability will continue to grow into the next period.

[redacted]

3.4 Industry practice

In August 2018, Australian Energy Market Operator (**AEMO**) developed a cyber security capability framework and maturity model – the Australian Energy Sector Cyber Security Framework (**AESCSF**) – in collaboration with industry and government stakeholders[10]. This framework was designed to enable assessment of cyber security capability and maturity for Australian National Electricity Market (**NEM**) participants. SA Power Networks has self-assessed as a high-criticality business under this framework in both 2022 and 2023. [redacted]

As a result of the AESCSF requirements, as well as the high level of business risk associated with cyber security, all network service providers within the NEM are including cyber security uplift programs within their current cycle regulatory proposals. Other comparable electricity utilities to SA Power Networks also have an existing recurrent cyber security function.

[10] including AEMO, ACSC, Cyber and Infrastructure Security Centre (CISC), and representatives from Australian energy organisations [redacted]

4. The identified need

The underlying driver for investment action to be considered in this business case is the containment and mitigation of the existing risks associated with cyber security threats. [redacted]

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, National Electricity Law and jurisdictional regulations. As a result of these considerations, the identified need for our recurrent cyber security program is as follows:

a. to respond to customers' concerns[12], 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 due to cyber incidents, and
    - maintain safety service performance – driven by a desire to not see deterioration in the safety risk posed by the network.

b. to comply with applicable regulatory obligations/requirements[13], in this case with specific reference to:
    - [redacted]

c. to maintain the reliability, safety and security of our distribution network services and system, [redacted]

[12] 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.

[13] This is pursuant to Clause 6.5.7(a)(2) of the NER, which requires expenditure in order to comply with all appliable regulatory obligation s or requirements associated with the provision of standard control services.

[14] [redacted]

[15] AESCSF overview: https://aemo.com.au/-/media/files/initiatives/cyber-security/aescsf/aescsf-framework-overview.pdf?la=en, page 9

5. Comparison of options

5.1 The options considered

Table 4: Summary of options considered

Option	Description
Option 1: Maintain current level of investment	This option proposes a continued investment in operational cyber security activities at the actual/forecast levels for the 2020–25 RCP. Given that the majority of activities this business case covers are operational in nature, it is proposed that the treatment of these activities be reclassified as opex from the start of the 2025–30 RCP.
Option 2: Maintain current level of risk given existing threat levels	This option proposes maintaining the current cyber security risk level (given current threat levels). This involves maintaining our operations, digital identity and risk and resilience capabilities at the 20-25 RCP level, plus an additional $0.5 million to support the material increase in the volume of activity covered within the teams supporting our operational cyber security capability. As with Option 1, this option requires that the majority of the proposed investment be reclassified from capex to opex.

5.2 Options investigated but deemed non-credible

Any options for reducing the level of expenditure to less than current business as usual level have been deemed non-credible due to the extreme overall residual risk level associated with these.

Any options that involve continuing to treat operational activities covered by this business case as capital moving forward have been deemed inappropriate due to non-conformance with generally accepted accounting principles.

5.3 Analysis summary and recommended option

5.3.1 Options assessment results

Table 5: Costs, benefits and risks of alternative options relative to the base case, $m real Jun 2022.

Option	10-year program costs			2025–30 program costs			10-year benefits[16]	10-year NPV[17]	Overall risk rating[18]	Ranking
	Capex	Opex	Total	Capex	Opex	Total				
Option 1 – Maintain current level of investment	8.3	27.1	35.4	4.1	13.5	17.7	n/a	-29.2	**Extreme**	2
Option 2 – Maintain current level of risk given existing threat levels	5.5	30.7	36.2	2.9	15.3	18.2	n/a	-29.9	**Extreme**	1

[16] Represents the total capital and operating benefits, including any quantified risk reduction/management benefits, 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.

[17] 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%.

[18] The overall risk level for each option after the proposed option is implemented. Refer to Appendix C - risk assessment for details.

5.3.2 Recommended option

The interconnected and interdependent nature of our network requires security and resilience safeguards to protect our systems, processes and people from vulnerabilities that can cause disruption to these critical systems.

Option 2 is recommended to safeguard our services to the public of South Australia and to protect the integrity of the systems supporting the NEM. SA Power Networks must continue to maintain adequate risk mitigation controls to ensure the proactive identification of, and response to, existing security threats.

Option 2 will:

- result in less cyber security incidents successfully breaching SA Power Networks' defences,
- assist in decreasing the breadth, impact and severity of incidents when controls are bypassed or fail,
- enable us to adapt the control environment (cyber security systems and processes) quickly and effectively, to respond to changes in the threat landscape and environment complexity as they occur,
- enable us to adapt the control environment consistently and methodically across the corporate and operational environments, addressing many of the cyber security challenges associated with the changes in the electricity distribution industry,
- support incident response emulation exercises so we can be prepared and resilient to the threats we continue to face,
- enable us to protect sensitive customer and asset data, and
- enable us to maintain compliance with relevant legislative requirements such as *The Privacy Act* [redacted]

While Option 1 will provide for continuation of the existing level of investment, the funding level is insufficient to cover the increase in the scale of existing operational cyber security activities into the 2025–30 RCP.

This option includes a reclassification of the expenditure relating to operational IT cyber security activities from capex to opex. This is in line with:

- the appropriate accounting treatment for such activities
- consistency with how other comparable entities treat similar activities
- consistency with how similar activities are treated in the SA Power Networks 2025–30 Cyber uplift business case.

5.4 Scenario and sensitivity analysis

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

5.5 Option 1: Maintain current level of investment

5.5.1 Description

Continued growth in the level of cyber threats means that there is an ongoing imperative for all businesses to remain vigilant on cybercrime. The increase in threats targeted [redacted] the energy sector specifically, means there is a high risk associated with not continuing to maintain our existing capability level.

This option reflects a continuation of the existing level of investment in recurrent cyber security activities, to mitigate the existing level of threat. However, it does not provide for increases in the cyber security user base and the corresponding uplift in the volume of existing operational and digital identity activities that has occurred, and is expected to continue into the next period.

5.5.2 Costs

The Option 1 forecast is $17.7 million, of which $4.1 million is capex and $13.5 million is opex, as shown in Table 6.

Table 6: Option 1 – Costs by cost type ($m real June 2022)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Capex	0.8	0.8	0.8	0.8	0.8	**4.1**
Opex	2.7	2.7	2.7	2.7	2.7	**13.5**
Total	**3.5**	**3.5**	**3.5**	**3.5**	**3.5**	**17.7**

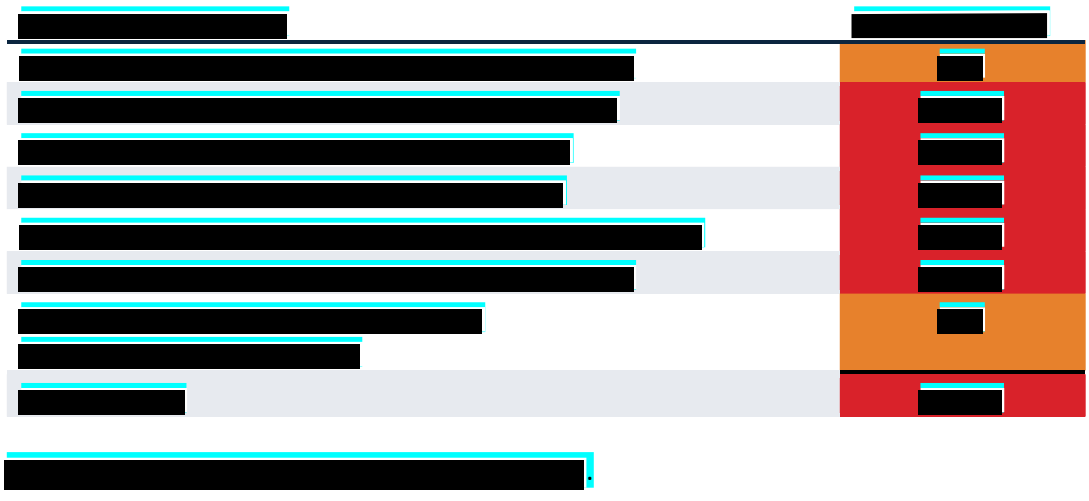
Given that this option is based on the continuation of the existing level of investment, the 2020-25 RCP average spend level has been used to determine the forecast (see Table 3).

Cost models are listed in Appendix A.

As discussed in section 3.3, this investment to maintain our cyber security capability is required to be reclassified as operating expense for consistency with accounting standards. This proposed treatment is supported by an independent assessment from BDO Australia[19]. Consistent with other accounting classification changes this is proposed as a step change, as summarised in Appendix B.

5.5.3 Risks

Table 7: Risk assessment summary



[19] External Review of ICT Cyber Expenditure Treatment, document 5.12.24
[20] The level of risk post current controls (ie after considering what we currently do to mitigate the risk).

[redacted]

5.5.4 Quantified benefits

There are no tangible quantifiable benefits associated with this option.

5.5.5 Unquantified benefits

Benefits of this option include:

- a strong enterprise-wide awareness of cyber security threats and risks
- protection of the data that our people, our customers and the public entrust to us
- management of sensitive data through our modern digital identity management solution

5.6 Option 2: Maintain current level of risk given existing threat levels

5.6.1 Description

Option 2 proposes maintaining the current cyber security risk level (given current threat levels) for our OT and IT systems and data.

The increase in threats targeted at [redacted] the energy sector specifically, mean that there is a high risk associated with not continuing to maintain our existing capability level. As discussed in section 3.3, there are a significant number of drivers for change in the cyber security area. Much of this change is catered for by the SA Power Networks Cyber Security Uplift business case included as part of this submission, as it relates to an uplift in the maturity level of our capabilities to support the increased threat levels anticipated in the 2025-30 period. However, that uplift business case does not cater for the large increase in the scale of existing capabilities, at current threat levels, that is discussed in section 3.3. Funding to cover an increase in the scale of existing activity levels has therefore been included in this business case within this option.

For the Operational Technology area, the required refresh works have been assessed based on equipment coming to the end of its useful life, with the most urgent works prioritised based on risk. [redacted]

5.6.2 Costs

The Option 2 forecast is $18.2 million, of which $2.9 million is capex and $15.3 million is opex, as shown in Table 8.

As per Option 1, this option proposes that the ongoing investment to maintain cyber security operational capabilities in the IT area be reclassified as operating expense, reflecting the appropriate accounting treatment for such activities. This is proposed as an opex step change (capex to opex shift) - further details of this are provided in Appendix B.

Table 8: Option 2 – Costs by cost type ($m real Jun 2022)

Cost type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Capex	0.5	0.5	0.8	0.5	0.5	**2.9**
Opex	3.1	3.1	3.1	3.1	3.1	**15.3**
Total	**3.6**	**3.6**	**3.9**	**3.6**	**3.6**	**18.2**

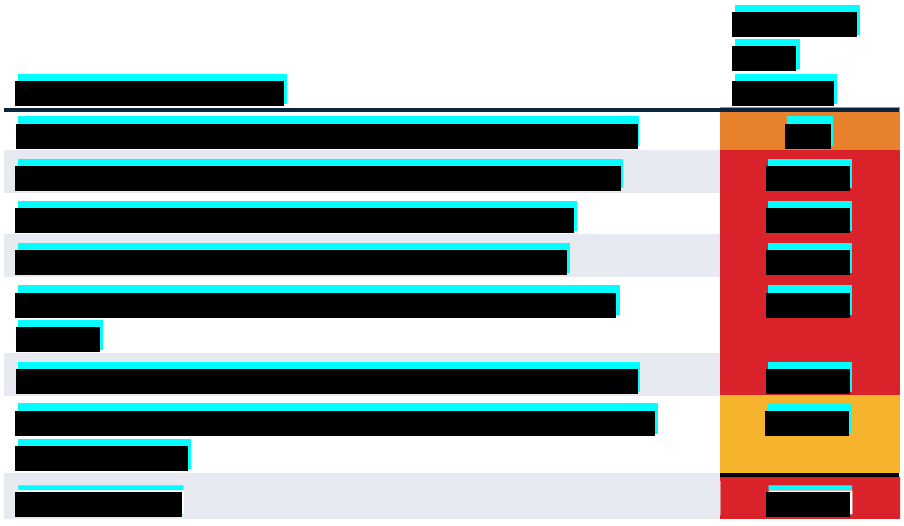
For Information Technology, the activities performed are ongoing and consistent from year to year. As a result, the forecast reflects the average 2020-25 RCP investment included in Option 1, increased to cater for the expected additional activity level.

For the Operational Technology area, the forecast is based on an estimate of the equipment items discussed above that require refresh.

Cost models are listed in Appendix A.

5.6.3 Risks

Table 9: Risk assessment summary



[redacted]

[21] The future level of risk once treatments proposed in this option have been implemented.

[redacted]

5.6.4 Quantified benefits

There are no tangible quantifiable benefits associated with this option.

5.6.5 Unquantified benefits

Benefits of this option include:

- a strong enterprise-wide awareness of cyber security threats and risks
- protection of the data that our people, our customers and the public entrust to us
- management of sensitive data through our modern digital identity management solution
- a reduction in the operational impact of cyber security incidents, service degradations and outages
- a reduction in the risk of reputational damage caused by cyber security incidents
- a reduction in the risk of legal and regulatory non-compliance caused by cyber security incidents, service degradations and outages.

6. Deliverability of recommended option

There is a stable recurrent cyber security capability in place within SA Power Networks. Additional resources will be developed inhouse through recruiting and upskilling graduates who work alongside experienced staff. We therefore do not foresee any issues with delivering this level of activity over the next RCP.

7. How the recommended option aligns with our engagement

SA Power Networks is committed to ensuring our business operations align with customer needs and priorities. By actively seeking input from stakeholders and customers, we ensure that decisions are informed by the needs and priorities of those they serve. This approach not only helps to improve customer satisfaction but also ensures our organisation is well-positioned to adapt to changes in the energy landscape and emerging technologies.

Customer engagement for the SA Power Networks 2025–30 Reset largely consisted of a two-part process. The first of these was a series of Focused Conversations workshops with key stakeholders and customers, aimed at delving deeper into priority topics and gaining a better understanding of our customers' current needs and future priorities for electricity. The second component of the Customer Engagement Program was a People's Panel two-day workshop. This was attended by a broad range of stakeholders who represent the community, including businesses, renewables, youth, regional stakeholders, customer advocacy groups, local government representatives and multicultural board members.

A significant focus of the IT component of these engagements related to cyber security, with both panels recommending an uplift in investment relative to the current expenditure level. That the second engagement (People's Panel) outcome was to support a level of funding for SA Power Networks cyber security capability above the highest AESCSF maturity level (Security Profile (**SP**) 3) in the 2025–30 RCP, highlights the high importance our customers attribute to cyber security health and mitigating these risks.

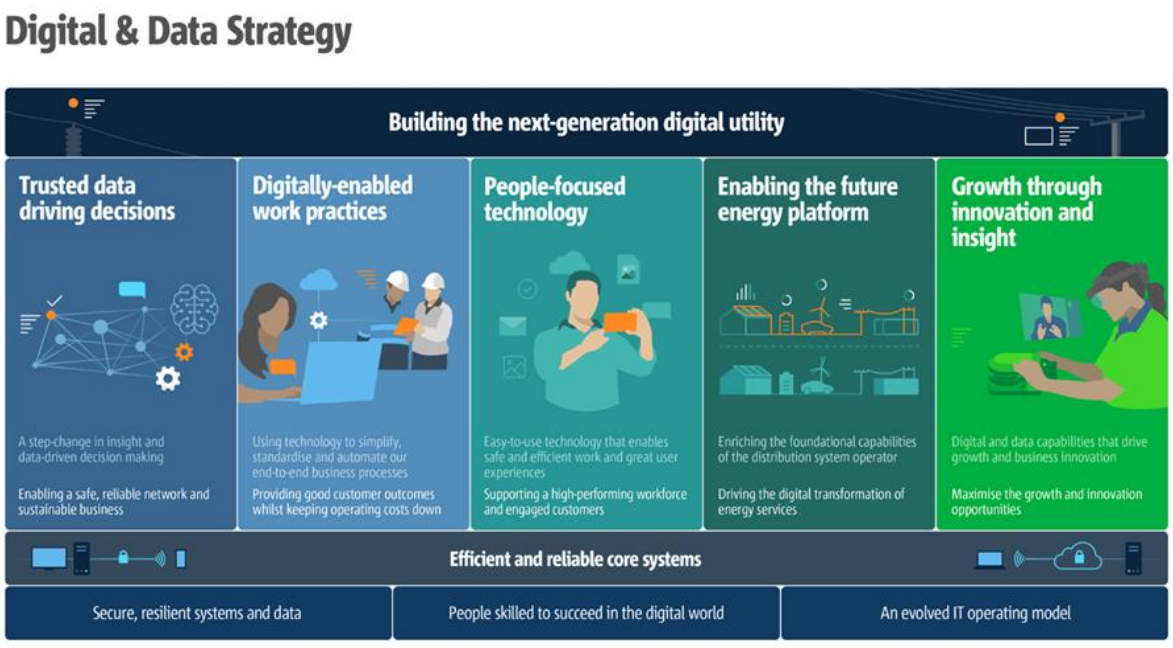
8. Alignment with our vision and strategy

SA Power Networks is the sole electricity distributor and plays an essential role in powering South Australia. As the utilities model evolves and energy sources become more distributed, we are adapting to the changing landscape by incorporating new technologies and data-driven approaches to meet customer needs and to optimise their operations. However, the increasing reliance on technology comes with the need for a strong cyber security posture to protect against cyber threats and ensure the safe and reliable operation of the electricity grid.

Our Digital and Data Strategy outlines the long-term strategic direction for IT, with a strong cyber security posture ('secure and resilient systems and data') highlighted as a critical enabler of this strategy. With data being a core enabler across the business in achieving desired outcomes over the next regulatory horizons, the strategy acknowledges that a cyber security breach could have significant consequences not only for the company but also for the wider community. Continued investment in recurrent cyber security activities supports the success criteria listed in the Digital and Data Strategy, in particular:

- Reduced time to identify, react and respond to incidents
- Continued movement towards proactive threat identification and management
- Resilient IT infrastructure and supporting processes
- Modern digital identity management

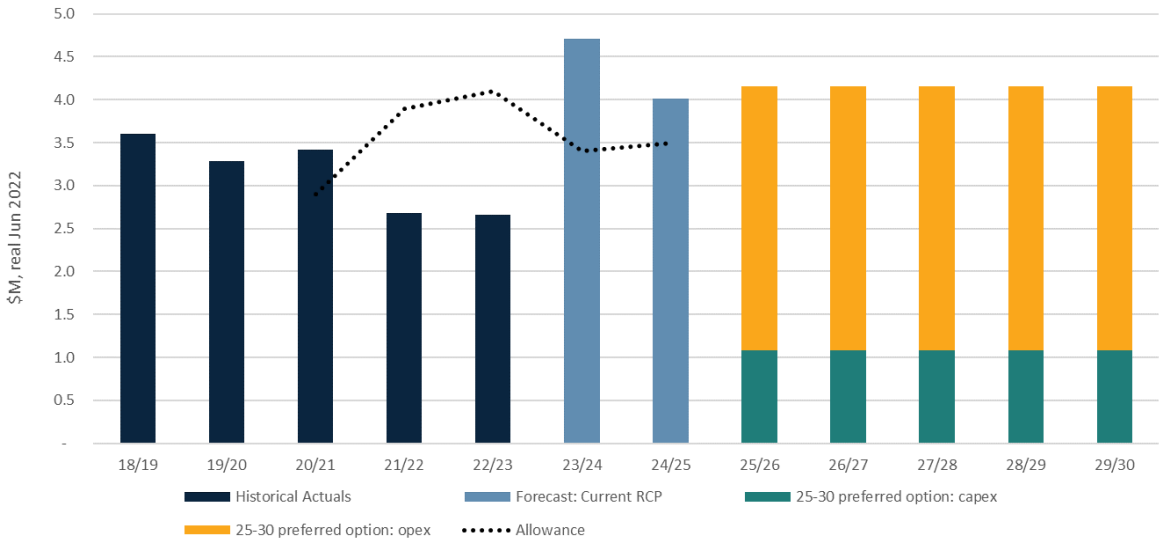
Figure 3: SA Power Networks Digital and Data Strategy



9. Reasonableness of cost and benefit estimates

The cost estimate for the proposed Option 1 reflects the evidenced cost of maintaining our cyber security capabilities (given the existing threat level) over time, plus an uplift to support the required increase in recurrent cyber security activity, as shown in Figure 4. This represents approximately 4% uplift above 2020-25 RCP levels, which is well below the increase in operating parameters that SA Power Networks has seen over the last five years across much of the operational cyber security environment.

Figure 4: Recurrent cyber security investment trend over time



10. Reasonableness of input assumptions

This business case assumes consistent inputs to those seen in the last five years; that is:

- a consistent level of resourcing
- a consistent resourcing mix.

A. Appendix A – cost models

Option 1:
2025 - 30 Reset - Cyber Security (recurrent) forecast template - Option 0.xlsm

Option 2:
2025 - 30 Reset - Cyber Security (recurrent) forecast template - Option 1.xlsm

B. Appendix B: Step Change (Preferred option)

Category	Application function	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Capex – Opex shift	Recurrent cyber security	3.1	3.1	3.1	3.1	3.1	15.3
	Total step change	**3.1**	**3.1**	**3.1**	**3.1**	**3.1**	**15.3**

Accounting treatment change

Topic	Detail
Background	[redacted]
Request	A step change of $15.3m ($3.1m per annum) as substitution for a similar value of capex.