



Business case: ICT Non- Recurrent - Cyber Security Uplift

2025-30 Regulatory Proposal

Supporting document 5.12.9

January 2024

Contents

Glossary.....	3
1. About this document.....	5
1.1 Purpose.....	5
1.2 Expenditure category	5
1.3 Related documents.....	5
2. Executive summary	6
3. Background	8
3.1 The scope of this business case.....	8
3.1.1 Exclusions	9
3.2 Our performance to date.....	10
3.3 Drivers for change	12
3.4 Industry practice.....	17
4. The identified need	19
5. Comparison of options	21
5.1 The options considered	21
5.2 Options investigated but deemed non-credible	22
5.3 Analysis summary and recommended option	22
5.3.1 Options assessment results.....	22
5.3.2 Recommended option	23
5.4 Option 0 – Do Nothing.....	24
5.4.1 Description	24
5.4.2 Costs.....	25
5.4.3 Risks	25
5.4.4 Quantified benefits	25
5.4.5 Unquantified benefits	25
5.5 Option 1: Basic controls.....	26
5.5.1 Description	26
5.5.2 Costs.....	28
5.5.3 Risks	28
5.5.4 Quantified benefits	29
5.5.5 Unquantified benefits	30
5.6 Option 2: Risk-based approach to cyber security.....	31
5.6.1 Description	31
5.6.2 Costs.....	44
5.6.3 Risks	45
5.6.4 Quantified benefits	45
5.6.5 Unquantified benefits	46
5.7 Option 3: Risk-based approach + Comply with AESCSF SP-3	47

5.7.1	Description	47
5.7.2	Costs.....	48
5.7.3	Risks	48
5.7.4	Quantified benefits	49
5.7.5	Unquantified benefits	50
6.	Deliverability of recommended option.....	51
7.	How the recommended option aligns with our engagement	53
7.1	Alignment to the views of other stakeholders.....	54
8.	Alignment with our vision and strategy.....	55
9.	Reasonableness of cost and benefit estimates.....	56
10.	Reasonableness of input assumptions.....	62
11.	Scenario and sensitivity analysis.....	63
B.	65
C.	Appendix C – How the controls address the key drivers.....	70
D.	Appendix D – How the controls mitigate the risks.....	71
E.	Appendix E – Cost models	72
F.	Appendix F – Opex step-changes (Preferred option)	73

Glossary

Acronym / term	Definition
ACSC	Australian Cyber Security Centre
ADMS	Advanced Distribution Management System
AEMO	Australian Energy Market Operator
AER	Australian Energy Regulator
AESCSF	Australian Energy Sector Cyber Security Framework
ASD	Australian Signals Directorate
ASIO	Australian Security Intelligence Organisation
BYOD	Bring Your Own Device
Capex	Capital expenditure
CISC	Cyber and Infrastructure Security Centre
DLP	Data Loss Prevention
DEM	Department of Energy and Mining
DNSP	Distribution Network Service Provider
ES-C2M2	United States Energy Sector Cyber Capability Maturity Model
EUD	End user device
FTE	Full-Time Equivalent
GWh	Gigawatt hour
ICT	Information and Communication Technology
ISM	Australian Information Security Manual
IT	Information Technology
MFA	Multi-Factor Authentication
MIL	Maturity Indicator Level
NATO	North Atlantic Treaty Organisation
NDR	Network Detection and Response
NEL	National Electricity Law
NEM	National Electricity Market
NER	National Electricity Rules
NIST	National Institute of Science and Technology
NPV	Net Present Value
Opex	Operating expenditure
OT	Operational Technology
OWASP	Open Worldwide Application Security Project
RaaS	Ransomware as a Service
RBAC	Role-Based Access Control
RCP	Regulatory Control Period
SaaS	Software as a Service
SACOSS	South Australian Council of Social Service
SAMM	Software Assurance Maturity Model
SCADA	Supervisory Control and Data Acquisition
SECOPS	Security operations
SLACIP Act	The Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
SOCI	The Security of Critical Infrastructure Act 2018
SOMM	Security Operations Maturity Model

Acronym / term	Definition
SoNS	Systems of National Significance
SP	Security Profile
SSDLC	Secure Software Development Lifecycle
ToT	Tool of Trade
VCR	Value of Customer Reliability
ZTA	Zero trust architecture

1. About this document

1.1 Purpose

This business case presents the economic justification to cost-effectively address the increased cyber security risks that are expected to emerge over the next decade. As an infrastructure organisation responsible for delivering electricity to customers in South Australia, SA Power Networks faces an increasingly complex and evolving threat landscape. Such cyber security risks materialising could cause significant harm to our operations, and therefore the continuity of core services provided to our customers.

1.2 Expenditure category

- Non-network Information and communication technology (ICT) Capital Expenditure (**Capex**): non-recurrent – compliance
- Non-recurrent ICT Operating Expenditure (**Opex**): Step Change- external factor

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
5.12.4 - IT Applications Refresh Business Case	SA Power Networks	Jan 2024
5.12.6 - Cyber Security Refresh Business Case	SA Power Networks	Jan 2024
5.12.7 - IT Infrastructure Refresh 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
Digital and Data Strategy	SA Power Networks	Jan 2024
IT Asset Management Plan	SA Power Networks	Jan 2024

2. Executive summary

This business case recommends spending \$44.7 million¹ in the 2025–30 Regulatory Control Period (**RCP**) to uplift our cyber security and Information Technology (**IT**) resilience capabilities to a level that adequately addresses expected threats.

Cyber threats are constantly evolving, with critical infrastructure networks targeted globally by both state and criminal cyber actors. Over the 2020–25 RCP, the critical infrastructure threat landscape has evolved rapidly, with a proliferation of new tactics, techniques and procedures being implemented and undertaken by cyber threat actors and criminals. This has escalated the number and seriousness of threats faced by SA Power Networks with utilities, including those within the energy sector, having fallen under increasing attention. This is evidenced by sophisticated cyberattacks against critical infrastructure in several global jurisdictions.²

Moving forward, threats will continue to evolve and increase in prevalence and sophistication. Gartner³ predicts that by 2025, 30% of critical infrastructure organisations will experience a security breach that will result in the halting of an operational or mission-critical cyber-physical system. Gartner also predicts that in the same timeframe, attackers will have weaponised a critical infrastructure cyber-physical system to successfully harm or kill humans.

With the growth in threat level, the Australian Energy Sector Cyber Security Framework (**AESCSF**) was developed in 2018 in collaboration with industry and government stakeholders, including the Australian Energy Market Operator (**AEMO**).

We have a mature and stable cyber security function, with an ongoing recurrent level of investment that allows us to manage risks for today’s level of cyber threat. We are uplifting our cyber maturity during the current period in response to current threats being experienced. However, with the continued increase in threat levels currently being observed, the disconcerting predictions noted above and the increased legislative obligations, there is a clearly evidenced need to significantly enhance our cyber security capabilities in coming years. Enhancement is needed to ensure adequate protections that minimise the likelihood as well as limit the impact of compromise or damage to our critical assets, ensuring the continuation of critical services as expected by our customers.

This business case proposes a threat-based and risk-based approach to uplifting our cyber security capabilities to minimise and mitigate increasing cyber security risks. The **2025–30 RCP forecast of \$44.7 million** expenditure for the program includes **\$2.6 million of capex and \$42.1 million in opex** (step change) to ensure the changes are maintained and risk is managed on an ongoing basis. This forecast represents the most efficient option to enable us to mitigate cyber security risks for the remainder of this decade.

Other options considered were:

- in addition to the risk-based activities, to complete the implementation of all controls (practices and anti-patterns⁴) in the AESCSF SP-3 level (\$47.5 million); and

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

² [Sandworm Disrupts Power in Ukraine Using a Novel Attack Against Operational Technology | Mandiant \(mandiant.com\)](#).

³ [Gartner predicts 30% of critical-infrastructure organisations will experience a Security Breach by 2025 | Gartner \(gartner.com\)](#).

⁴ The AESCSF consists of implementing a number of ‘practices’ (good behaviours) as well as addressing ‘anti-patterns’ (indicators of bad practice).

- to provide a minimal uplift in capabilities that would allow us to address only our most critical cyber security gaps (\$10.4 million).

The preferred option was selected because:

- it delivers a prudent reduction in cyber security risk, incorporating appropriate practices from the AESCSF as well as other relevant frameworks. This includes addressing key aspects absent from the AESCSF framework such as an enhanced Operational Technology (OT) security capability, a boosted information protection and awareness program, and a 'bring your own device' security capability;
- it delivers the majority of controls included within AESCSF SP-3, which we expect will be a legislated requirement at some point in the future; and
- not constraining our investment to the current AESCSF framework was supported by our customers via the People's Panel recommendations, in noting that: "The consequences of inadequate spending on cyber are catastrophic, and we are not willing to accept this risk as a community"⁵.

Together with our ongoing program to maintain existing cyber security capabilities⁶, the uplift in maturity and capability provided by the preferred option in this business case will minimise and manage the substantial risks of a failure of cyber security practices. Delivering this will ensure that our customer services remain secure, reliable and available, and are provided at the lowest possible cost. By 2030, this will result in a stronger and more resilient energy network capable of proactively managing areas of risk, using automation to supplement the workforce as well as reduce response times, and provide a single trusted identity for all ICT users at SA Power Networks.

Table 2: Options assessment summary, \$million, June 2022⁷

Option	Total program costs			2025–2030 costs			Program or 10-year estimates		Residual risk rating ⁸
	Capex	Opex	Total	Capex	Opex	Total	Benefits	NPV ⁹	
1. Basic controls	0.8	16.9	17.8	0.8	9.6	10.4	85.6	48.2	Extreme
2. Risk-based approach	2.6	68.9	71.4	2.6	42.1	44.7	225.7	107.0	Medium
3. Risk-based approach + Comply with AESCSF SP-3	2.6	71.7	74.3	2.6	45.0	47.5	225.9	104.6	Medium

⁵ [SA Power Networks People's Panel: Final Report – Balancing Service & Price, pages 21 & 22 | SA Power Networks \(talkingpower.com.au\)](https://talkingpower.com.au)

⁶ See SA Power Networks ICT Recurrent Cyber Security Refresh Business Case, document 5.12.6.

⁷ Note: Totals presented in tables throughout this document may not exactly match the sums of individual figures due to rounding.

⁸ The overall risk level for each option after the proposed option is implemented. Refer to Appendix B – risk assessment for details.

⁹ 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, critical 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.

As a [REDACTED] infrastructure provider that is responsible for distributing electricity to customers in South Australia, we have a duty to maintain the reliability, availability, and safety of our electricity network.

[REDACTED]

[REDACTED]

In August 2018, AEMO developed a cyber security capability framework and maturity model – the AESCSF – in collaboration with industry and government stakeholders. This framework was designed to enable assessment of cyber security capability and maturity for Australian National Electricity Market (NEM) participants. The AESCSF leverages existing frameworks, such as the National Institute of Science and Technology (NIST) cyber security framework, the United States Energy Sector Cyber Capability Maturity Model (ES-C2M2), ISO27001, and the Australian Information Security Manual (ISM). Version 2 of this framework has now been released in late 2023.

Under the AESCSF, SA Power Networks is classified as a high criticality Distribution Network Service Provider (DNSP). This is the outcome from our 2022 and 2023 assessments under the AESCSF Electricity Criticality Assessment Tool, which uses basic business inputs and then provides an assessment of business criticality. As the sole DNSP in South Australia, we are responsible for providing electricity to more than one million customers across the state, as well as to more than twenty thousand critical and commercial customers each year, delivering between ten and fifteen thousand gigawatt hour (GWh) of power annually. A high criticality utility’s target state under the AESCSF is the 3rd maturity level (SP-3).

3.1 The scope of this business case

Key activities covered in the cyber security function are:

- **Cyber security operations** – includes logging, monitoring, detecting, and responding to cyber security incidents, vulnerability management, basic threat intelligence collection and threat hunting.
- **Digital identity management** – includes managing the digital identity, identifying lifecycle monitoring, applying risk reduction controls, and developing/enhancing digital identity repositories.

10 [REDACTED]

- **Cyber risk and Resilience** – includes managing the cyber security architectural resources for business projects, overseeing the IT Resilience function, and providing a security awareness program.
- **Operational Technology** – includes the periodic refresh of cyber security architecture (infrastructure purchases and software upgrades) to provide visibility of operational technology assets via monitoring and tightly managed network controls.

Ongoing recurrent investment in these activities is essential for funding the resources and software required to maintain our current level of cyber security maturity, given the existing threat level¹³. However as described above, the evolving threat landscape and the related compliance obligations mean that organisations must take significant additional proactive measures to improve their cyber security maturity, ensuring that their operations remain secure and resilient into the future.

To start to address these risks, a business case to begin to uplift capability towards the required cyber security maturity levels was approved by the Australian Energy Regulator (**AER**) in the 2020-25 Determination for SA Power Networks. While we have made significant progress towards a higher level of maturity in the current RCP, more effort is required to ensure continued risk mitigation and compliance with obligations into the future. This business case considers the additional uplift in capability and corresponding investment required in the 2025–30 RCP to achieve these critical requirements.

3.1.1 Exclusions

This business case excludes:

- maintaining our existing cyber security capabilities, which is partly covered by our Cyber Security Refresh business case¹⁴ and partly funded via opex and covered by the base year roll-forward;
- uplift to support an increase in the scale of existing cyber security capabilities associated with continued growth in the cyber security user base across many operational activities. This is also covered by our Cyber Security Refresh business case;
- business applications security patching, which is included in our IT Applications Refresh business case¹⁵; and
- infrastructure security patching, which is covered by our IT Infrastructure Refresh business case¹⁶.

There is no overlap between expenditure included in this business case and expenditure in other business cases. Specifically, all new and existing cyber-security-related expenditure (IT and OT) is covered in this business case, our Cyber Security Refresh business case, and base-year opex. There is no new or existing cyber-security-related investments across any other business cases in our 2025–30 Regulatory Proposal.

¹³ This recurrent investment is partly covered under operating expenditure (i.e. funded under the base-year roll-forward), with the remainder being the subject of SA Power Networks Cyber Security Refresh business case (Document 5.12.6) included in this submission.

¹⁴ Document 5.12.6 - Cyber Security Refresh Business Case

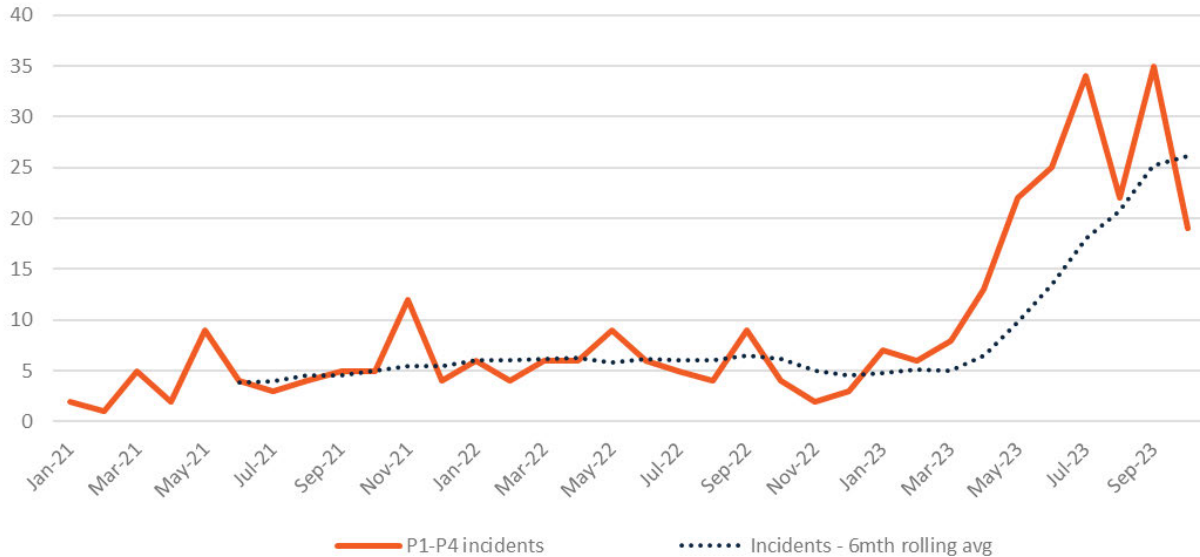
¹⁵ Document 5.12.4 - IT Applications Refresh Business Case

¹⁶ Document 5.12.7- IT Infrastructure Refresh Business Case

3.2 Our performance to date

Our operating environment has received a growing number of cyber security breaches in recent years. Figure 1 shows the number of breaches since the start of the current RCP.

Figure 1: SAPN Cyber actual breaches over least three years



In expectation of this escalating threat, we submitted an uplift program for the 2020-25 RCP. This approved program sought to ‘largely complete’ AESCSF Maturity Indicator Level (MIL) 3 controls by the end of 2024¹⁷. However, the rapidly changing cyber security environment resulted in:

- a change in the AESCSF requirements, with version 2 of the AESCSF replacing version 1, resulting in a large number of additional controls and a significant additional scope of work associated with them;
- a large rise in the cost of security personnel due to the surge in competition for resources from businesses both within and external to our industry; and
- significant increases in real costs of software licencing for cyber security related products.

In addition, we have a more mature understanding of the threats we face and consider that any single generic framework is unlikely to adequately fully respond to the complexity of every organisation. The upside of the proliferation of threats is a significantly expanded range of frameworks available, many of which are focussed on mitigating specific risks.

As a result of these changes, we rationalised and reprioritised our cyber security uplift activities, using a proactive risk-based approach to prioritising controls to achieve the greatest risk reduction in the areas that we assessed as requiring immediate attention. This included configuration reviews, incident response plans, privacy compliance, program updates, industry participation, risk management, logging and monitoring, threat and vulnerability management, workforce responsibilities, training evaluation, and awareness effectiveness. It included implementing some controls that sit outside of the AESCSF framework, such as:

- automation that reduces the time taken to reset account passwords, reducing the impact of a cyber incident;

¹⁷ The business case specified meeting the majority of AESCSF ‘MIL-3’ practices, as opposed to SP-3. Consistent with regulatory requirements, evaluation of maturity has now changed to using the Security Profile (SP) classification.

- detective controls, [REDACTED], to allow us to highlight potential attack paths, as well as areas of weakness with our identities; and
- breach and attack simulation software that allows us to assess our vulnerabilities and verify the implementation of controls.

[REDACTED]

[REDACTED]

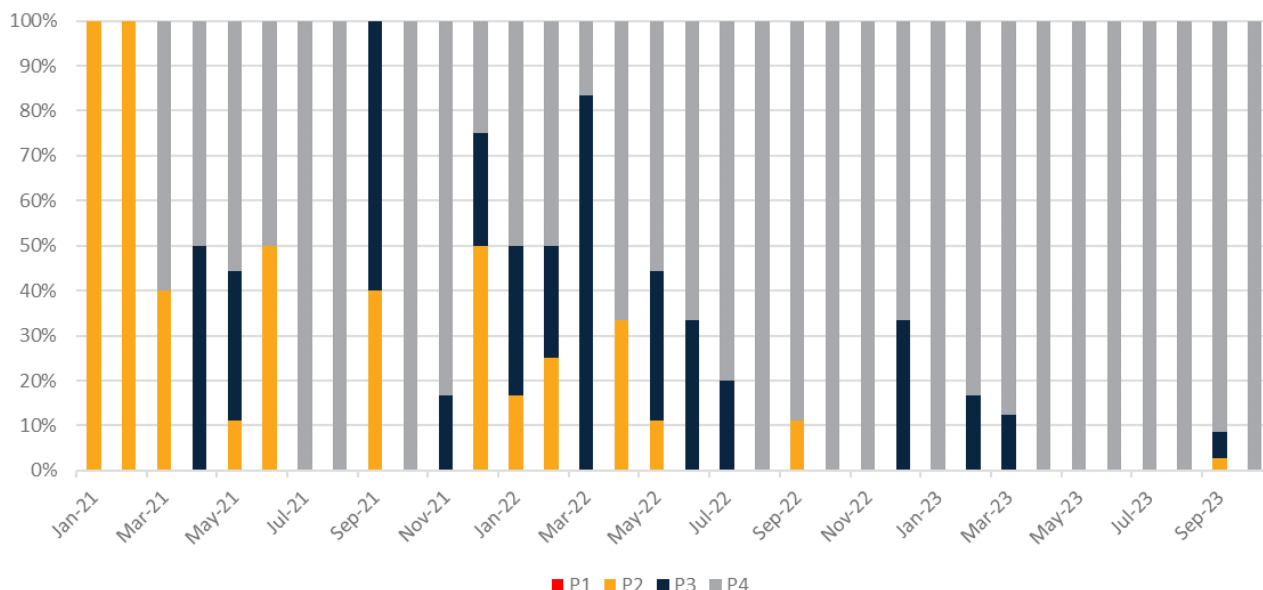
This uplift program has led to a large reduction in high impact cyber security incidents. We classify cyber security incidents using the Enterprise Risk Framework, according to the result of the event, e.g. theft of sensitive data, unauthorised access to our systems or data availability. While over the 2020-25 RCP the total number of cyber security incidents increased, Figure 3 shows that the rate of high severity incidents²⁰ has decreased over the period. This reflects the strength of the additional embedded controls from the current uplift period, despite the increasing threat level.

¹⁸ It must be highlighted that counting controls comes with significant limitations. Many of the controls that have already been implemented have been prioritised because these are relatively simple and so we were able to achieve ‘quick wins’. The controls remaining to be implemented are on average far more complex, time-consuming and costly.

¹⁹ Based on a self-assessment of the new AESCSF version 2 controls and conversion of existing AESCSF version 1 controls that were independently reviewed by KPMG.

²⁰ Cyber security incidents are classified as to severity on a scale of Priority 1 (P1 - most severe) to Priority 4 (P4 - least severe).

Figure 3: Breach consequence over the 2020-25 RCP



The current RCP forecast expenditure to deliver this uplift in our cyber security maturity is \$6.2 million, compared to the \$5.7 million AER forecast / allowance, as shown in Table 3. While we are delivering controls based on our highest priority risks, our existing resource capacity cannot accommodate delivering any additional controls during the current RCP. It is also evident that a risk-based approach to the order of control implementation is the most effective way to reduce cyber security risk.

Table 3: SP-2 uplift program, \$million, June 2022

	2020–21	2021–22	2022–23	2023–24 F	2024–25 F	TOTAL
Allowance	-	1.9	2.6	1.2	-	5.7
Actual/forecast	-	1.9	1.3	1.3	1.7	6.2

3.3 Drivers for change

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

Threats against critical infrastructure are increasing rapidly in Australia. The Australian Cyber Security Centre’s (ACSC) 2022 Cyber Threat Report²¹ stated that 95 Cyber Security incidents occurred against critical infrastructure in the 2021–22 financial year. Cyber threats to Australia’s critical infrastructure is an enduring concern, because the social or economic wellbeing of the nation depends on critical infrastructure assets working in cohesion.

The most relevant recent critical infrastructure incident is where the corporate network of the Queensland electricity generator CS Energy was targeted by the Russia-aligned Conti ransomware group. CS Energy became aware of a ransomware incident affecting its corporate network and immediately severed the external internet connection to its corporate network and initiated business continuity procedures. This had a significant impact to the organisation’s operations and resulted in considerable resource effort and financial cost to respond to the incident.

²¹ [ACSC Annual Cyber Threat Report 2022 | Australian Signals Directorate \(cyber.gov.au\)](https://www.cyber.gov.au/australian-signals-directorate/annual-cyber-threat-report-2022)

In May 2023, the ACSC, together with multiple agencies around the world, released a report into a recently discovered cluster of activity affecting networks across US critical infrastructure sectors. The attacker techniques outlined in the report were assessed by the authoring agencies as posing a significant risk to the critical infrastructure sector²². Further to this, many of the behavioural indicators included in the report can also be legitimate system administration commands that appear in benign activity. This report highlights the targeted nature of this compromise, adding to the complexity of identifying future compromises.

This threat is predicted to increase year on year, 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 systems²³.

Increasing compliance obligations

As the sophistication of adversaries grows, it is the role of government to create legislation to protect the public from these attacks. [REDACTED]

[REDACTED] As the cyber security landscape continues to evolve and the importance of protecting critical infrastructure becomes more evident, regulatory bodies are likely to enforce stricter cyber security measures to ensure the resilience and security of essential services.

A changing electricity distribution industry

Customer expectations of SA Power Networks, as well as the demand for new energy services, is growing rapidly. As a DNSP, we continue to facilitate the transformation to a distributed energy system and as we do, our importance to the NEM grows.

The future network²⁴ will continue to leverage a wider use of technology and include more integration and data sharing between corporate IT and OT systems and devices and a range of new market participants that have varying cyber security practices and maturity levels.

This dependency on technology exposes the energy sector to an unprecedented level of cyber security risk. 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 that supports 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.

Recent reporting indicates that the energy sector is not immune to targeted malicious software. In October 2022, a malicious software known as a 'wiper', with intent to render systems unusable, was used against an energy sector organisation in Ukraine²⁵.

²² [People's Republic of China \(PRC\) State-Sponsored Cyber Actor Living Off the Land to Evade Detection | Australian Signals Directorate \(cyber.gov.au\)](#)

²³ [Gartner Predicts 30% of Critical Infrastructure Organisations Will Experience a Security Breach by 2025 | Gartner \(gartner.com\)](#)

²⁴ [SA Power Networks Future Operating Model 2016-2031](#) describes a multi-dimensional electricity system with more participants in the storage and generation of electricity.

²⁵ [APT activity report T3 2022 | ESET \(welivesecurity.com\)](#)

Escalating ransomware threat

The ACSC’s 2022 Cyber Threat Report shows an increase in the trend of ransomware attacks, with the agency responding to 135 incidents involving ransomware – a 75% increase from their 2019–2020 report. Despite regular backups being a common mitigation strategy, victims may still face reputational damage from double extortion tactics²⁶. In 2022, ransomware actors continued to incorporate additional extortion tactics to more effectively extract payment from victims.

Critical infrastructure organisations have been attacked, with wide reaching impact to consumers across the country. Recently, the Darkside cybercrime group infected the IT environment of Colonial Pipeline with ransomware, effectively locking key business systems, including the billing system. The billing system relies on data from Colonial Pipeline’s OT environment to measure gas usage and bill customers, with this data exchange from OT into IT being key to the financial operation of the business.

This resulted in the most materially significant cyberattack in the history of the United States. As the ransomware rendered the billing system inoperable, Colonial Pipeline, which services the south-eastern United States, took the unprecedented step of disabling the gas pipeline.

Through deep analysis of our attack surface, we identified that, in quarter one of 2023, we were actively targeted by known cybercriminal groups attempting to deploy ransomware. During this period, we were scanned more than 11,000 times by a notorious threat actor group known as ‘Royals’, with the intent to deploy the Royal ransomware variant. Royal actors have been attributed to numerous targeted attacks against critical infrastructure sectors including, but not limited to, manufacturing, communications, healthcare and public healthcare and education. In addition to encrypting files, Royal actors also engage in double extortion tactics where they threaten to publicly release the encrypted data if the victim does not pay the ransom.²⁷

Growing supply chain risk

Supply chain risk is an increasing concern for us, as the interconnectivity of IT and OT environments presents potential threats to the security and resilience of operations. The ACSC’s 2022 Cyber Threat Report highlights the growing trend of malicious actors targeting the supply chain as a priority vector for compromise.

We also continue to see a rise in attacks in the software components of our supply chain. In 2022, more than 7300 malicious components were identified within GitHub components, according to the GitHub Advisory Database²⁸. For us, this means we must continue to uplift our vulnerability management processes to identify potentially malicious code within our applications. In May 2021, The White House released an Executive Order on Improving the Nation’s Cybersecurity. Within this was a detailed set of requirements to enhance software supply chain security, further supporting the need for critical infrastructure organisations such as ourselves to do the same.

Developments in, and increasing adoption of, emerging technologies such as robotics, artificial intelligence, quantum computing and predictive intelligence

The rapid development and increasing adoption of emerging technologies, such as robotics, artificial intelligence, quantum computing, and predictive intelligence, poses significant challenges and risks to cyber security. These technologies can create new attack vectors, and their complexity makes them difficult to secure effectively. Furthermore, cybercriminals are already leveraging these technologies to develop sophisticated attack techniques that can bypass traditional security measures, increasing the likelihood of successful cyber-attacks. As these technologies become more widespread, the risk to cyber security will only

²⁶ Double extortion ransomware tactics are where an attacker will try to force an organisation into paying by utilising an additional form of leverage, such as releasing stolen data, as opposed to only encrypting your data and holding that for ransom.

²⁷ [#StopRansomware: Royal Ransomware | US Cybersecurity & Infrastructure Agency \(cisa.gov\)](#)

²⁸ [Unit 42 - Cloud Threat Report, Volume 7: Navigating the Expanded Attack Surface | paloalto networks \(paloaltonetworks.com\)](#)

continue to grow, and we must be vigilant in adapting our security strategies to keep up with the evolving threat landscape.

Large language models have recently received much attention, with many organisations working on integrating these into business processes. There are multiple cyber security concerns with these services, including information leakage. Recently, Samsung Electronics found three instances of this occurring²⁹. As technology continues to evolve in novel ways, our cyber security capability needs to be prepared and capable to enable the organisation to respond in new ways.

Increasing bring your own device adoption

The adoption of bring your own device (**BYOD**) has experienced rapid growth at SA Power Networks, initially prompted by COVID-19 and subsequently supported by the organisation's hybrid working approach. The use of BYOD is expanding from just desk staff to maintenance depots and other support elements that enable us to continue to provide safe and reliable electricity.

The increasing adoption of BYOD introduces inherent risks to the organisation's security landscape. While our Mobile Device Manager provides control over mobile devices, personal computers used for work purposes remain outside of our direct control. This lack of control becomes even more concerning with the growing prevalence of Software-as-a-Service (**SaaS**) applications, where enforcing administrator responsibility becomes increasingly challenging.



Increasingly sophisticated adversaries

Cyber security risks are a growing concern for us, with threats in the cyber domain constantly evolving and becoming more sophisticated. According to the 2023 ACSC Threat Report³⁰, there was a 23 percent increase in cybercrime reports to previous years, with a total of more than 94,000 reports. This meant that, on average, the ACSC received one report of cybercrime every 6 minutes.



The report also highlights that the severity of cyber security incidents is on the rise, and that cybercrime has a significant impact on organisations of all sizes. Additionally, it notes that cybercrime and cyber security incidents are often underreported, indicating that the actual number of incidents may be even higher.

The geopolitical landscape has also shifted greatly over the current RCP, and the world has seen cyber become weaponised and used to attack critical infrastructure to deter and demoralise the opposition.

This was evident during the Russia/Ukraine conflict, where one country used malware specifically designed to attack and destroy critical infrastructure systems. This highlights that, as geopolitical tensions increase, so does the risk of Australian critical infrastructure being targeted.

The Australian Security Intelligence Organisation (**ASIO**) outlined in its 2021–22 Annual Report³¹ that cyber-enabled disruptive and damaging attacks on infrastructure are well within the reach of some foreign powers.

²⁹ [\[Exclusive\] concerns become reality... Samsung Electronics continues to 'abuse' ChatGPT as soon as it unlocks it | The Economist \(economist.co.kr\)](#)

³⁰ [ASD cyber threat report 2023 | Australian Signals Directorate \(cyber.gov.au\)](#)

³¹ [Threats to our way of life | Australian Government Transparency Portal \(transparency.gov.au\)](#)

These attacks have been used abroad by foreign powers as coercive or punitive means to achieve economic or geopolitical objectives against other countries. To date ASIO have not observed an attack of this nature in Australia, but assess it is possible. Vulnerabilities within Australia’s highly interconnected infrastructure networks provide opportunities for foreign powers to pre-position and deploy their disruptive and damaging cyber capabilities. This further demonstrates that we could be a target for disruptive and damaging attacks. Attacks against infrastructure in other nations, while attributed to criminal groups, demonstrate the potential harm that may result from such activities.

As these attacks become more widespread and more visible, we are beginning to see and understand just how capable these adversaries are. We are also seeing previously capable threat groups disband and reform into groups with greater capabilities and a change of tactics, techniques and procedures. On the dark web, we are also seeing a rise in the use, distribution and service-like structure of ransomware, with Ransomware-as-a-Service (**RaaS**). This enables groups that previously had no ransomware ability to easily deploy ransomware attacks.

Growing risks in the increasingly interconnected operational environment

As the boundaries between OT, IT, and the Industrial Internet of Things become increasingly blurred, traditional security controls such as air gaps are proving to be less effective in safeguarding the operational environment. This convergence of technology brings about new complexities and challenges, requiring a more holistic and integrated approach to security.

As there is increased risk through interconnectivity, there is also an increase in malicious, harm-causing software being developed specifically for OT networks. A May 2023 report from Mandiant³² describes malicious software that is specifically designed to cause electric power disruption by interacting with devices, such as remote terminal units. Remote Terminal Units are frequently leveraged in electric transmission and distribution operations within SA Power Networks and utilities around the world. The intention of this software allows the attacker to send remote commands to affect the actuation of powerline switches and circuit breakers to cause power disruption.

Recurring significant cyber security incidents

Despite the significant efforts to uplift our cyber security maturity during the current period, we have experienced seven priority 2 cyber security incidents since the start of 2022. This suggests that at current cyber security maturity levels, it is only a matter of time until a major (priority 1) incident occurs. We have also observed a continued increase in lower severity incidents across the RCP, indicating that our systems are continually targeted by advanced threat actors, and controls can fail. An increase in lower severity incidents, including level 1 controls, indicates that the likelihood of higher impact and severity incidents is increasing.

A complex digital identity

As the security obligations for each employee increase, so does the complexity they face in managing them. Tasks such as updating personal account information, access details, photos, email addresses, and multi-factor authentication settings can be confusing and time consuming. With the current setup, there are multiple touchpoints for individuals, leading to inefficiencies within the IT department and a rise in service desk call.

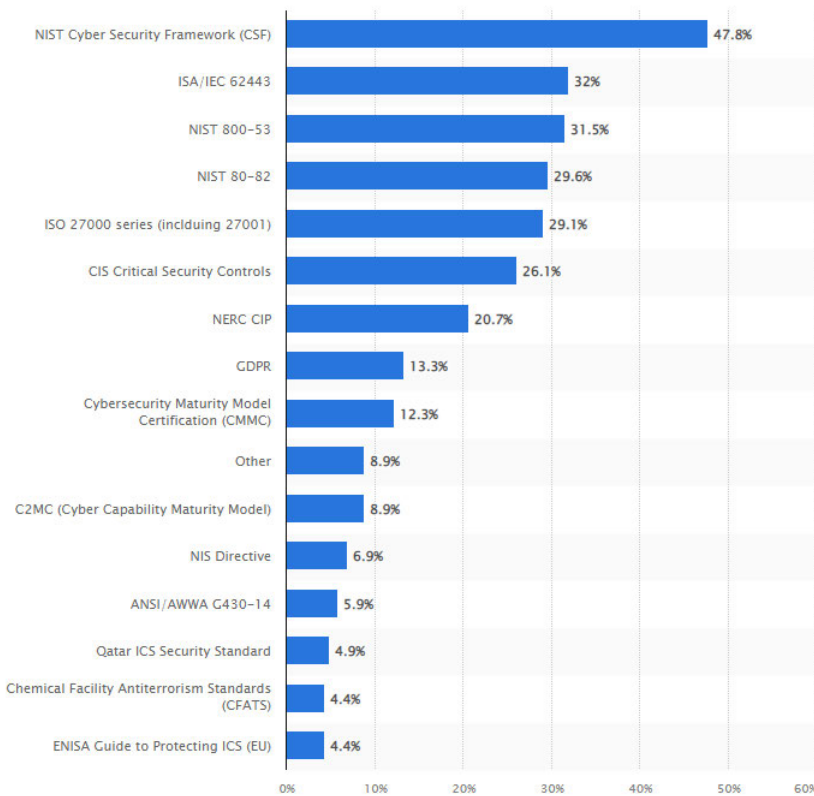
³² [COSMICENERGY: New OT Malware Possibly Related To Russian Emergency Response Exercises | Mandiant \(mandiant.com\)](#)

3.4 Industry practice

Expenditure on cyber security is rising. A global cross-industry survey conducted by Hiscox Group³³ demonstrates a growing willingness globally to invest in cyber security in response to the escalating threat landscape. This increased spending reflects the importance of mitigating cyber risks and protecting critical assets as organisations strive to safeguard their operations and data from potential cyber threats.

In addition to this spend increase, frameworks that organisations use and trust has shifted. A survey conducted by Statista, in cooperation with Nozomi Networks and SANS Institute³⁴, identifies that out of 480 worldwide cross-industry respondents, 47.8% utilise the NIST cyber security framework and 29.1% utilise ISO 27000 series, including ISO 27001. The level of use of different frameworks is shown in Figure 4.

Figure 4: Use of various cyber security frameworks – Statista survey



The Australian Signals Directorate (**ASD**) has developed a security baseline known as Essential 8³⁵. The ASD Essential 8 was first published in June 2017 and is updated regularly. This baseline reflects the ACSC’s experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations.

As discussed in section 3, the standard framework followed for cyber security within the energy industry in Australia is the AESCSF, which has incorporated components of various other good practice frameworks. Within the NEM, all of our peers are proposing significant programs to uplift cyber security maturity and capability. To date, uplifts in cyber security programs have been endorsed by the AER for all businesses, highlighting the regulatory appetite for critical infrastructure providers to take appropriate measures to mitigate risk.

³³ [Hiscox Cyber Readiness Report 2022 | Hiscoxgroup \(hiscoxgroup.com\)](https://www.hiscoxgroup.com/insights/cyber-readiness-report-2022)

³⁴ [Cybersecurity standards usage control systems 2021 | Statista \(statista.com\)](https://www.statista.com/statistics/1102142/cybersecurity-standards-usage-control-systems-2021/)

³⁵ [Essential Eight | Australian Signals Directorate \(cyber.gov.au\)](https://www.cyber.gov.au/essential-eight)

While a large amount of the detail around the proposed activity is confidential, approaches appear to be broadly based around uplifting maturity by introducing controls included within the AESCSF. The recent AER Ausgrid draft determination³⁶ determined a \$70 million benchmark efficient average investment program (+/- 20%, over the next five-year regulatory period) for uplifting AESCSF maturity levels. This benchmark average was calculated based on three peer Australian NEM DNSPs. While the businesses were not specified, it is assumed that this includes a mix of High and Moderate criticality entities under the AESCSF self-assessment. It is also unclear exactly how this benchmark has been calculated, however it appears to reflect an improvement in maturity level to somewhere between SP-2 and SP-3 of the AESCSF.

Further benchmarking information is provided in section 9.

³⁶ [Ausgrid Draft Decision Attachment 5 - Capital expenditure – Ausgrid – 2024-29 Distribution revenue proposal – September 2023](#), page 21 | AER

4. The identified need

By the end of the 2025-30 RCP we will have completed an uplift program that addresses the key identified risks associated with the current cyber security threat level. [REDACTED]

[REDACTED] However as highlighted, this level of maturity will not suffice to address the significant increase in threat level that is anticipated over the coming years. There is therefore a need to continue to contain and mitigate these threats by addressing gaps in our existing cyber security capabilities. [REDACTED]

In considering potential responses to these drivers, 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 (NEL) and jurisdictional regulations. As a result of these considerations, the identified need for our cyber security uplift program is as follows:

- a. to prudently and efficiently meet and manage demand for standard control services³⁷ and comply with applicable regulatory obligations and requirements applying to the management and operation of our distribution network that may be impacted by cyber security threats by responding to customers' concerns³⁸, 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
 - maintain safety service performance – driven by a desire to not see deterioration in the safety risk posed by the network, and
 - sufficiently invest in cyber security to address risks as they continue to emerge in dynamic cyber and energy environments to the extent that exceeds the regulatory requirements, and avoids the potentially catastrophic consequences to the community of underinvestment in this area – based on the customer understanding that:
 - technology and data are playing much larger roles in our everyday management of energy than ever before, creating a more connected grid and also one where the risks become more personal and shared, and
 - the cyber risk will evolve significantly between now and 2030, and likely at rates much faster than legislation can adjust;
- b. to comply with applicable regulatory obligations/requirements³⁹, in this case with specific reference to:
 - the Privacy Legislation Amendment Act 2022
 - [REDACTED]

³⁷ This is pursuant to Clause 6.5.7(a)(1) of the NER

³⁸ 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.

³⁹ This is pursuant to Clause 6.5.7(a)(2) of the NER, which requires expenditure in order to comply with all applicable regulatory obligations or requirements associated with the provision of standard control services.

⁴⁰ [REDACTED]

⁴¹ [AESCFS Framework Overview](#), page 9 | Australian Energy Market Operator (aemo.com.au)

○ [REDACTED]

- c. to maintain the reliability, safety and security of our distribution network services and system, in relation to the risk of harm to workers, consumers and community.

5. Comparison of options

5.1 The options considered

Table 4: Summary of options considered

Option	Description
The base case	No investment ⁴²
Alternative options	
Option 1 – Basic controls	Option 1 involves implementing the cyber security controls from the ASD Essential 8 framework that are not yet implemented, specifically Application control and User access.
Option 2 – Risk-based approach to cyber security	<p>Option 2 has been developed using a threat-based and risk-based approach to uplifting cyber security capability. It proposes controls and measures based on our assessment of the specific risks faced by our business within the 2025-30 RCP. Controls have been drawn from the AESCSF Framework (version 2) as well as from other internationally endorsed industry best practice frameworks, and are grouped into the following controls:</p> <ul style="list-style-type: none"> • Operational Technology • information protection • Tools of trade devices • BYOD cyber strategy • Network detection and response • Cyber awareness program • MyID • Zero-trust architecture • Security Operations (SECOPS) • IT resiliency lifecycle • Secure software development lifecycle • Third-party management <p>By utilising a risk-based perspective, we can ensure that our cyber security measures align with our organisational risk tolerance, and therefore effectively mitigate potential threats.</p>
Option 3 – Risk-based approach + Comply with SP-3	<p>Option 3 proposes fifteen additional practices required for completion of all controls within AESCSF SP-3, in addition to the risk-based controls included in option 2. These practices include:</p> <ul style="list-style-type: none"> • Strengthening asset management • Strengthening risk management • Architectural patterns for asset and change

⁴² While the base case for this business case is no investment, ongoing costs associated with maintaining our current level of cyber security maturity are included SA Power Networks ICT Recurrent Cyber Security Refresh Business Case (document 5.12.6), as well as in base year roll-forward opex.

5.2 Options investigated but deemed non-credible

As discussed above, the rapidly evolving threat landscape and increasing complexity of cyber-attacks mean it is crucial that we take proactive steps to mitigate cyber risks and ensure the safety and security of our operations. While our cyber security maturity is progressing well, a high level of risk remains. Zero additional uplift investment in cyber security is therefore deemed non-credible, as it would result in us being unable to mitigate any evolving and future cyber risks

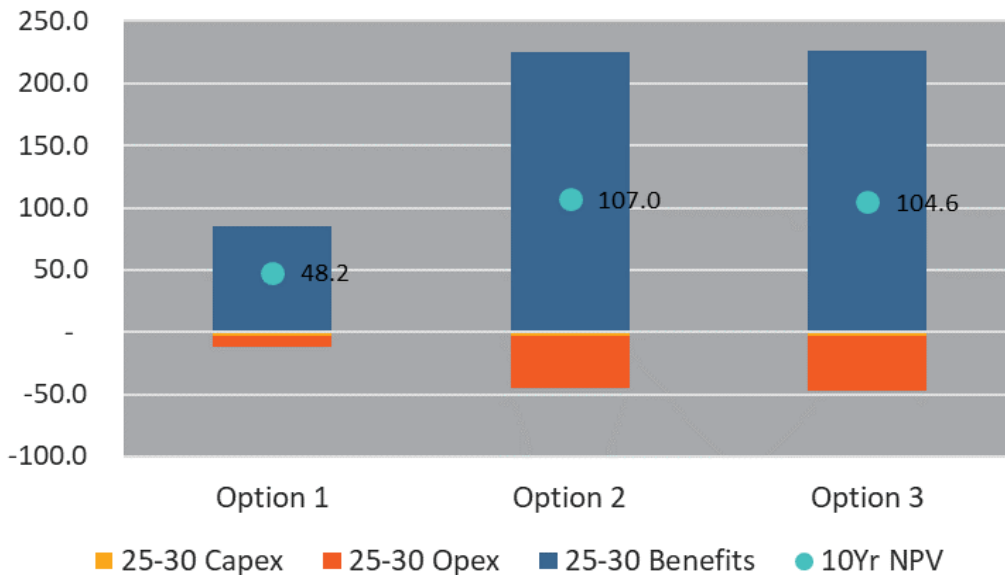
5.3 Analysis summary and recommended option

5.3.1 Options assessment results

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

Option	10-year program/project costs			2025–30 Program/project costs			10-year benefits ⁴³	10-year NPV ⁴⁴	Overall risk rating ⁴⁵	Ranking
	Capex	Opex	Total	Capex	Opex	Total				
Option 0 – Do nothing	-	-	-	-	-	-	-	-	Extreme	4
Option 1 – Basic controls	0.8	16.9	17.8	0.8	9.6	10.4	85.6	48.2	Extreme	3
Option 2 – Risk-based approach	2.6	68.9	71.4	2.6	42.1	44.7	225.7	107.0	Medium	1
Option 3 – Risk-based approach + Comply with SP-3	2.6	71.7	74.3	2.6	45.0	47.5	225.9	104.6	Medium	2

Figure 5: NPV outcome by option (\$m, real Jun 2022)



⁴³ 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.

⁴⁴ 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%.

⁴⁵ The overall risk level for each option after the proposed option implemented. Refer to [Appendix B](#) – risk assessment for details.

The options sections that follow describe the controls addressed by each of the three considered options, and outline the costs and benefits associated with each. A high-level summary of the controls addressed in each option is provided in Table 6. Each of the controls is described in more detail in the sections below.

Table 6: Summary of the key controls addressed under each option

Key controls	Total cost (\$m real Jun-22)	Option 1	Option 2	Option 3
	Role-based user access	8.4	X	X
Application control	2.0	X	X	X
Total Option 1	10.4			
Zero trust architecture	6.0		X	X
Security Operations (SECOPS)	10.1		X	X
IT resiliency lifecycle	1.6		X	X
Secure software development lifecycle	1.7		X	X
Third-party security	0.6		X	X
Operational technology	4.9		X	X
Information protection	2.8		X	X
Tool of trade devices	1.4		X	X
BYOD cyber strategy	2.1		X	X
Network detection and response	1.0		X	X
Cyber awareness	1.5		X	X
MyID	0.6		X	X
Total Option 2	44.7			
Other AESCSF principles	2.9			X
Total Option 3	47.5			

Assumptions

Estimates are based on version 2 of the AESCSF, as it is assumed that this version will be released and mandated for compliance before the start of the 2025–30 RCP.

5.3.2 Recommended option

The increasing use of the cyber domain as a tool of warfare, coupled with the ever-evolving threat landscape for infrastructure in the cyber domain and an increasing reliance on digital systems and networks, drive the need to uplift and maintain strong cyber security measures [REDACTED].

Without significant additional investment, we will be unable to address the drivers discussed in section 3.3 and protect against the increasing complexity, prevalence and targeted nature of cyber security threats. The recommended solution is to implement a comprehensive cyber security uplift program, to improve our cyber security posture and reduce both likelihood and consequence of cyber threats. The program will adopt a risk-based approach to cyber security maturity that focuses on increasing the scope of cyber security preventative controls, automation, and resilience to reduce risks. It will prioritise threat intelligence within a risk-based approach, adjusting the program to reduce risks, and identifying alignment between cyber security needs and other projects.

Implementing the cybersecurity uplift program will provide the following benefits:

- improved cybersecurity posture and reduced risk of cyber threats
- enhanced protection of sensitive information and prevention of its unauthorised disclosure
- improved incident response and significant costs avoidance
- reduced overall risk to the operational technology environment
- simplified management of identity and access control

By adopting a risk-based approach and implementing good industry practices, we can remain agile in responding to, mitigating and reducing the impact of evolving cyber security threats.

Option 1 provides only minor risk reduction. It fails to address most of the major risks identified, leaving the network vulnerable to complex and evolving threats. [REDACTED]

Option 2 addresses all core identified threats and reduces risk outcomes associated with these to an acceptable level. This option considers various cyber frameworks, including AESCSF, and also considers controls that sit outside of these frameworks. Adopting Option 2, we can establish a robust cyber security posture, ensuring comprehensive protection for infrastructure and sensitive data. This approach aligns with our commitment to proactive risk management and resilience in the face of evolving cyber threats.

Option 3 incorporates all the risk-mitigation activities included in Option 2 as well as including the AESCSF SP-3 v2 controls that are not included within Option 2. While we believe that Option 3 is a prudent approach for the 2025-30 RCP, and this level of investment has been supported by our customer 'People's Panel', SP-3 is not a regulatory requirement at this current time.

As a result, Option 2 has been selected as the preferred option.

5.4 Option 0 – Do Nothing

5.4.1 Description

Option 0 involves making no investment above recurrent expenditure. It therefore does not address any of the drivers discussed in section 3.3, including:

- the increasing risk profile resulting from more complex and targeted threats (including ransomware) emerging from increasingly sophisticated adversaries, as technology advances and the business landscape evolves;
- [REDACTED];
- rapidly escalating risks in the operational environment driven by the emergence and convergence of new technologies;
- the growing supply-chain risk, with malicious actors increasingly targeting this area;
- the risks of new and emerging technologies, such as robotics, artificial intelligence, quantum computing and predictive intelligence, and of cyber criminals using these technologies to improve their chances of bypassing traditional security measures; and
- the risks from the lack of control associated with increasing adoption of BYOD.

⁴⁶ Reputational damage drives costs in managing communications with the public and or government following a breach event.

5.4.2 Costs

There is no upfront capex or opex associated with Option 0⁴⁷. However, our capability to address evolving threats would rapidly deteriorate over time and business costs associated with operational outages and breach of obligations, [REDACTED], would quickly grow to uneconomic levels.

5.4.3 Risks

Table 7: Risk assessment summary

Risk consequence category	Current risk level ⁴⁸
Safety – Harm to a worker, contractor or member of the public	High
Network – Failure to transport electricity from source to load	Extreme
Customers – Failure to deliver on customer expectations	High
Technology – Disruption of access to, or use of, systems	Extreme
Technology – Unauthorised access, modification or control of systems	Extreme
Technology – Unauthorised access or disclosure of information	Extreme
Overall risk level	Extreme

Section 3.2 describes our maturity level at the end of the 2025-30 RCP relative to a comparable baseline (i.e. the AESCSF). Figure 1 evidences an increasing number of breaches despite the current uplift program. With no further uplift in controls, we would expect this to increase at an accelerated rate. With no uplift in controls, we would also expect the incidence of higher priority incidents will return as attacks become better and new threats emerge.

We expect that by the end of the 2025-30 RCP, not further uplifting controls would result in a ‘Possible’ likelihood of a Priority 1 major cyber security incident that results in disruption of the electricity network (predicted once every five years). In addition, this option results in the ‘Likely’ outcome of a Priority 1 major IT system loss or Major data loss (one every year). These events all have significant (Moderate, Major or Catastrophic) consequences associated with them if controls are not further [REDACTED]

This option therefore results in a residual risk level of Extreme well before the end of the 2025–30 RCP.

The full risk assessment is provided in Appendix B.

5.4.4 Quantified benefits

There are no quantified benefits associated with this option.

5.4.5 Unquantified benefits

There are no unquantified benefits associated with this option.

⁴⁷ While the base case for this business case is no investment, ongoing costs associated with maintaining our current level of cyber security maturity are included SA Power Networks ICT Recurrent Cyber Security Refresh Business Case (document 5.12.6), as well as in base year roll-forward opex

⁴⁸ The level of risk post current controls (ie after considering what we currently do to mitigate the risk).

5.5 Option 1: Basic controls

5.5.1 Description

Option 1 involves implementing basic cyber security controls that are not yet in place at SA Power Networks. The ASD has developed a security baseline known as Essential 8⁴⁹. The ASD Essential 8 was first published in June 2017 and is updated regularly. This baseline reflects the ACSC’s experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations.

Two of the controls included in the Essential 8 baseline - ‘Role-based access’ and ‘Application control’ are yet to be implemented within our environment. Each of these controls is described below. Appendix C provides a table that shows how each of these controls supports the drivers for change described in 3.3.

Role-based access

Our current environment

[REDACTED]

The solution

Role-based access control (**RBAC**) is a security model that restricts permissions based on a user’s assigned role within an organisation. RBAC simplifies access permissions management by granting users permissions based on their job function or responsibilities, rather than their individual identity. Permissions can then be assigned or revoked as needed. This approach minimises the risk of unauthorised access and security breaches.

[REDACTED] With RBAC, we can control what end-users can do at both broad and granular levels. We can designate whether the user is an administrator, a specialist user or an end-user, and align roles and access permissions with employees’ positions within the organisation. Permissions are allocated with only enough access as needed for employees to do their jobs.

RBAC will be implemented at SA Power Networks via creation of an organisation-wide RBAC matrix (ie, of permission by role). The RBAC matrix will be driven through creation of HR-based job families and subsequent subordinate positions, which will define a set of access controls based on least privileged access.

With the implementation of the automated role-based access controls, all legacy access will be removed when a position change occurs, and a new set of access controls applied. This ensures the user will always have the current and correct access associated with their position. Changes will be initiated by either the onboarding of a new user or a change to the user’s position throughout the entire lifecycle of the account.

Application control

Our current environment

Application control refers to the process of controlling executables (applications/software/scripts) on a system to only those who are trusted and authorised. This is typically achieved using allowlisting or blocklisting techniques, which allow administrators to specify which executables are allowed to run on a system and which are not.

⁴⁹ [Essential Eight | Australian Signals Directorate \(cyber.gov.au\)](#)

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

Our intent is to introduce specialist software, process, and personnel in order to implement all controls within this maturity framework to Maturity Level 4.

5.5.2 Costs

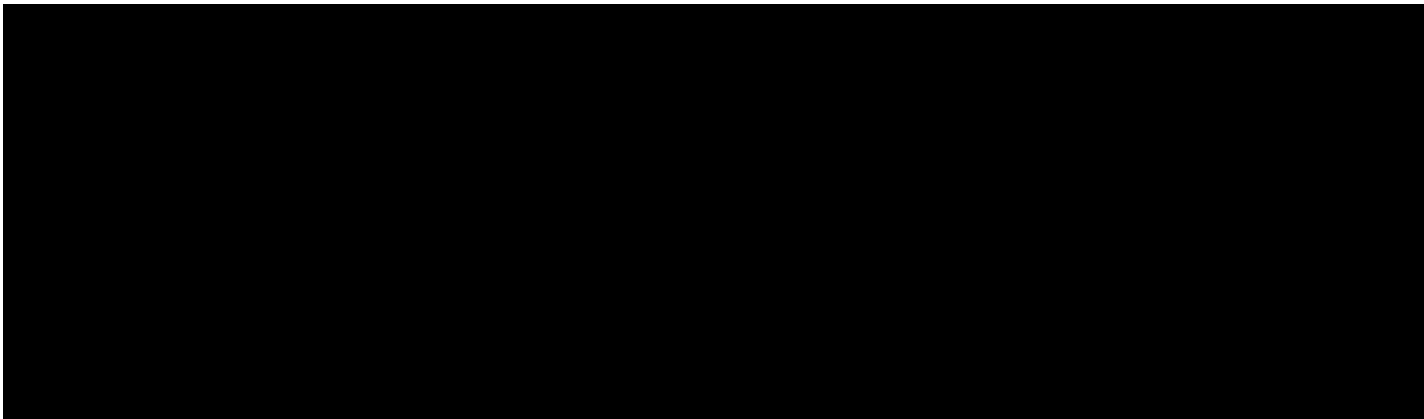
Option 1 was forecast on a bottom-up basis. Total expenditure for this option in the 2025–30 RCP is \$10.4 million, including \$0.8 million capex and \$9.6 million opex. This includes a recurrent opex step change of \$5.5 million. The expenditure breakdown is provided below in Table 8, with a more detailed breakdown provided in the attached costing spreadsheets (Appendix E).

Table 8: 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	2030–31	2031–32	2032–33	2033–34	2034–35	Total 2030–35
Recurrent												
Capex	-	-	-	-	-	-	-	-	-	-	-	-
Opex	0.6	1.2	1.2	1.2	1.5	5.5	1.5	1.5	1.5	1.5	1.5	7.3
Recurrent total	0.6	1.2	1.2	1.2	1.5	5.5	1.5	1.5	1.5	1.5	1.5	7.3
Non-recurrent												
Capex	-	0.3	0.2	0.4	-	0.8	-	-	-	-	-	-
Opex	0.5	2.1	1.0	0.5	-	4.1	-	-	-	-	-	-
Non-recurrent Total	0.5	2.3	1.2	0.9	-	4.9	-	-	-	-	-	-
Total capex	-	0.3	0.2	0.4	-	0.8	-	-	-	-	-	-
Total opex	1.1	3.2	2.1	1.7	1.5	9.6	1.5	1.5	1.5	1.5	1.5	7.3
TOTAL COST	1.1	3.5	2.4	2.0	1.5	10.4	1.5	1.5	1.5	1.5	1.5	7.3

5.5.3 Risks

Table 9: Risk assessment summary



The ASD Essential 8 framework is based on a Windows-only environment. So while this may mitigate a majority of threats for some businesses, it would not be as effective for SA Power Networks due to the complex nature of our environment, which includes many different technologies and operating systems, such as Linux, containerisation, Industrial Control Systems and more. It also does not contain many of the controls that are embedded in other good practice frameworks (such as AESCSF).

⁵⁰ The level of risk post current controls (ie after considering what we currently do to mitigate the risk).

⁵¹ The future level of risk once treatments proposed in this option have been implemented.

This option would not address the majority of the drivers discussed in section 3.3. While addressing some specific key risks, we would remain vulnerable to other critical risks, such as the increasing risk profile from more complex threats, the changing threat landscape, operational security risks, and evolving technology risks.

[Redacted]

[Redacted] this option results in the Extreme residual risk level remaining at the end of the 2025–30 RCP.

The full risk assessment is provided in Appendix B.

5.5.4 Quantified benefits

The quantified benefits associated with Option 1 include the following:

Cost avoidance (\$14.3 million)

[Redacted]

Risk monetisation (\$71.4 million)

[Redacted]

Both likelihood and consequence are impacted (ie. reduced) by the option treatment, and the benefit reported is the difference between the calculated benefits under the base case and the treated option. Conservative consequences of these events are derived from various sources, as detailed in section 9.

[Redacted]

5.5.5 Unquantified benefits

Appendix D summarises how each of the controls addressed by this option mitigates each of our defined risk events and impacts overall risk reduction.

5.6 Option 2: Risk-based approach to cyber security

5.6.1 Description

All frameworks have advantages and disadvantages. While the AESCSF is specifically crafted for the energy sector, it fails to account for some of the critical security controls identified in other internationally recognised cyber security frameworks. An example of this is that while AESCSF talks about having an awareness program, it doesn't truly outline an effective program that would reduce risk.

To combat this, we adopt a threat-based and risk-based approach to effectively identify cyber security areas of concern. In instances where the AESCSF does not provide specific controls, or fails to meet our desired level of tolerance, we proactively seek guidance from other frameworks or maturity models to ensure comprehensive coverage. This approach involves leveraging threat intelligence to gather information on potential threats and their likely targets. We also use attack simulation software, conduct penetration testing and perform social engineering tests to assess the effectiveness of our existing controls and identify any areas of weakness that require immediate attention. This approach allows us to identify any gaps in our security measures and use this to plan or actively strengthen our overall cyber resilience by prioritising our efforts and allocating resources where they are needed most. It ensures that our cyber security measures effectively mitigate our key identified cyber security risks, and therefore align with our organisational risk tolerance.

The controls included within Option 2 are grouped into the following key controls:

- Zero-trust architecture
- Security Operations (**SECOPS**)
- IT resiliency lifecycle
- Secure software development lifecycle
- Third-party security
- Operational technology
- Information protection
- Tools of trade devices
- BYOD cyber strategy
- Network detection and response
- Cyber awareness
- MyID

Each of these is discussed below. Appendix C provides a table that shows how each of these controls supports the drivers for change described in 3.3.

Zero trust architecture

Our current environment

Zero trust architecture (**ZTA**) is a security model that assumes all resources, both internal and external to the organisation, are potentially compromised and must be verified before access is granted. This approach requires that every user, device, and application attempting to access a system or network be authenticated and authorised before any access is granted. It is a security framework that does not automatically trust any device, user, or application, whether they are inside or outside the organisation. ZTA requires a set of technologies and processes that enable a granular approach to access control.

The Zero Trust Maturity Model released by CISA⁵² in April 2023 provides a framework against which to assess Zero Trust maturity, with four maturity levels – Traditional, Initial, Advanced and Optimal. [REDACTED]

[REDACTED]

[REDACTED]

Implementing a Zero Trust security model offers a comprehensive solution to the challenge of insufficient separation between critical and non-critical systems within the same zone. Through micro-segmentation, the network can be divided into isolated segments, ensuring that critical systems reside in dedicated spaces, distinct from non-critical counterparts. Zero Trust's emphasis on access controls, policies, and the principle of least privilege ensures that users only have the minimum necessary access, reducing the risk of unauthorized exposure of critical data.

We are seeking to increase our ZTA maturity [REDACTED]. This will reduce the likelihood of a data breach as well as assist with addressing the risk posed by future technology. We will follow a risk-based approach to control and process improvement, [REDACTED]

⁵² [Zero Trust Maturity Model Version 2.0, April 2023 | US Cybersecurity & Infrastructure Security Agency \(cisa.gov\)](https://www.cisa.gov/zero-trust-maturity-model-version-2.0)

Security Operations (SECOPS)

Our current environment

SECOPS plays a crucial role in safeguarding the cyber security of SA Power Networks by detecting, controlling, and eliminating threats against the organisation. As threat actor groups continue to grow and advance in sophistication, it is imperative for the SECOPS team to expand and enhance their capabilities to effectively combat these groups.

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

The solution

Addressing the existing gaps in our security operations involves several key protections:

- [REDACTED]
- **Bolstering our collection and analysis of cyber threat intelligence:** Timely advice and intelligence are vital for SECOPS operations. With the growing sophistication and increase in the volume of cyber threats, there is a need to improve how we collect, store, utilise and share threat intelligence. Leveraging threat intelligence enables the organisation to anticipate adversaries with a higher degree of certainty, anticipate potential attack vectors and even predict the timing of attacks.
- [REDACTED]
- **Establishing and maintaining clear and well-defined states of operation for both the IT and OT environments:** Building and testing distinct operating models involves documenting predefined states of operations aligned to the cybersecurity state of our systems. These can also be triggered from other areas such as intelligence received. The process includes documenting the architecture and topologies of each state, supporting documentation, and is based upon a detailed understanding of our assets and their priorities. It also includes criteria for triggering the state change, authorities for approval, checklists for moving between states, how long we can operate in each state and the required monitoring during each state. These models require constant uplift, aligning to the changes in the organisations systems, the threats it faces and operating model priorities.
- [REDACTED]

IT resiliency lifecycle

Our current environment

IT resiliency is the ability of IT systems and infrastructure to withstand, adapt to, and recover from disruptions or outages. This is a continuous process that involves proactive planning, preparation, and testing to ensure the organisation can maintain business continuity in the face of unexpected events.

The NIST, Special Publication 800-53 Security and Privacy Controls for Information Systems and Organisations, USA⁵⁴ outlines a multitude of controls that should be implemented for organisations. The contingency planning section has been used to assess our current implemented IT resilience controls against. Within section CP-4, it is outlined that an organisation should have methods for testing contingency plans to determine the effectiveness of the plans and identify potential weaknesses include checklists, walk-through and tabletop exercises, simulations (parallel or full interrupt), and comprehensive exercises. [REDACTED]

[REDACTED]

⁵⁴ [NIST Special Publication 800-53 Revision 5: Security and Privacy Controls for Information Systems and Organisations | US National Institute of Standards and Technology \(nvlpubs.nist.gov\)](https://nvlpubs.nist.gov)

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

Secure software development lifecycle

Our current environment

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]



Table 12: SA Power Networks audit against SAMM V2 SSDLC Maturity Model

A large black rectangular redaction covering the entire content area of the page, including the table mentioned in the caption.

The solution

The goal of our SSDLC is to identify and mitigate security risks throughout the entire software development lifecycle, from design to deployment and maintenance. A key focus of this will be creating a sustainable program that not only incorporates secure software development practices, but also skilled personnel who are equipped to identify and mitigate security risks throughout the software development lifecycle. The process guidance from the SAMM V2 maturity model will be utilised to ensure that we are aligned to good industry practice. This includes establishing secure coding standards and guidelines, implementing security

testing tools and processes, and providing regular training and education to developers and other personnel involved in the software development process.

By improving our SSDLC maturity, we will reduce the likelihood of vulnerabilities and security breaches in our software systems. We will also maintain the security of software in use via increased governance and better transparency. In combination with verification testing and more scalable processes, we will reduce the likelihood of a cyber security incident that is caused from an insecure, immature, and inadequate SSDLC.

Third-party security and cyber supply chain risk management

Our current environment

[REDACTED]

[REDACTED] Australian organisations face many cyber threats, including from the ICT supply chain. Malicious cyber actors who target upstream suppliers, such as by compromising a cloud host, may be able to impact downstream customers by exploiting the trust between that supplier and its customers. An attacker could then conduct data theft and extortion activities, or other attacks like denial-of-service. An organisation’s cyber security posture is only as strong as its weakest link, which could be an entity in its ICT supply chain’.

[REDACTED]

The solution

To address these gaps effectively, a more robust and continuous monitoring system is imperative to ensure a comprehensive and real-time assessment of third-party security, thereby enhancing our overall cybersecurity posture. Third-party monitoring services will provide a comprehensive risk score for our vendors based on publicly available information, providing us with a deeper understanding of the risk exposure associated with each third party.

By leveraging third-party monitoring services, we can access real-time insights and notifications regarding any breaches or security incidents involving the third-party organisations. This proactive approach provides us with a more robust and reliable risk assessment mechanism, allowing us to stay informed about potential risks and take appropriate actions in a timely manner. It enhances the organisation's ability to identify and address potential security vulnerabilities introduced by third-party providers, thereby minimising the overall risk landscape. By staying proactive and well informed, we can strengthen our security posture and maintain a higher level of trust and confidence in third-party relationships.

⁵⁵ [Improving the Nation's Cybersecurity | US Presidential Document \(federalregister.gov\)](#)

⁵⁶ [Cyber Supply Chain Risk Management, May 2023 | Australian Signals Directorate \(cyber.gov.au\)](#)

⁵⁷ [ASD Cyber Threat Report 2022-2023, Nov 2023 | Australian Signals Directorate \(cyber.gov.au\)](#)

Operational technology (OT)

Our current environment

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Large redacted text block]

⁵⁸ [How to enhance the cybersecurity of operational technology environments | McKinsey \(mckinsey.com\)](#)

⁵⁹ [The threat to Operational Technology | Canadian Centre for Cyber Security \(cyber.gc.ca\)](#)

[Redacted]

[Redacted]

The solution

[Redacted]

[Redacted]

[Redacted]

[Redacted]

Information protection

Our current environment

[Redacted]

60

[Redacted]

[Redacted]

[Redacted]

The solution

While the AESCSF highlights the importance of information protection, the focus is primarily on identifying information assets. The framework does not provide guidance on how to protect these assets. To address this gap, our proposed activity encompasses automated identification of both information assets and business assets that contain or utilise information. This process will enable us to gain a comprehensive view of our assets and their associated security requirements.

Once the assets are identified, we will implement specific security controls tailored to their unique characteristics and risk profiles. These controls will ensure effective protection of our information assets, mitigating the risk of unauthorised access, data breaches, and other security incidents.

Additionally, as part of our information protection efforts, we will implement a DLP solution. The DLP solution will provide granular control over movement and handling of sensitive information, allowing us to prevent data leaks and unauthorised disclosure.

By combining automated asset identification, targeted security controls and a DLP solution, we will establish a robust framework for protecting our information assets and maintaining the confidentiality, integrity and availability of sensitive data such as customer data. This proactive approach to information protection will enhance our overall security posture and strengthen our ability to safeguard valuable data assets.

Tools of trade

Our current environment

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

The solution

This initiative aims to comprehensively assess the tool of trade devices and highlight any control deficiencies that exist. By conducting a thorough evaluation, we can identify areas where additional controls are needed to close the security gaps effectively.

The uplift program will not only focus on identifying control deficiencies but also on implementing appropriate security measures to address the identified risks. Furthermore, the controls will establish a baseline for future deployment and ongoing monitoring of the tool of trade devices. It will enable us to track and evaluate the effectiveness of implemented controls, identify any emerging security risks, and promptly address them to maintain a robust and secure operational environment.

BYOD cyber strategy

Our current environment

[Redacted]

[Redacted]

The solution

[Redacted]

Additionally, the program will involve an ongoing process of identifying areas of weakness introduced by BYOD use, such as data access vulnerabilities or the possible introduction of malware. By actively identifying these weaknesses, we can proactively work towards implementing appropriate controls to close these gaps effectively. This approach ensures that BYOD adoption aligns with the organisation's security requirements and mitigates the potential risks associated with uncontrolled access to sensitive data.

By implementing these measures and actively addressing the risks introduced by BYOD, we aim to strike a balance between enabling flexible working practices and maintaining a robust security posture. This proactive approach to BYOD security will help safeguard the organisation's data, systems, and infrastructure, ensuring the integrity and confidentiality of sensitive information while allowing employees to leverage the benefits of BYOD in their work environment.

Network detection and response

Our current environment

[Redacted]

[Redacted]

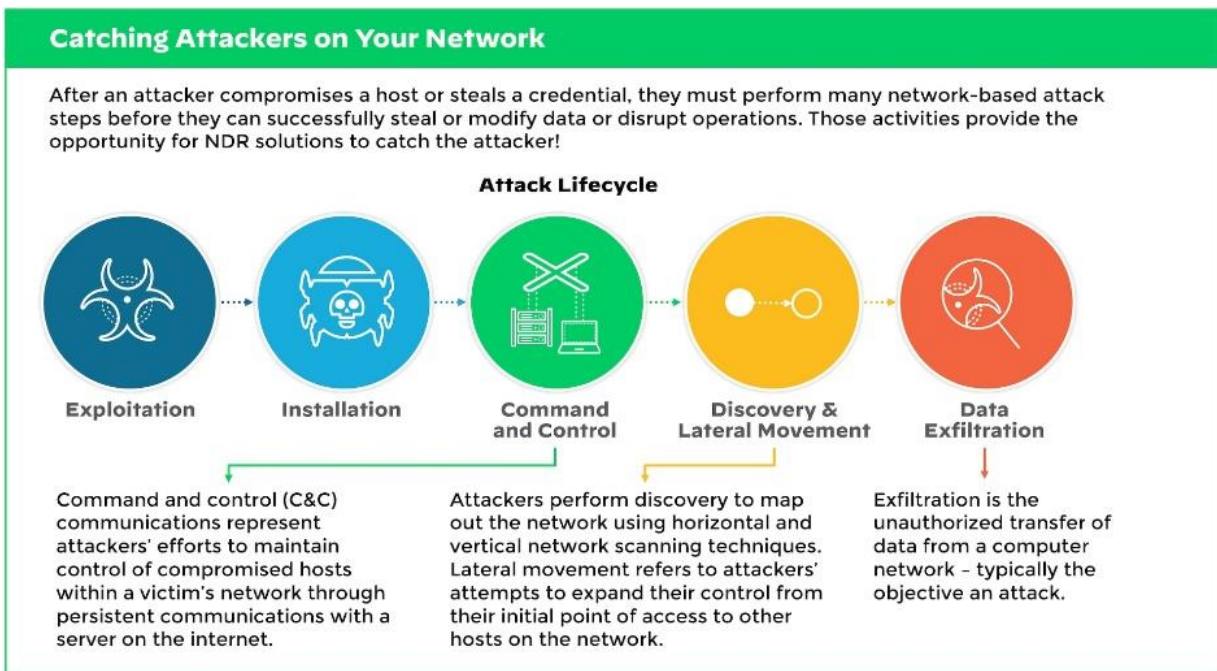


The solution



As part of uplifting our cyber security controls, we will investigate and implement an NDR solution⁶². This solution will enhance our network visibility and monitoring capabilities, allowing us to proactively detect and respond to potential threats and anomalous activities within our network infrastructure. By investing in an NDR solution, we aim to strengthen our overall cyber security posture and better protect our critical assets and sensitive information from sophisticated cyber threats. Figure 6 shows how this solution operates.

Figure 6: Network detection and response approach



Cyber awareness

Our current environment



⁶² Note that while the Architecture section within the AESCSF emphasises the significance of a network intrusion detection system (NIDS) and a network intrusion protection system (NIDPS), it overlooks the importance of a NDR system.

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

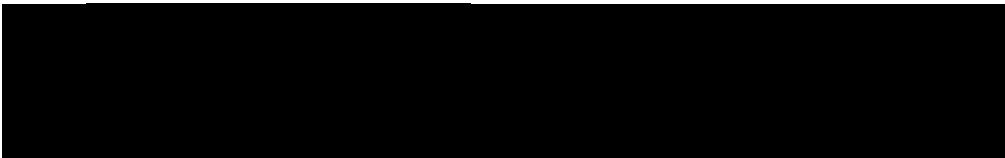
[Redacted]

The solution

To address this deficiency, the following activities will be incorporated into our approach:

- actively collaborating with other departments, partners, and collaborators from various areas to leverage their expertise and resources in enhancing cyber awareness;
- delivering ongoing reinforcement training, including lunch and learn sessions, regular internal news articles, and education on the latest threats and scams;
- identifying areas of the business that pose an increased or unique human risk and implementing targeted awareness initiatives to address these areas;
- establishing a formal incentive program to recognise individuals, groups or departments that excel in cyber security or demonstrate key behaviours aligned with industry best practices;
- empowering staff across the business to become cyber security awareness ambassadors, fostering a culture of proactive security awareness and incident reporting; and
- identifying key metrics to measure the performance of the awareness program and reporting on these to senior leadership.

By embracing the SANS security awareness roadmap and implementing these initiatives, we aim to strengthen the cyber resilience of the organisation, enhance employee awareness and vigilance, and cultivate a proactive security culture that effectively mitigates cyber risks and safeguards critical assets.



MyID

Our current environment

[Redacted content]

[Redacted content]

The solution

[Redacted content]

This information will then flow into our identity automation suite to be delivered to connected end points.

5.6.2 Costs

Option 2 was forecast on a bottom-up basis. Total expenditure for this option in the 2025–30 RCP is \$44.7 million, including \$2.6 million capex and \$42.1 million opex. This includes a recurrent opex step change of \$15.9 million. The expenditure breakdown is provided below in Table 13.

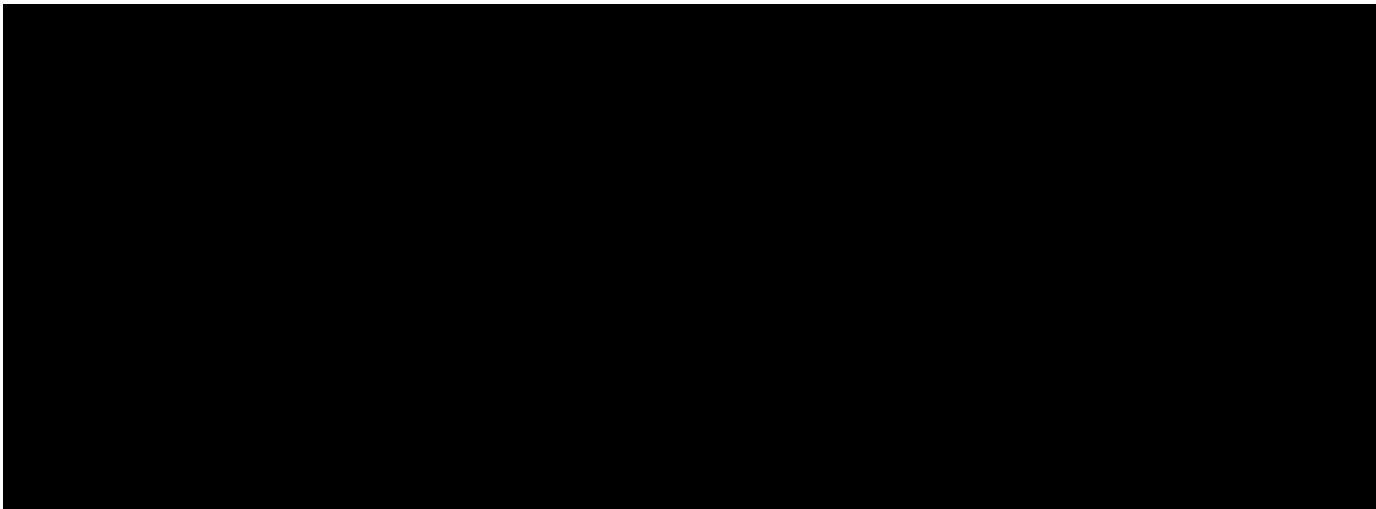
Table 13: Option 2 Costs by Cost Type (\$m June 2022 Real)

Cost Type	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30	2030–31	2031–32	2032–33	2033–34	2034–35	Total 2030–35
Recurrent												
Capex	-	-	-	-	-	-	-	-	-	-	-	-
Opex	1.5	2.7	2.9	3.5	5.4	15.9	5.4	5.4	5.4	5.4	5.4	26.8
Recurrent total	1.5	2.7	2.9	3.5	5.4	15.9	5.4	5.4	5.4	5.4	5.4	26.8
Non-recurrent												
Capex	0.1	0.5	0.8	0.8	0.4	2.6	-	-	-	-	-	-
Opex	2.6	6.9	7.2	5.8	3.8	26.2	-	-	-	-	-	-
Non-recurrent Total	2.6	7.4	8.0	6.6	4.2	28.8	-	-	-	-	-	-
Total capex	0.1	0.5	0.8	0.8	0.4	2.6	-	-	-	-	-	-
Total opex	4.1	9.6	10.0	9.2	9.2	42.1	5.4	5.4	5.4	5.4	5.4	26.8
TOTAL COST	4.1	10.1	10.9	10.0	9.5	44.7	5.4	5.4	5.4	5.4	5.4	26.8

The \$26.2 million non-recurrent opex component of the forecast relates to developing the uplift in our cyber security capability. This includes development and implementation of systems capabilities as well as process uplifts associated with the new systems. We consider that these activities do not materially add to the value of existing assets, and as such, this expenditure should be classified as Operating. This proposed treatment is supported by an independent assessment from BDO Australia⁶⁶.

There is also a forecast \$15.9 million (\$5.4 million per annum moving forward) recurrent opex component. The majority of this relates to licensing fees for software required to support the capability uplift. The remainder is the cost of additional resources to maintain the uplifted cyber security systems and processes.

5.6.3 Risks



Option 2 will substantially reduce cyber security risk, reducing all key risk consequence categories to at least a Medium risk. In particular, this addresses the extreme residual risks associated with a major cyber security incident that causes:

- [Redacted]
- [Redacted]
- [Redacted]

The full risk assessment is provided in Appendix B.

5.6.4 Quantified benefits

The quantified benefits associated with Option 2 include the following:

Cost avoidance (\$24.4 million)

[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]
[Redacted]

⁶⁶ External Review of ICT Cyber Expenditure Treatment, document 5.12.24

⁶⁷ The level of risk post current controls (ie after considering what we currently do to mitigate the risk).

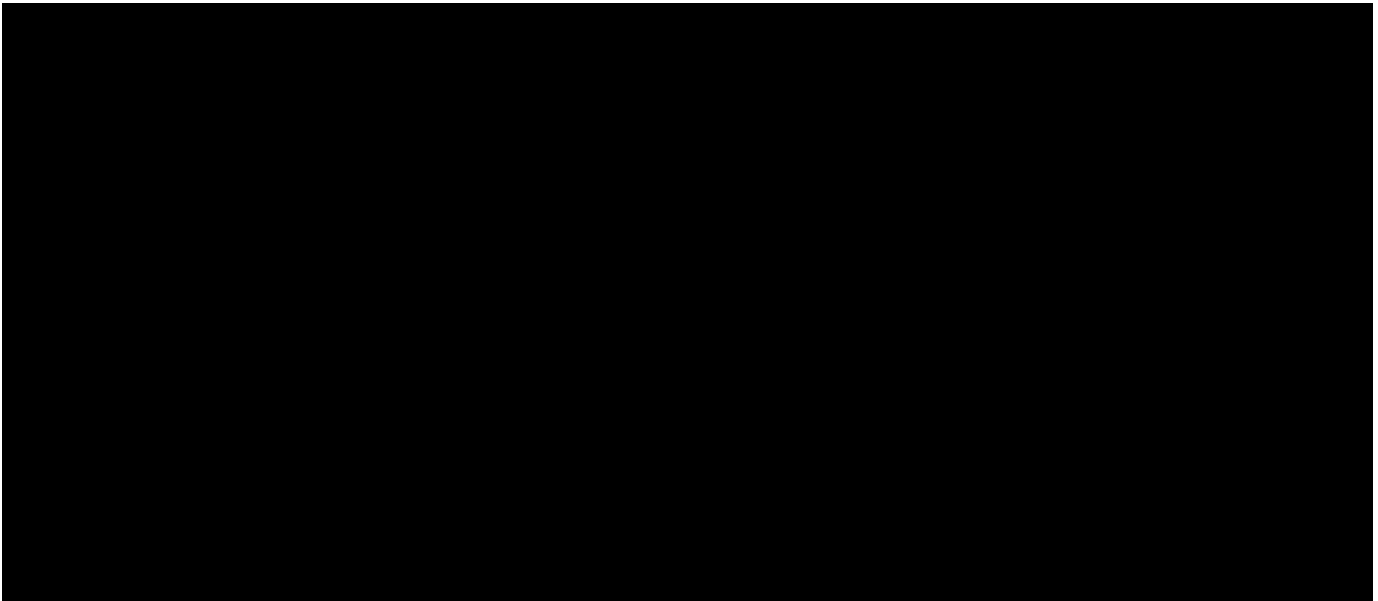
⁶⁸ The future level of risk once treatments proposed in this option have been implemented.

Risk monetization (\$201.2 million)

A table with five rows of content that has been completely redacted with black boxes.

Both likelihood and consequence are impacted (ie reduced) by the option treatment, and the benefit reported is the difference between the calculated benefits under the base case and the treated option. Conservative consequences of these events are derived from various sources, and these are assumptions are detailed in section 9.

Table 15: Quantified benefits for Option 2

A large table area that has been completely redacted with a solid black box.

5.6.5 Unquantified benefits

Appendix D summarises how each of the controls addressed by this option mitigates each of our defined risk events and impacts overall risk reduction.

5.7 Option 3: Risk-based approach + Comply with AESCSF SP-3

5.7.1 Description

There are a number of AESCSF version 2 principles that do not fall within any of the core Option 2 activities that we have identified as required to deliver the highest level of risk mitigation for our business in the 2025-30 RCP. However, these are still good business practices that would enable further mitigation of risk. Option 3 builds on our risk-based approach (Option 2) and proposes the delivery of the remaining AESCSF controls to enable us to complete SP-3 within the 2025–30 RCP. The specific principles that fall within this category are described below.

Other AESCSF principles

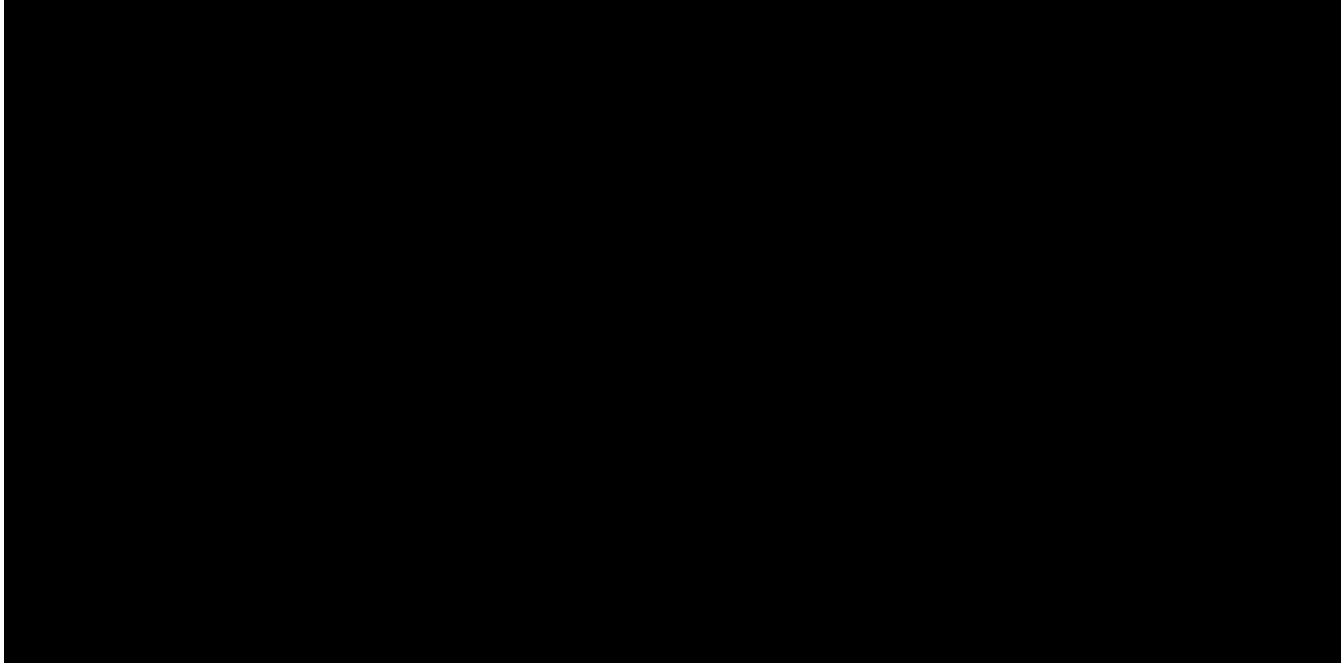
This category represents activities that implement areas of the AESCSF not included in other initiatives but are necessary to meet SP-3. These are:

- **Access-3g** - Physical access requests are reviewed and approved by the asset owner
- **Architecture-3l** - Configuration of and changes to firmware are controlled throughout the asset lifecycle
- **Asset-4i** - Change logs include information about modifications that impact the cybersecurity requirements of assets.
- **Asset-AP3** - Asset inventories have not been updated in the past 24 months.
- **Privacy-1k** - A documented process exists for responding to privacy enquiries and complaints, including customer correction of their personal information.
- **Response-4l** - Spares for selected IT and OT assets are available.
- **Response-4m** - Continuity plans are aligned with identified risks and the organisation's threat profile (THREAT-2e) to ensure coverage of identified risk categories and threats.
- **Response-4o** - The results of continuity plan testing or activation are compared to recovery objectives, and plans are improved accordingly.
- **Risk-1g** - The cyber risk management program aligns with the organisation's mission and objectives.
- **Risk-2h** - Cyber risk identification activities leverage asset inventory and prioritisation information from the ASSET domain, such as IT and OT asset end of support, single points of failure, information asset risk of disclosure, tampering, or destruction.
- **Risk-2l** - Information from ARCHITECTURE domain activities (such as unmitigated architectural conformance gaps) is used to update cyber risks and identify new risks.
- **Risk-2m** - Cyber risk identification considers risks that may arise from or impact critical infrastructure or other interdependent organisations.
- **Risk-3g** - Cyber risk analyses are updated periodically and according to defined triggers, such as system changes, external events, and information from other model domains.
- **Risk-4d** - Results from cyber risk impact analyses and cybersecurity control evaluations are reviewed together by enterprise leadership to determine whether cyber risks are sufficiently mitigated, and risk tolerances are not exceeded.
- **Risk-4e** - Risk responses (such as mitigate, accept, avoid, or transfer) are reviewed periodically by leadership to determine whether they are still appropriate.

5.7.2 Costs

Option 3 was forecast on a bottom-up basis. Total expenditure for this option in the 2025–30 RCP is \$47.5 million, including \$2.6 million capex, and \$45.0 million opex. This includes a recurrent opex step change of \$15.9 million. The expenditure breakdown is provided below in Table 16. Details associated with the step change are provided in Appendix F.

Table 16: Option 3 – Total cost by cost type (\$m Jun 2022 Real)

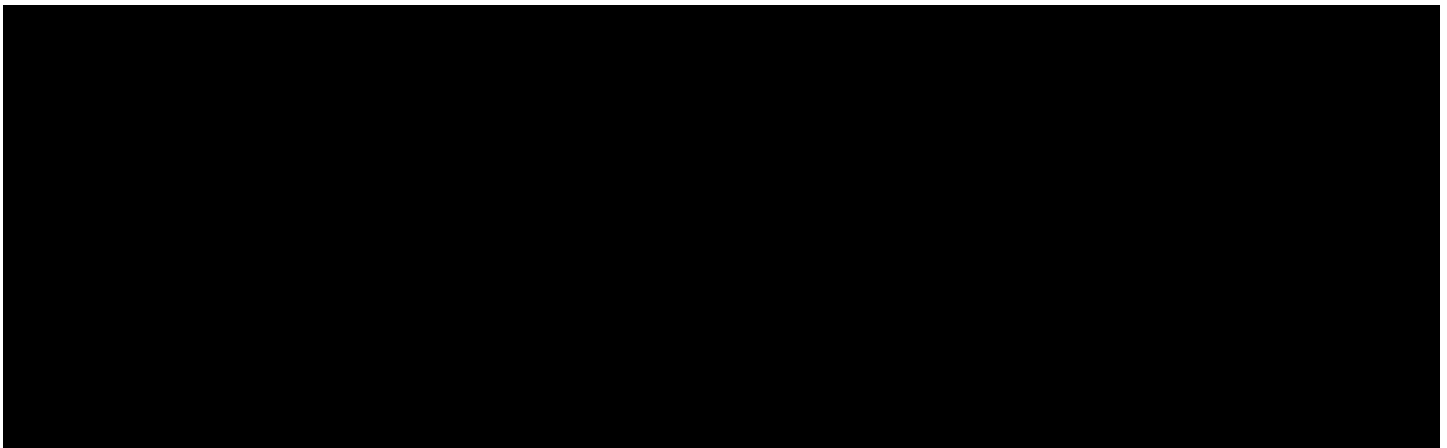
A large black rectangular redaction box covers the content of Table 16, which would otherwise show the total cost by cost type for Option 3.

The \$29.0 million non-recurrent opex component of the forecast relates to developing the uplift in our cyber security capability. This includes development and implementation of systems capabilities as well as process uplifts associated with the new systems. As the software in question is all cloud based (SaaS), accounting guidance mandates that this expenditure be treated as opex.

There is also a forecast \$15.9 million (\$5.4 million per annum moving forward) recurrent opex component. The majority of this relates to licensing fees for software required to support the capability uplift. The remainder is the cost of additional resources to maintain the uplifted cyber security systems and processes.

5.7.3 Risks

Table 17: Option 3 – Risk assessment summary

A large black rectangular redaction box covers the content of Table 17, which would otherwise show the risk assessment summary for Option 3.

⁶⁹ The level of risk post current controls (ie after considering what we currently do to mitigate the risk).

⁷⁰ The future level of risk once treatments proposed in this option have been implemented.

As with Option 2, Option 3 results in all risk categories being mitigated to at least a Medium risk. The full risk assessment is provided in Appendix B.

5.7.4 Quantified benefits

Similar to Option 2, the quantified benefits associated with Option 3 include Cost avoidance and Risk monetisation.

Cost avoidance (\$24.6 million)



This table is redacted with black bars, obscuring the specific data points for cost avoidance benefits.

Risk monetisation (\$201.2 million)

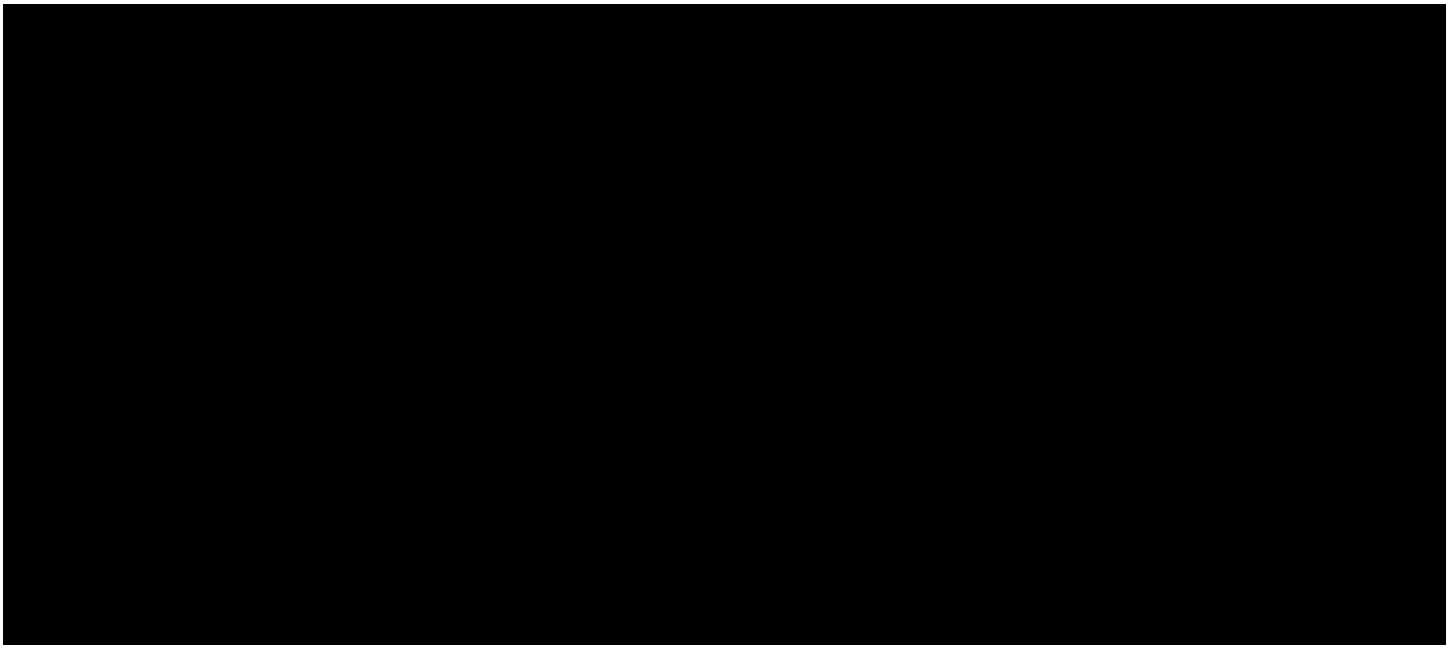


This table is redacted with black bars, obscuring the specific data points for risk monetisation benefits.



This table is redacted with black bars, obscuring the specific data points for additional quantified benefits.

Table 18: Quantified benefits for Option 3



The main body of Table 18 is completely redacted with a large black block, preventing any data from being visible.

5.7.5 Unquantified benefits

Appendix D summarises how each of the controls addressed by this option mitigates each of our defined risk events and impacts overall risk reduction.

6. Deliverability of recommended option

The 2023 Cybersecurity Workforce Study conducted by ISC2⁷¹ describes the shortage of skilled cyber security professionals that exists worldwide. According to the report, the global workforce currently lacks 4.0 million qualified cyber security professionals, a significant increase from the previous year's estimate, and this is expected to continue to rise. This shortage poses a significant risk to organisations as they struggle to protect their networks and sensitive data from increasingly sophisticated cyber threats.

We are aware that this gap presents a real threat to the safety and security of our business and our customers, and we are taking several proactive steps to ensure that we can deliver the increase in capability required to implement of the preferred option.

Workforce building

Due to the issues identified above, we identified in 2020 that we needed to build a sustainable capability. In attempting to hire operational analysts during the previous RCP, it was evident that there are less skilled analysts within the workforce than there are skilled and experienced analysts. As a result, we identified the need to select supporting security technologies that were, among other things, easy to learn and use. For example, in choosing a security and event manager tool, we chose a solution for its ease of use and ability to correlate events in a graphical approach. This has enabled us to hire less-experienced security operation analysts and then train them in the skills needed to work within the capability.

From this, we have then been able to build a capable workforce and will use this experience and approach to continue to build into the future and deliver this program of work. This also facilitates our more experienced analysts moving to the next stage of their career during this program of work and leading the delivery of aspects of the uplifts outlined in this business case. With our own experienced analysts working on the uplift program of work, we also retain critical business knowledge and have a higher chance of successful change management and delivery of outcomes.

In addition to the above approach to workforce building and operations, to identify and attract new talent, we are planning on partnering with educational institutions to offer internships and work experience programs for students interested in pursuing a career in cybersecurity. This allows us to identify and nurture talent from an early stage, provide them internal career growth opportunities, and build a pipeline of skilled professionals. In utilising this workforce-building approach, we are ensuring that we retain and build on organisational knowledge and understanding.

Workforce upskilling

To develop the skills our cyber security workforce requires, we are collaborating with industry experts to provide training and development programs to both new and existing staff. This upskilling of our staff provides them with the knowledge and tools necessary to identify and mitigate cyber threats effectively, as well as positioning us as an employer of choice for cyber security professionals.

As noted above, we will be partnering with educational institutions to offer internships and work experience programs for students interested in pursuing a career in cyber security. This allows us to identify and nurture talent from an early stage and build a pipeline of skilled professionals.

Most recently, our collaboration with industry and government included partaking in the North Atlantic Treaty Organisation (**NATO**) Cooperative Cyber Defence Centre of Excellence (**CCDCOE**) exercise, Locked Shields. The exercise aims to train technical teams of cyber professionals (rapid reaction teams) and strengthen their cooperation with legal, media, and strategic decision-making entities through a simulated

⁷¹ [ISC2 Cybersecurity Workforce Study 2023 | ISC2 \(media.isc2.org\)](https://www.isc2.org/resources/insights/articles-tools/cybersecurity-workforce-study-2023)

hostile and vulnerable cyber and information crisis. Other participating partners included McGrathNicol, CyberOps, Flinders University, DTEX, SecureState, SAAB, CISCO and Veroguard.⁷²

In preparing for the next phase of cyber security maturity uplift, we will continue to facilitate the development of our internal talent and then utilise these resources in delivery. By providing our current workforce with opportunities to develop and stretch their capabilities outside of their current skillset, we believe we can reduce the operational impact to our capability and rely less on hiring external resources for uplift focussed work.

Automation and artificial intelligence

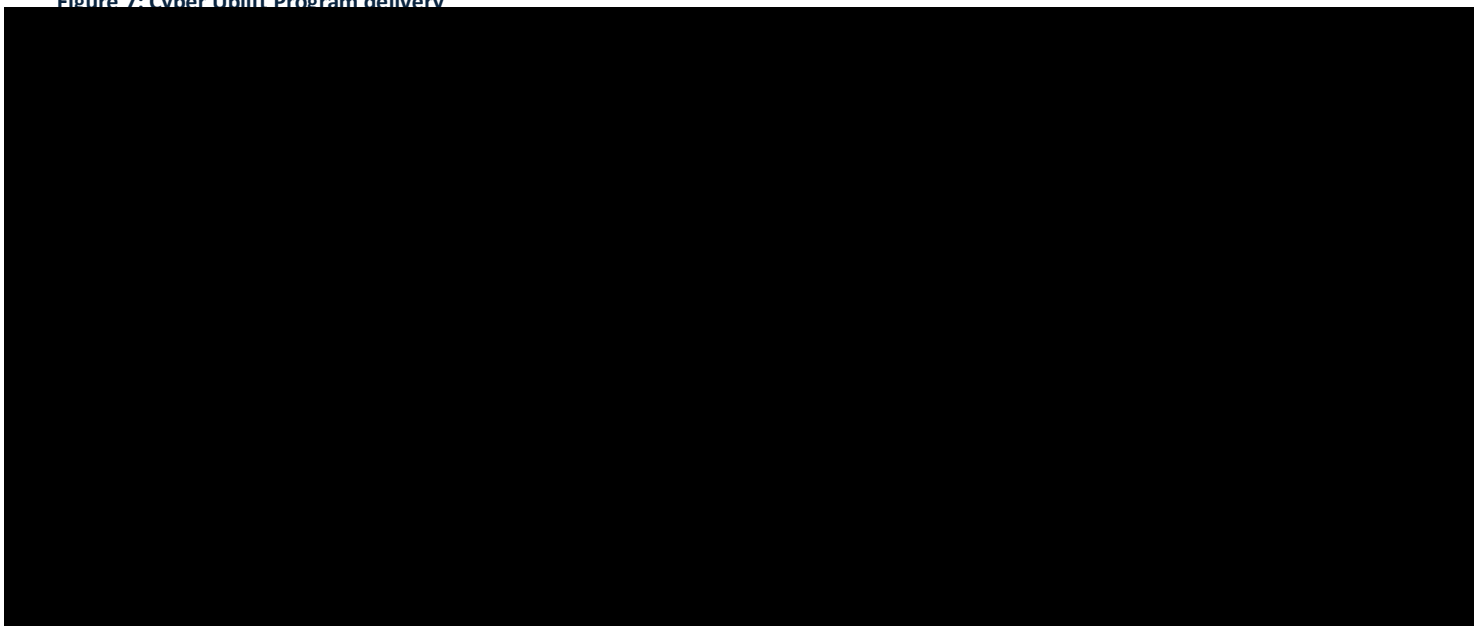
We are also exploring innovative solutions such as automation and artificial intelligence to help bridge the skills and people gap. These tools are designed to augment our existing cyber security capabilities and reduce the burden on our existing staff. This not only helps to address the skills gap but also improves our overall cyber security posture by reducing the reliance on key staff and people in general.

Strategic Partnerships

We have a large and trusted network of strategic partners, who we use to augment our internal resources when required, using standard negotiated rates. These partnerships will continue to play a critical role in the expanding program.

We believe that by investing in our staff and exploring innovative solutions, we will have the resources available to deliver on the preferred option. Figure 7 shows the planned delivery profile of the Cyber Security Uplift program, by control.

Figure 7: Cyber Uplift Program delivery



⁷² [NATO CCDCOE Locked Shields 2023 Partner Run — Australian Cyber Collaboration Centre \(cybercollaboration.org.au\)](https://www.cybercollaboration.org.au)

7. How the recommended option aligns with our engagement

The expenditure and program proposed in this business case is designed to achieve service outcomes that were directly supported by our customers, as ultimately reflected in the recommendations of the People’s Panel. This is noting that:

- Cyber Security has been an important topic in our consumer and stakeholder engagement program. One of the four key themes that framed our engagement under a desire to ‘focus on what matters’ to our consumers has been that of ‘a reliable, resilient, and safe electricity network’.
- In engaging on this theme, and under the specific topic of ‘IT and cyber security’, we undertook a deep-dive workshop called a ‘Focused Conversation’ with a broad range of consumer, industry, government and regulatory body representatives, and members of our CAB. For this Focused Conversation, the level of engagement agreed by our CAB was ‘inform and communicate’ with respect to the overall quantum of our potential IT expenditure proposal,⁷³ and ‘engage’ with respect to cyber security – we therefore sought recommendations on the service outcomes that customers prefer and expect in relation to cyber security.⁷⁴
- With particular regard to the cyber security program, we engaged on the identified need by outlining information on: the totality of our IT expenditure and what our IT function undertakes in the whole organisation; the role of cyber security programs; and the risks of cyber threats to the company and customer services. We then posed three scenarios of how we could respond to the need and the expected outcomes for customers in relation to service, expenditure and price – these include (1) no uplift in cyber investment (2) spending to meet compliance with SP-3 and (3) spending to go beyond SP-3 requirements.
- While our customers and stakeholders were consistently mindful of energy affordability concerns, the Focused Conversation arrived at a clear consensus recommendation to the People’s Panel as the next stage in our engagement program, that SA Power Networks should sufficiently invest to meet SP-3 compliance by the end of the 2025-30 RCP.⁷⁵
- Ultimately, the People’s Panel deliberated on the totality of the recommendations made in the Focused Conversations and the overall balance of service and price. The People’s Panel did not agree with the recommendation of the Focused Conversation as it considered that the level of investment was insufficient to adequately protect infrastructure and support the level of services that customers will expect over 2025-30. The People’s Panel instead recommended that SA Power Networks invest in a level of cyber security maturity that exceeds SP-3. In doing so, the People’s Panel noted:
 - the consequences of inadequate spending on cyber are catastrophic, and the community is unwilling to accept this risk.
 - the AESCSF SP3 was not as high a standard as that employed in Europe and the United States, and the Panel is therefore seeking a more comprehensive cyber defence level.
 - the importance of cyber security in one of the most critical pieces of infrastructure in the state – inadequate spending on cyber security could be catastrophic and therefore a cautious approach was taken.
- the formal recommendation of the People’s Panel reflects a desire of our customers to not be bound by the SP3 level of maturity, and therefore aligns with the preferred option set out in this business case.

⁷³ It should be noted that a number of IT expenditure areas were subject of ‘engage’ level Focused Conversations via separate engagement topics wherein recommendations on service and price outcomes were sought (this includes: expenditure on an ‘assets and works program phase 3’ and expenditure on more ‘personalised and on demand services’).

⁷⁴ This was covered in the IT and Cyber Security Focused Conversation. Materials presented at the Focused Conversations are available on our TalkingPower website under the page titled ‘focused conversations’. [<https://www.talkingpower.com.au>].

⁷⁵ The recommendations of the Focused Conversation are contained in documents published on our TalkingPower website under the page titled ‘focused conversations’. SAPN, *final outputs and recommendations to the People’s Panel for Reliability and Bushfire Safety*, October, 2023. Accessible on: [<https://www.talkingpower.com.au>].

Since conducting the People’s Panel process, we published a Draft Proposal to play back how we have given effect to customer recommendations and to confirm that those recommendations remain valid given continued cost of living pressures and to obtain further input to refine our Regulatory Proposal. Submissions received on the Draft Proposal suggest there are some mixed views on the recommendation now set out in this business case. However, on balance, we consider that submissions have not raised any information to suggest that the recommendations of the People’s Panel in relation to cyber security do not remain valid. This is noting that:

- Members of the People’s Panel affirmed that their recommendations, including in respect of the cyber security uplift program as set out in this business case, remain current.⁷⁶
- Some parties such as South Australian Council of Social Service Submission (**SACOSS**)⁷⁷ and the Department of Energy and Mining (**DEM**)⁷⁸ generally urged further consideration of the overall magnitude of our forecast capex in totality. Further, while SACOSS considered that SA Power Networks should not look to exceed its expected legislative obligations, DEM did not outline that it disagreed with the program, rather that they expect it will need to be shown to be prudent and efficient. This business case provides the detailed evidence and justification of the prudence and efficiency of the recommended option.

More generally, we have also observed a view from our customers and stakeholders that we ensure that we are only investing where it is prudent and efficient to do so. Accordingly, since our Draft Proposal we have amended our approach to uplifting our cyber security by selecting option 2 rather than option 3 in this business case, in order to take a risk prioritised approach that best maximises benefits to consumers of mitigating cyber threats.

7.1 Alignment to the views of other stakeholders

ASIO outlined in its 2021–22 Annual Report that cyber espionage remains the most pervasive approach adopted by our adversaries. The increasing organisation of our economy, coupled with changes in how and where people work, will create new vulnerabilities that when targeted, could have significant consequences for Australia’s economic prosperity, security, and sovereignty. A more interconnected society, combined with evolving hostile cyber capabilities, will continue to provide foreign powers with opportunities and the means to remotely disrupt and/or damage Australia’s infrastructure and economy.⁷⁹ We are a key part of Australian society and require suitable cyber security controls and management to maintain trust in, and the reliability of, our network.

⁷⁶ DemocracyCo, *Submission: SA Power Networks Draft Regulatory Proposal 2025-30*, 30 August 2023.

⁷⁷ SACOSS, *on SA Power Networks’ 2025-30 Draft Regulatory Proposal*, September 2023.

⁷⁸ DEM, *South Australian Department of Energy and Mining – Submission*, October 2023.

⁷⁹ [Threats to our way of life | Australian Government Department of Home Affairs Transparency Portal \(transparency.gov.au\)](https://transparency.gov.au)

8. Alignment with our vision and strategy

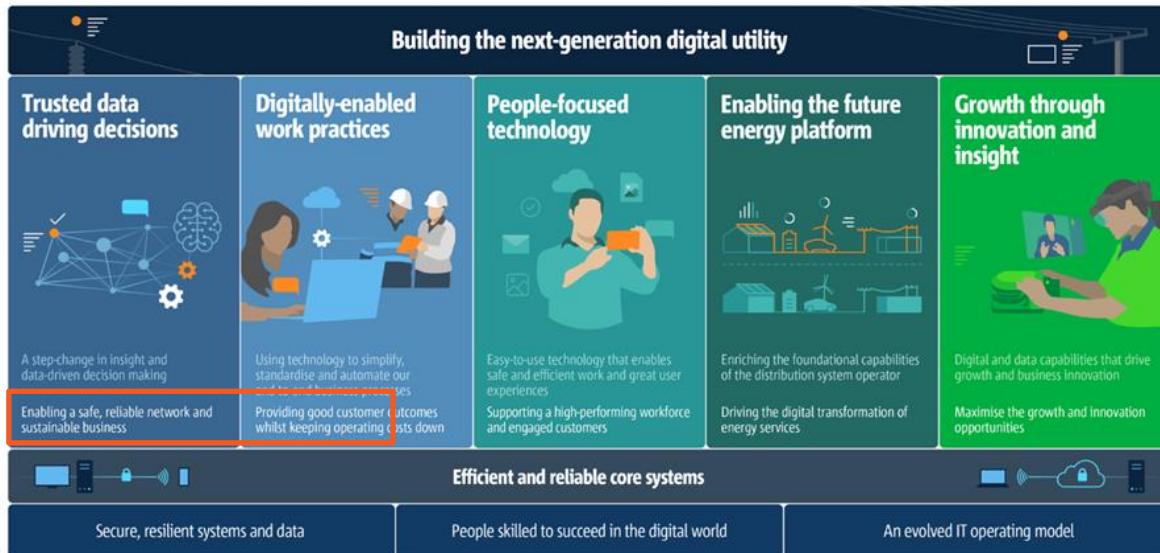
We are the sole electricity distributor and play a vital role in powering South Australia. As the utilities model evolves and energy sources become more distributed, we are adapting to the changing landscape by incorporating new technologies and data-driven approaches to meet customer needs and optimise their operations. However, with the increasing reliance on technology comes 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 (Figure 8) outlines the long-term strategic direction for IT – a strong cybersecurity posture (‘secure and resilient systems and data’) is 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; and
- modern digital identity management.

Figure 8: SA Power Networks Digital & Data Strategy

Digital & Data Strategy



9. Reasonableness of cost and benefit estimates

Labour

Most labour costs for this business case have been calculated using standard SA Power Networks internal labour rates. These rates are aligned with industry standards and consistent with other network service providers in the sector. External labour costs for cyber security architects and minor estimated costs for professional services have been based on current prices.

The labour effort required for implementing the security controls outlined within this business case reflects our experience and knowledge gained from our current and previous uplift programs, leveraging lessons learned. This approach ensures that our labour resources are effectively allocated and that we have a realistic understanding of the time and resources required for the successful execution of our cybersecurity initiatives.

Software costs

The number of software licenses required reflects the size and needs of our organisation. Where appropriate, cost increases associated with certain software applications have been factored in to reflect expected increase in capability, ie, additional modules that will be taken up during the period to meet evolving requirements and as the organisation matures to this level. This reflects the need to adapt and stay up to date with the latest technologies and solutions to effectively address emerging cyber threats. Unit prices for each software application and module reflect market rates as at December 2021.

Cost benchmarking

As alluded to in section 3.4, a \$ 70 million (+/- 20%, over the next five year submission period) benchmark 'efficient average' total cyber security investment for DNSPs was included in the recent AER Ausgrid determination⁸⁰. Table 19 shows the breakdown of the total cyber security investment included in our 2025-30 Regulatory proposal. The SA Power Networks \$71.7 million total is similar to the \$70 million benchmark.

Table 19: SA Power Networks total cyber security investment in 2025-30 (\$June 2022)

Category	Estimate (\$m)	Source
Current		
Recurrent IT Opex	8.6	Base Year roll-forward (23/24 estimate x 5)
Recurrent IT Capex – Opex switch	15.3	Recurrent Cyber business case 5.12.6
Recurrent OT Capex	3.1	
Current Totex	27.0	
New (this business case)		
Non-recurrent IT & OT Opex	26.6	Cyber uplift business case (this business case)
Non-recurrent IT & OT Capex	2.6	
Recurrent IT & OT Opex	15.4	
New Totex	44.7	
Total Forecast	71.7	

⁸⁰ [Ausgrid Draft Decision Attachment 5 - Capital expenditure – Ausgrid – 2024-29 Distribution revenue proposal – September 2023](#), page 21 | AER (aer.gov.au)

Additionally:

- we are a High criticality entity, so would expect to be towards the upper end of the spectrum of High and Moderate criticality entities included in the \$70 million AER cost benchmark;⁸¹
- as discussed in section 5.6.1, we believe that the risk-based uplift that we are proposing achieves a level of maturity, and therefore risk reduction, that is above the AESCSF in many areas; and

- [REDACTED]

Cost of remediation

While not a similar organisation, Medibank suffered a significant cyber security incident in October 2022. Recently, Medibank released estimates of the cost of that cyber security incident to their organisation. For the ransomware incident that occurred, Medibank is estimating a cost of \$40 million to \$45 million to recover from this incident and increase cyber security to levels aligned to their risk appetite. While Medibank and SA Power Networks are different organisations, the user base is similar in size, indicating that technology, processes, and people uplift investment would align. The requested investment over the regulatory period for us, when considering Medibank’s experience and employee size, indicates a level of reasonableness for the cost of this investment request.

On 16 March 2023, Latitude Financial disclosed a cyber security incident⁸² where a threat actor stole an employee’s login to breach two of the company’s service providers that were holding Latitude’s customer data. Latitude believes that 14 million customers or loan applicants from Australia and New Zealand have been affected. They also found that the attacker stole 53,000 passport numbers. Latitude Financial is forecasting a first-half loss of between \$95 million and \$105 million after the attack left them with a severely restricted ability to earn income for five weeks.⁸³ The company is setting aside approximately \$53 million after tax for the first half of the year for costs associated with the cyber incident. This includes \$7 million in costs already incurred and an additional \$46 million after tax for other remediation costs. Although Latitude Financial is not in the same industry as us, this demonstrates the exceptionally high cost associated with a cyber security incident.

Benefits

Section 3.2 describes the reduction in higher frequency incidents that occurred through the period due to the additional cyber controls embedded as operational capability and as part of the 2020-25 RCP cyber uplift program. However the rapidly evolving threat landscape and increasing complexity of cyber attacks discussed means that not continuing to uplift controls further in the 2025-30 period will result in higher impact incidents, with the reversion to a higher incidence of higher consequence breaches as seen as the start of the current RCP (see Figure 1). P4 breaches will become P3s; P3 breaches will become P2s, etc.

Forecast incidence of P2-P4 breaches

As shown in Figure 1 in section 3, we have had control failures resulting in an increasing trend of breaches in cyber security over the current RCP. Our Base case (no increase in controls) extrapolates this trend using a linear growth rate, in order to forecast the total number of cyber breaches

⁸¹ It is assumed that the Ausgrid peer entities include a mix of High and Moderate criticality entities under the AESCSF.

⁸² [Latitude Financial data breach now impacts 14 million customers | BleepingComputer \(bleepingcomputer.com\)](#)

⁸³ [ASX Announcement - Half and Full Year Guidance and Cyber Update 26 May 2023 | Latitude \(announcements.asx.com.au\)](#)

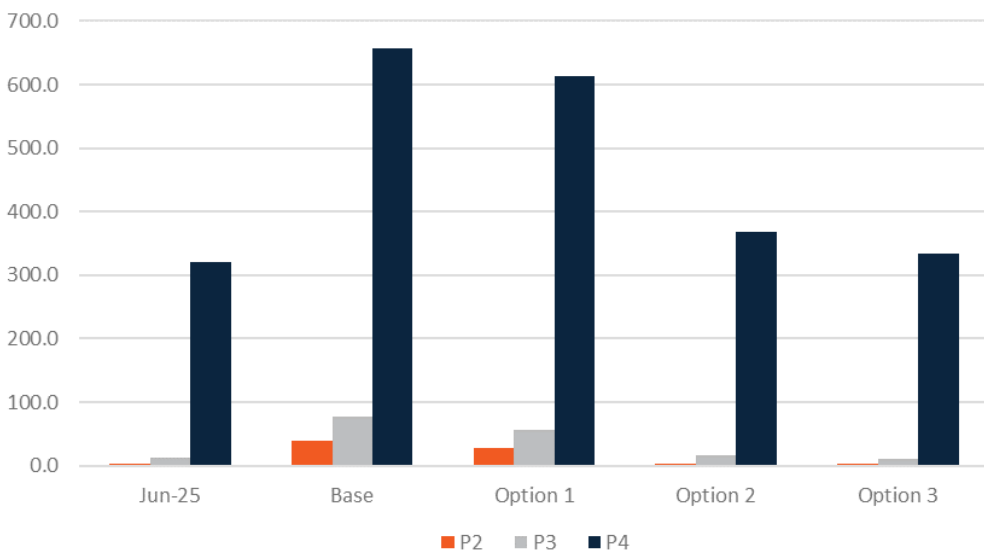
over the ten-year (2025-2035) benefit period. We consider the linear growth rate a conservative assumption, with there being a reasonable likelihood that the volume of attacks, and therefore breaches, will escalate exponentially without any uplift in capability (as shown by the escalating number of breaches over the last twelve months).

When there is an increase in early control failures, the additional controls in place to provide security in depth are increasingly likely to also be attacked and fail. We have seen this in current RCP with the evolution of MFA. While SMS was considered sufficient three years ago, due to attacks on this method we needed to evolve our MFA processes, and now need to use applications and ‘phishing resistant’ MFA to better protect ourselves. Without investment in the uplift of controls, and the controls that detect malicious activity when other controls fail, the likelihood of a significant major incident increases.

As discussed above, we expect that with no uplift in controls the incidence of higher priority incidents will return as attacks become better and new threats emerge. However, our base case forecasts only a 5% incidence of P2 events and a 10% incidence of P3 events by the end of the 2025-30 RCP (with the rest remaining as P4 events). This is a conservatively lower estimate than the actual proportion of P2 and P3 incidents evidenced in the first two years of the current RCP.

The other options included in our business case, including our preferred option, assume a reduction in both the number of breaches, as well as the number of higher consequence breaches. The resulting breach trend over time under each option is shown in Figure 9.

Figure 9: Forecast breaches by breach type by June 2030 under the Base case and each alternative option



[Redacted content]

[Redacted content]

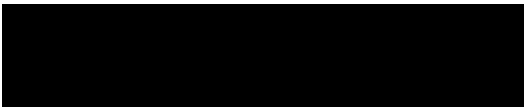
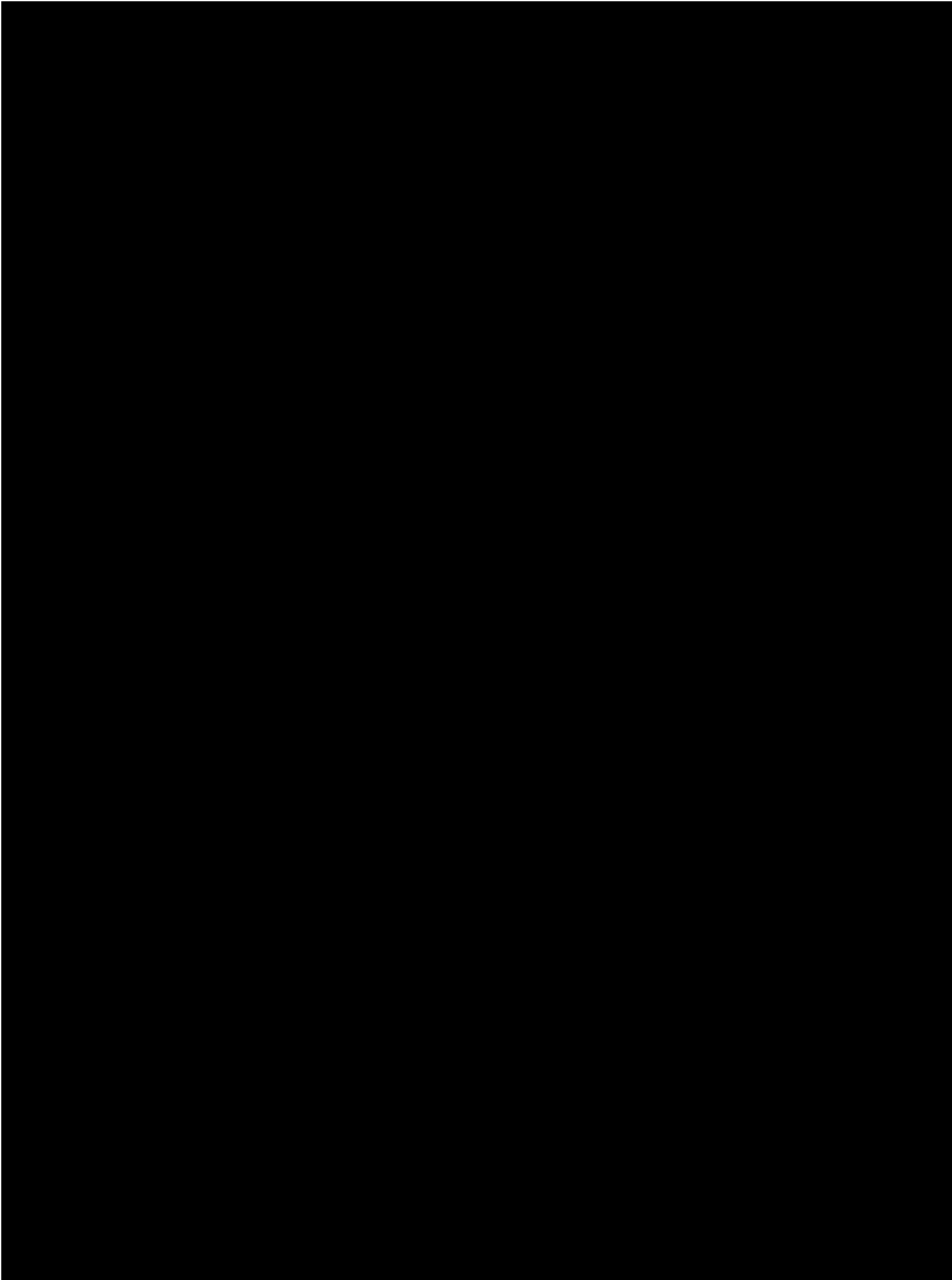
[Redacted]

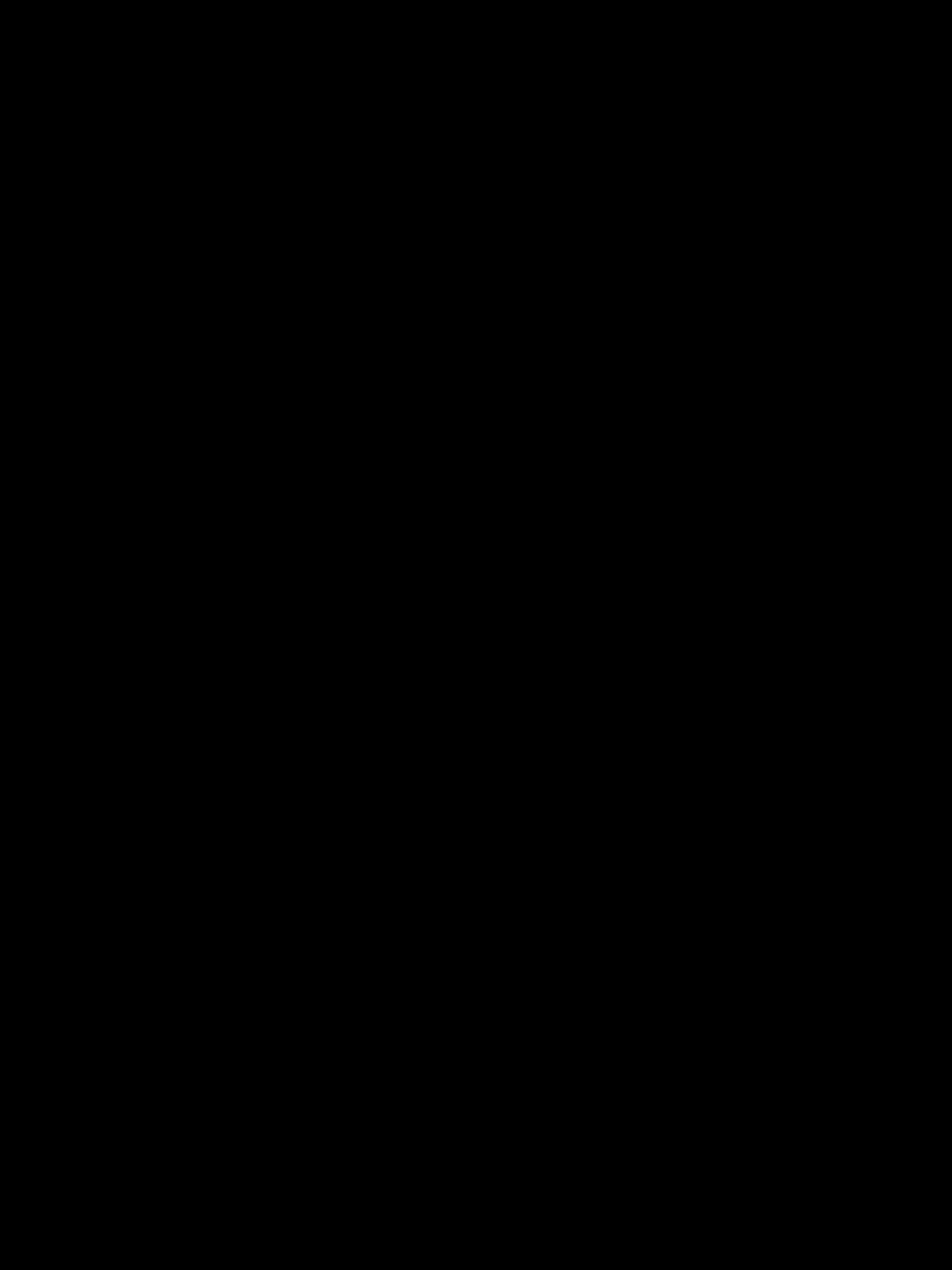
[Redacted]

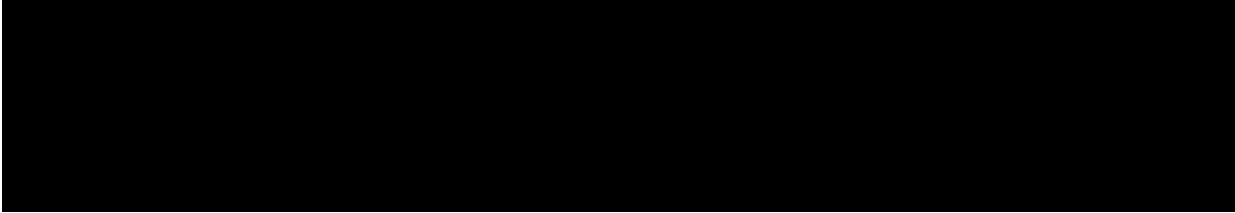
[Redacted]

[Redacted]

[Redacted]







10. Reasonableness of input assumptions

AESCSF version

We recognise the importance of staying consistent with industry standards and regulations. With version 2 of the AESCSF having been released in late October 2023, Option 3 of this business case (Risk-based approach + Comply with AESCSF SP-3) was finalised to reflect this version. We expect that compliance with AESCSF version 2 will become a legislated requirement in the future.

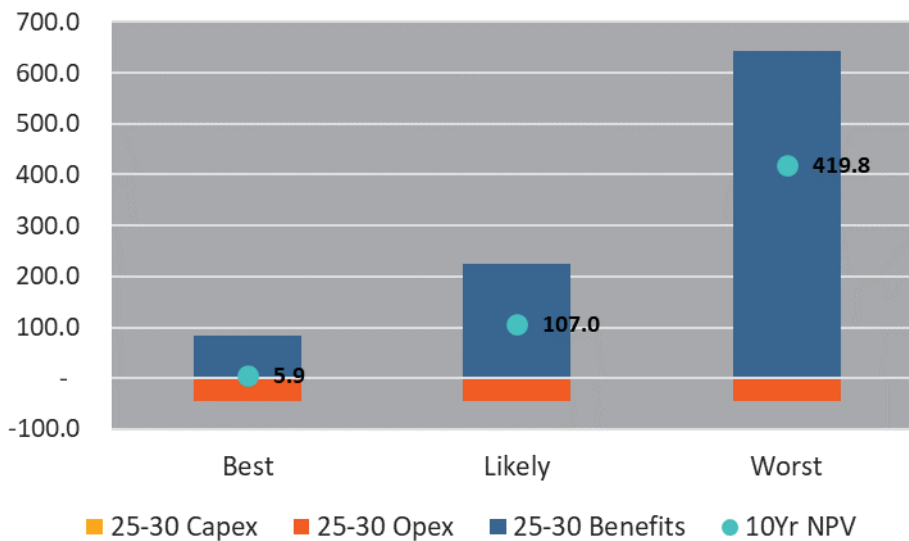
11. Scenario and sensitivity analysis

As detailed in section 9, we modelled three benefits scenarios for this program. These benefit assumptions are combined with our standard range of discount rates to provide a set of possible NPVs under each of a Best, Likely and Worst-case scenario⁸⁹. As shown in Table 23, positive NPVs are achieved under all nine scenarios for our preferred option. While the central discount rate scenario for the Likely case is \$107.0 million, even the lowest NPV (upper bound discount rate under the ‘Best Case’ scenario) is positive, at \$5.2 million across the 10-year period modelled.

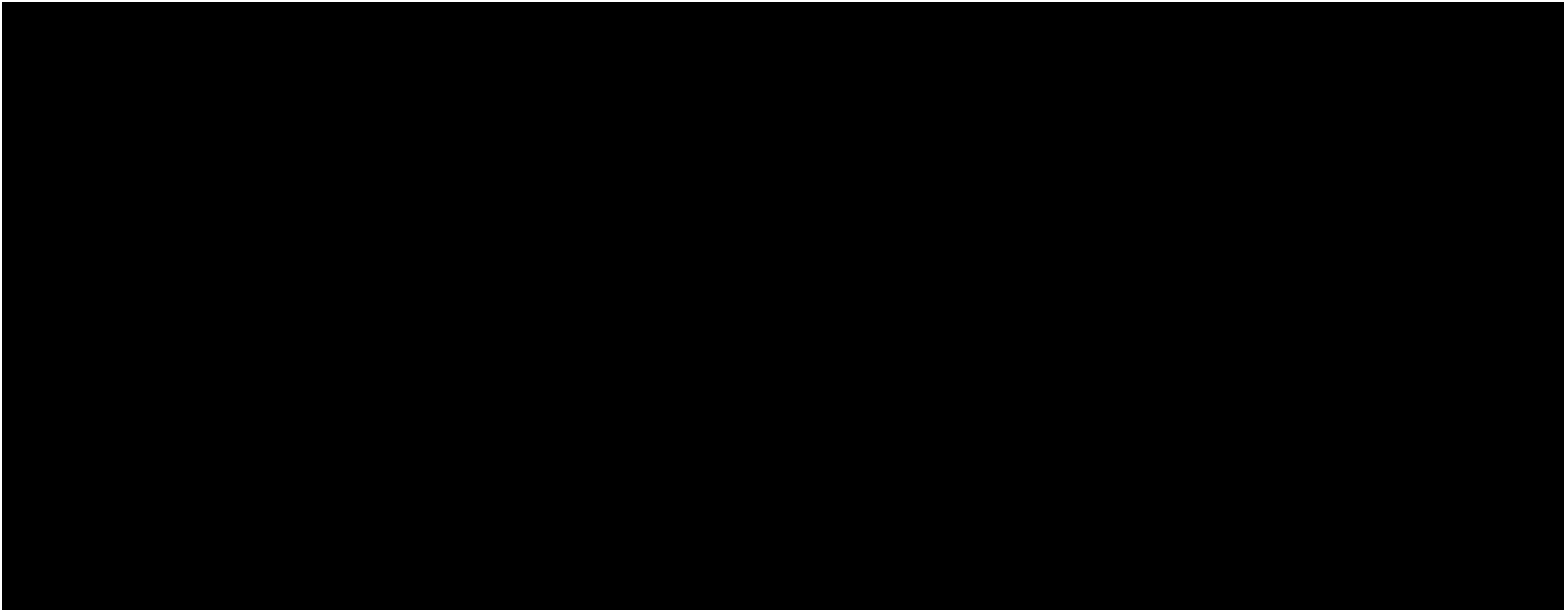
Table 23: Preferred option NPV under different benefit consequence and discount rate scenarios (\$m, real Jun 2022)

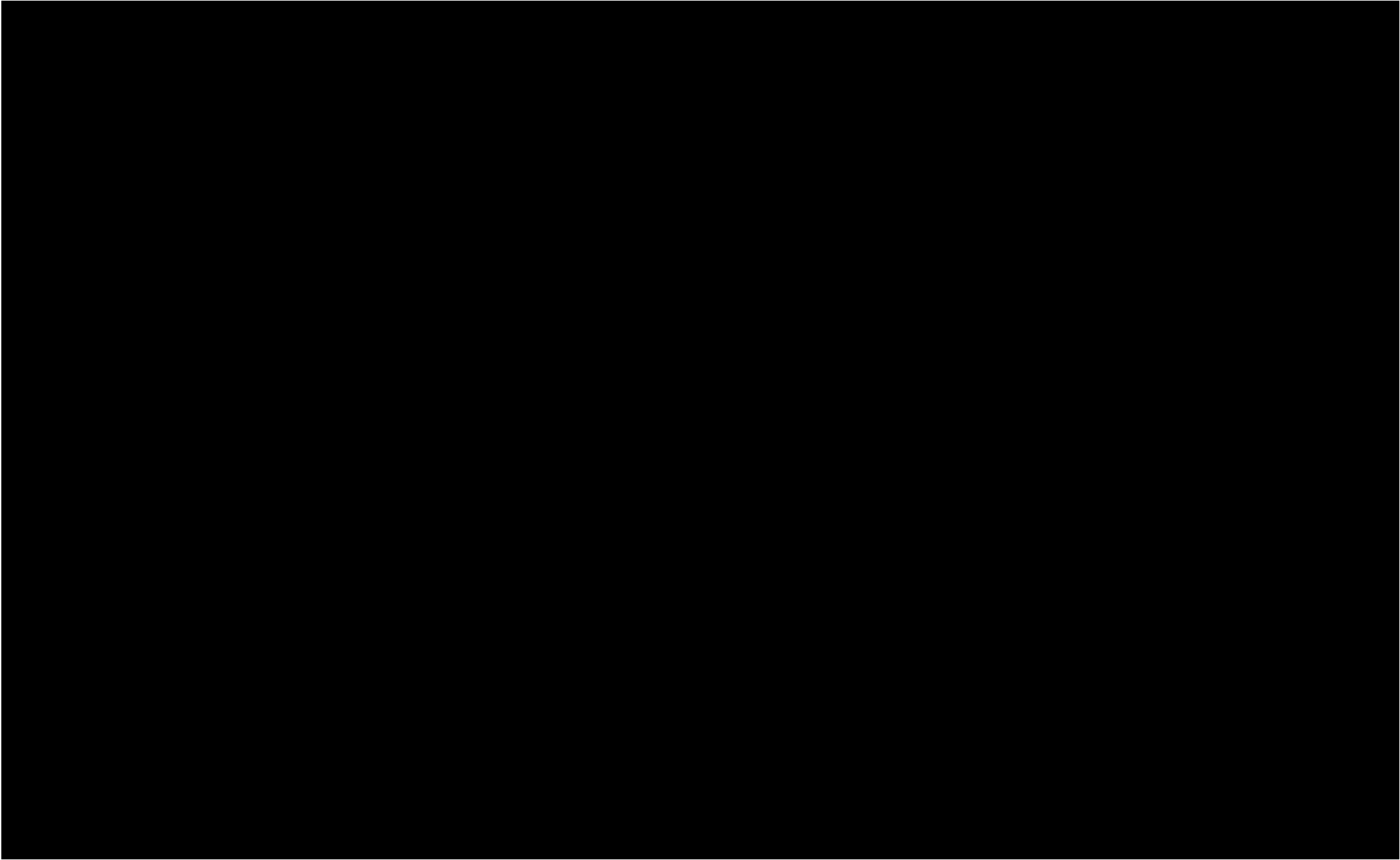
Benefits scenario	Discount rate	10 year Benefits	10 year NPV
Best case	Lower	84.9	6.8
	Central		5.9
	Upper		5.2
Likely case	Lower	225.7	112.4
	Central		107.0
	Upper		102.8
Worst case	Lower	644.1	437.5
	Central		419.8
	Upper		405.9

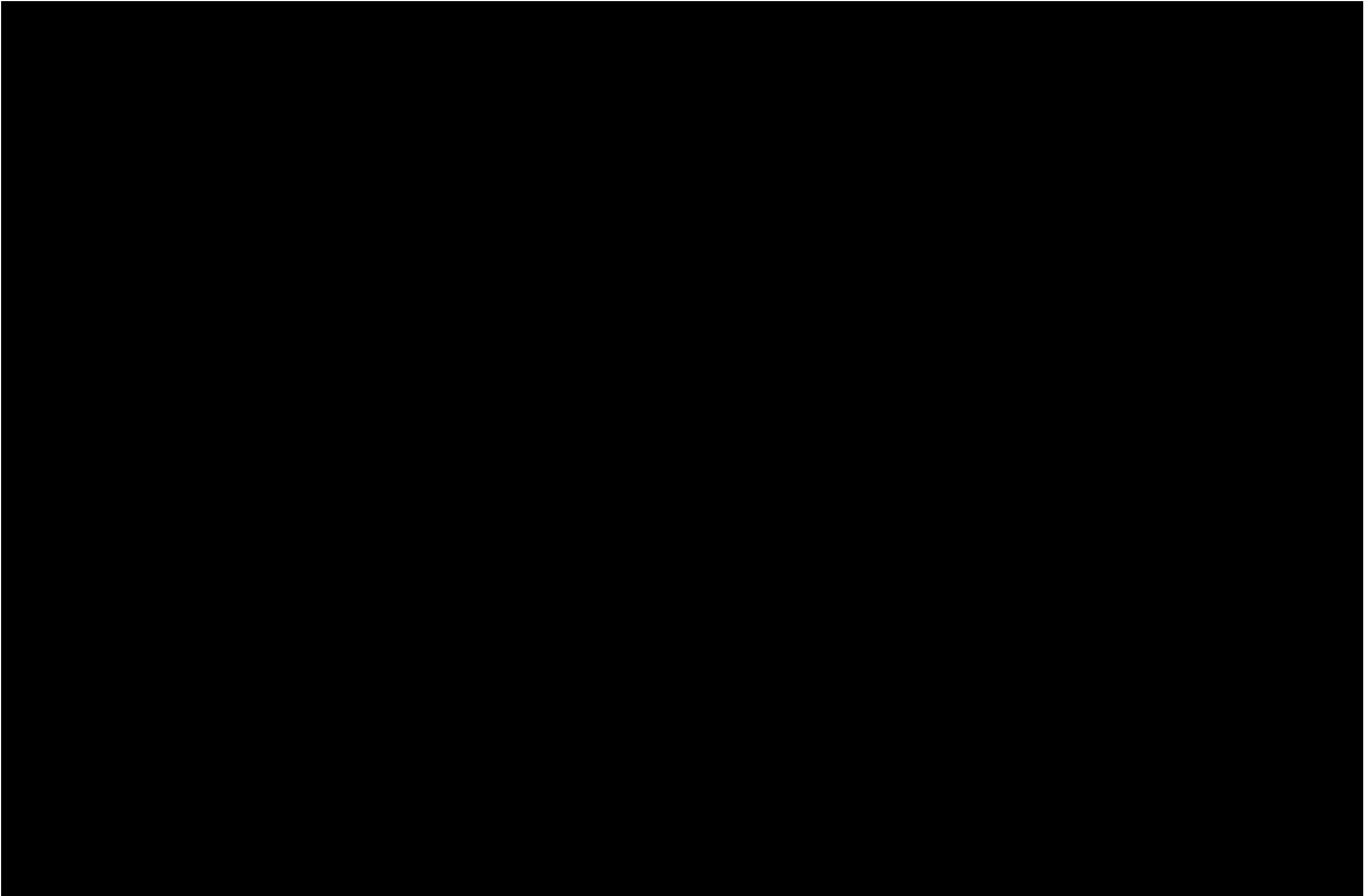
Figure 10: NPV outcome by scenario – preferred option (\$m, real Jun 2022)

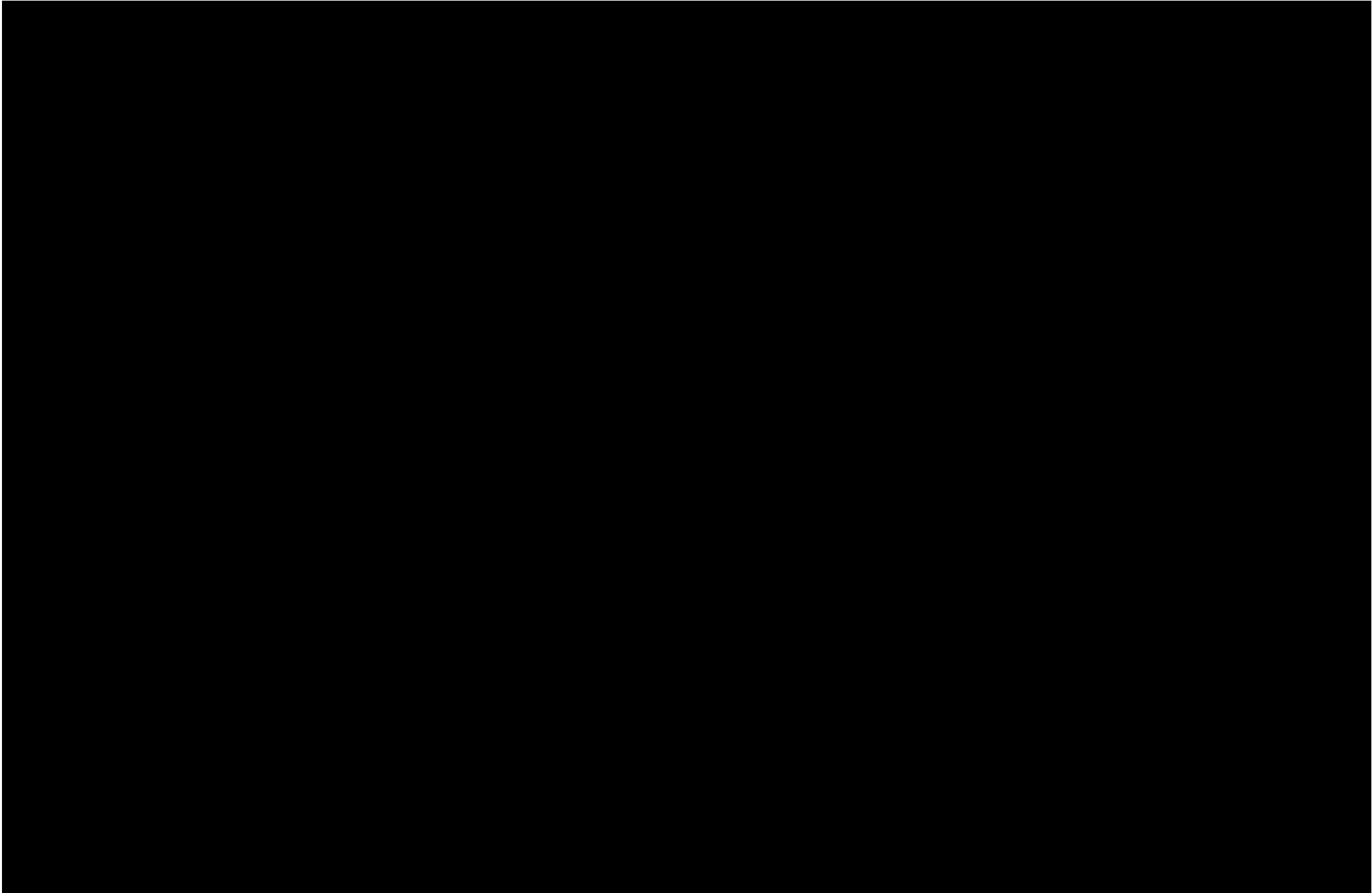


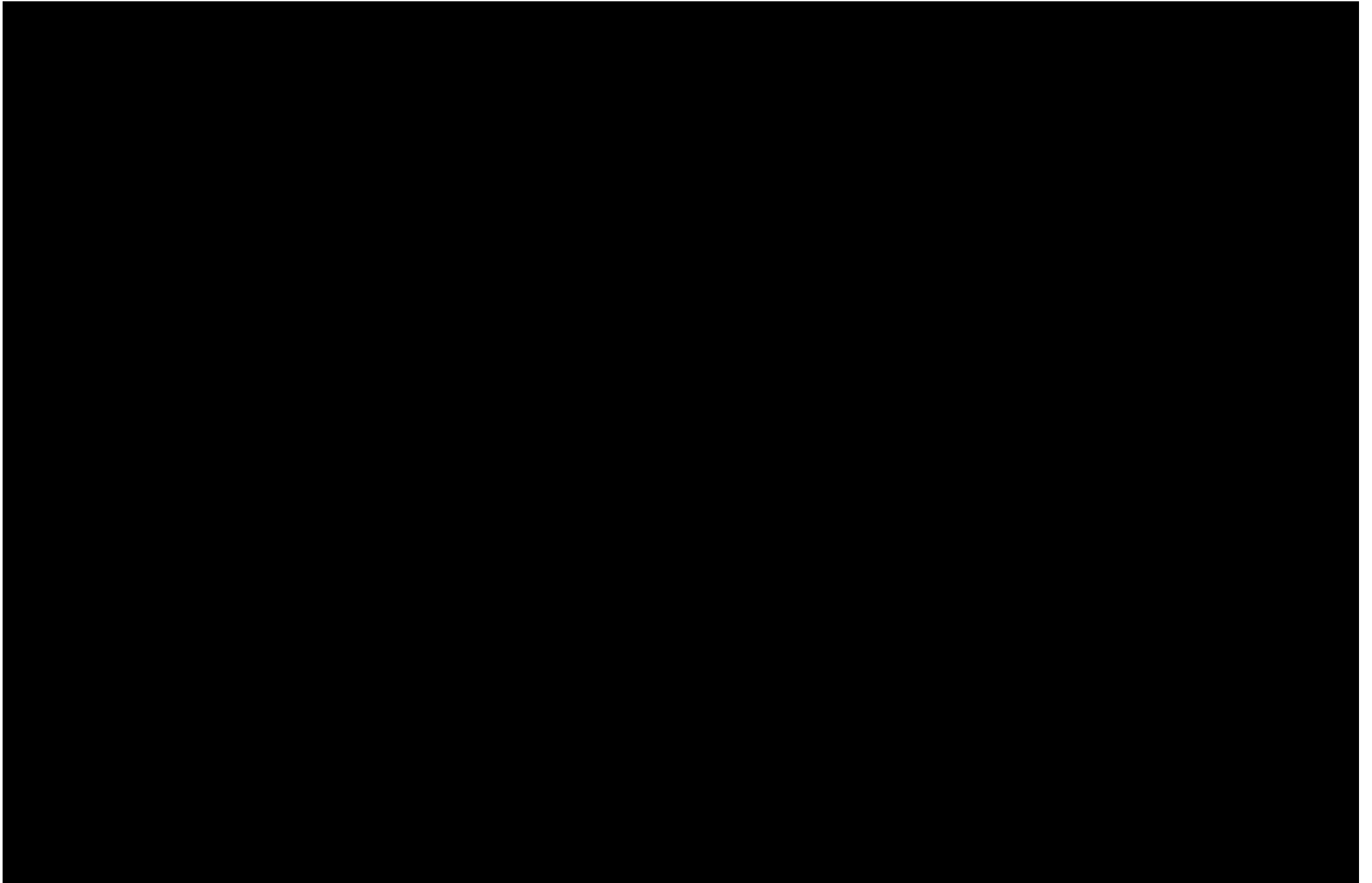
⁸⁹ These descriptions reflect the best and worst case for SA Power Networks and our customers, ie the best case scenario reflects the minimum likely estimated consequences, and the worst case reflects the maximum likely estimated consequences.











C. Appendix C – How the controls address the key drivers

	Controls	The increasing complexity, prevalence and targeted nature of cyber security threats	Increasing compliance obligations	A changing electricity distribution industry	Escalating Ransomware Threat	Growing Supply Chain Risk	Developments in, and increasing adoption of emerging technologies such as robotics, artificial intelligence (AI), quantum computing and predictive intelligence	Increasing BYOD adoption	Increasingly sophisticated adversaries	Growing risks in the increasingly interconnected operational environment	Recurring significant cyber security incidents	A complex digital identity
Option 1	Role based user access	X	X	X		X	X	X	X	X	X	X
	Application Control	X	X		X		X		X		X	
Option 2 Option 3	Zero trust architecture	X	X	X	X		X	X	X	X	X	
	Security operations (SECOPS)	X	X	X	X	X	X	X	X	X	X	
	IT resiliency lifecycle	X	X		X				X		X	
	Secure software development l	X	X	X			X		X		X	
	Third-party security	X	X		X	X			X		X	
	Operational technology	X		X					X	X	X	
	Information protection	X		X				X	X		X	
	Tool of Trade devices	X		X	X				X		X	
	BYOD Cyber Strategy	X						X	X		X	
	Network detection and response	X			X	X	X		X		X	
	Cyber awareness	X		X	X	X	X	X	X	X	X	
	MyID											X
	AESCSF principles	X	X	X	X					X	X	X

D. Appendix D – How the controls mitigate the risks

Option 1
Option 2
Option 3

Controls	Non-recurrent cost (\$m)				Recurrent cost (\$m)				Total 25 30 Cost (\$m)	Ongoing recurrent cost pa (\$m)	
	Labour	Software	Services	Total	FTE count	Labour cost	Software	Services			
Role based user access	4.2	-	-	4.2	1	0.3	3.9	-	4.2	8.4	1.2
Application Control	0.7	-	-	0.7	-	-	1.3	-	1.3	2.0	0.3
TOTAL	4.9	-	-	4.9	1.0	0.3	5.2	-	5.5	10.4	1.5

Zero trust architecture	4.1	0.6	-	4.7	-	-	1.3	-	1.3	6.0	0.3
Security operations (SECOPS)	4.3	-	1.0	5.3	2	0.9	3.8	-	4.7	10.1	1.3
IT resiliency lifecycle	1.2	-	0.4	1.6	-	-	-	-	-	1.6	-
Secure software development lifecycle	0.7	-	-	0.7	1	0.5	0.6	-	1.0	1.7	0.5
Third-party security	0.2	-	-	0.2	-	-	0.4	-	0.4	0.6	0.1
Operational technology	3.9	-	-	3.9	3	0.9	-	-	0.9	4.9	0.9
Information protection	2.1	-	-	2.1	-	-	0.6	-	0.6	2.8	0.2
Tool of Trade devices	1.4	-	-	1.4	-	-	-	-	-	1.4	-
BYOD Cyber Strategy	1.0	-	-	1.0	-	-	1.1	-	1.1	2.1	0.3
Network detection and response	0.8	-	-	0.8	-	-	0.2	-	0.2	1.0	-
Cyber awareness	1.5	-	-	1.5	-	-	-	-	-	1.5	-
MyID	0.6	-	-	0.6	-	-	-	-	-	0.6	-
TOTAL	26.8	0.6	1.4	28.8	7	2.7	13.3	-	15.9	44.7	5.1

AESCSF principles	2.9	-	-	2.9	1	-	-	-	-	2.9	-
TOTAL	29.7	0.6	1.4	31.6	8	2.7	13.3	-	15.9	47.5	5.1

	Major Cyber Security Incident	Unable to identify or respond to cyber risks / vulnerabilities	Unable to securely manage user access and deprovisioning	Unable to effectively respond to cyber incidents	OT security risks go unidentified	Loss of Sensitive information through mismanagement	Failure to address evolving technology	Victim of ransomware attack	Supply chain failure	Inability to recover critical systems	Insider attack intentional and unintentional
Starting Risk:	Extreme	Extreme	Extreme	Extreme	Extreme	Extreme	High	High	High	High	High
	M		E			H	S				H
	M						S	E			
Residual Risk:	Extreme	Extreme	Medium	Extreme	Extreme	Extreme	High	Medium	High	High	High

	M	H		H		H	E	H	S		H
	M	H		E		M		M	M	M	M
	H	M		M	M			H		E	
	S	S		S		M					
	S								H		
	E	H			E						
						E					
	H				H			M			
						H					
	M	M		M	M	M		M	M		
Residual Risk:	Medium	Medium	Medium	Medium	Medium	Low	Medium	Low	Medium	Low	Medium

	M				M	M		M	M		
Residual Risk:	Medium	Medium	Medium	Medium	Medium	Low	Medium	Low	Medium	Low	Medium

Extremely effective: E
Highly effective: H
Moderately effective: M
Somewhat effective: S

E. Appendix E – Cost models

5.12.9 Cyber Uplift estimate - Option 1 (Basic Controls).xslm

5.12.9 Cyber Uplift estimate - Option 2 Preferred (Risk-based).xslm

5.12.9 Cyber Uplift estimate - Option 3 (Compliance).xslm

F. Appendix F – Opex step-changes (Preferred option)

Category	Application function	2025–26	2026–27	2027–28	2028–29	2029–30	Total 2025–30
Step change: Regulatory obligation	Cyber security capability development (non-recurrent opex)	2.6	6.9	7.2	5.8	3.8	26.2
	Cyber security capability maintenance (recurrent opex)	1.5	2.7	2.9	3.5	5.4	15.9
	Total opex step-change in period	4.1	9.6	10.0	9.2	9.2	42.1

Accounting treatment change

Topic	Detail
Background	Costs to continue to meet the risks associated with the significant increase in cyber security threats. Similar to cyber security recurrent costs, the majority of these activities are of an operational nature and hence are majority opex.
Request	An opex step change of \$42.1 million to account for the maintenance of cyber security capabilities moving forward.