



30 November 2023

Ausgrid's 2024-29 Revised Proposal

Attachment 5.9.2 – Cyber Security Program

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



Summary of how we have responded to the Draft Decision

The Australian Energy Regulator (AER) raised concerns with the quantum of cyber security expenditure proposed and the risk analyses being overstated, noting “there is not a regulatory requirement to fully implement Security Profile 3 (SP-3)” and would consider a compromise between SP-2 and SP-3 levels of risk more appropriate. Ausgrid continues to consider SP-3 an appropriate maturity target based on our criticality. Ausgrid is independently assessed as high criticality under the Australian Energy Sector Cyber Security Framework (AESCSF), which recommends a maturity target of SP-3 for high criticality market participants.

Notwithstanding the above, in addressing the AER concerns the Revised Regulatory Proposal reflects reduced expenditure of \$70 million (from \$91 million) and a corresponding reduction of ongoing operational expenditure to \$18 million (from \$21 million). These reductions are achieved by a re-prioritisation of the cyber risk program and by applying new knowledge from recently completed and in-flight programs.

How this investment meets the NEO, and the objectives and criteria within the NER

Continued efficient investment in, and use of electricity services requires Ausgrid to expand and extend the deployment and use of modern communicating, monitoring and control devices and utilise increasingly sophisticated data sharing platforms with field operatives and customers. Effectively leveraging these technologies and evolving the network and our operations in this way is in the long-term interest of consumers with respect to price, quality, safety, reliability security of supply and reducing Australian’s greenhouse gas emissions.

However, doing so increases the risk posed by cyber threats, presenting more opportunities for data to be intercepted or systems interfered with in such a way that threatens the safety, reliability, and security of the distribution system and the provision of standard control services.

At the same time, the sophistication and frequency of cyber-attacks is increasing. Ausgrid’s proposed cyber program and forecast represents the efficient and prudent investment required to cost effectively meet our statutory obligations and maintain the reliability and security of the distribution system, in the context of an evolving and increasing threat landscape.

Ausgrid has used independent assessments against established national frameworks to determine the appropriate cyber maturity target based on our criticality, demonstrating that the forecast represents costs that a prudent operator would require to achieve the capital expenditure objectives.

Ausgrid undertakes competitive market procurement to ensure all major investments within the cyber program are efficient and have based the forecast on detailed cost build ups based on historical costs, knowledge of recent market procurement for equivalent capability and services, demonstrating that the forecasts are both realistic and efficient.

Overview	Project summary		
Cyber Security Program Brief	Ausgrid’s proposed Cyber Security expenditure protects our organisation against cyber-attacks by implementing industry best practice safeguards in line with SP-3 of the AESCSF.		
FY25-29 \$m, real FY24	Initial Proposal	Draft Decision	Revised Proposal
Capex	\$44.4m	\$25.0m	\$34.8m
Implementation opex	\$46.7m	\$27.0m	\$35.4m

<p>Total</p>	<p>\$91.1m</p>	<p>\$52.0m</p>	<p>\$70.2m</p>
<p>Trend analysis</p>		<p>Why our Revised Proposal meets the needs of customers</p>	
<p>Our revised proposal is:</p> <ul style="list-style-type: none"> • 35% more than the Draft Decision • 23% less than our Initial Proposal 	<p>Our Revised Proposal of \$70 million is less than our Initial Proposal (\$91 million).</p> <p>Working within a reduced funding envelope, we remain committed to implementing the highest level of cyber security protections (SP-3) given the criticality of our network. To achieve this, we will need to unlock efficiency savings.</p>		
<p>AER draft decision</p>		<p>How we have responded</p>	
<p>The cost of the cyber security program is not reasonable based on AER benchmarking analysis</p>	<p>The AER raised concerns with the quantum of cyber security expenditure proposed, \$91 million, and provided a draft decision of \$52 million. Based on a review of the FY25-29 Cyber Security Program, the Revised Regulatory Proposal reflects a reduced expenditure forecast of \$70 million to continue to target SP-3.</p> <p>This reduction was achieved by re-evaluating the proposed cyber expenditure to achieve SP-3 and took into account:</p> <ul style="list-style-type: none"> • delivery of the FY23 and FY24 program to date; • the annual review of the strategic plan; <p>Cost efficiencies were partly offset by:</p> <ul style="list-style-type: none"> • the introduction of version 2 of the AESCSF; and • the competitive labour market for in-demand skillsets driving increased costs. <p>Ausgrid’s proposed operational expenditure step change of \$21 million was reduced by the AER to \$18 million in the draft allocation. This has been accepted by Ausgrid due to a corresponding lower ongoing operational expenditure forecast associated with the reduction of the capital program.</p>		
<p>The quantification of the consequences of some of the events appears to be excessive</p>	<p>Sensitivity analysis supporting the initial proposal has been reviewed and updated after receiving technical analysis feedback from the AER. The AER’s technical analysis mis-interpreted consequences within the cost benefit analysis (CBA) modelling were related to each other and therefore inherited the same likelihood values.</p> <p>Further, new benefits were incorporated into the sensitivity analysis resulting from recent privacy legislation changes that include penalties increasing to \$50 million from \$0.4 million.</p>		
<p>There is not a regulatory requirement to fully implement SP-3 and a risk-prioritised approach is considered more appropriate</p>	<p>The AER raised concerns with the quantum of cyber security expenditure proposed and the risk analyses being overstated, noting “there is not a regulatory requirement to fully implement SP-3” and would consider a compromise between SP-2 and SP-3 levels of risk more appropriate.</p> <p>Ausgrid continues to consider SP-3 an appropriate maturity target based on our criticality. Ausgrid is independently assessed as</p>		

	<p>high criticality under the AESCSF, which recommends a maturity target of SP-3 for high criticality market participants.</p>
--	---

Table of Contents

1.	Document governance	6
1.1.	Purpose of this document	6
	Related documents	6
	Document history	6
	Approval(s).....	6
2.	Executive summary	7
3.	CONTEXT	10
3.1.	Background	10
3.2.	Problem/opportunity	10
3.3.	Compliance obligations	12
3.4.	Risk appetite	16
3.5.	Cyber Security Strategy	17
3.5.1.	Inclusion of Version 2 of AESCSF – Revised Proposal	18
3.6.	Investment objectives.....	19
3.7.	Customer outcomes	19
4.	OPTIONS	21
4.1.	Overview of options.....	21
4.2.	Option 1: Maintain Cyber Security Maturity Level	22
4.2.1.	Option 1 costs	22
4.2.2.	NPV analysis.....	24
4.3.	Option 2: Enhanced Cyber Security Maturity Level	24
4.3.1.	Option 2 costs	24
4.3.2.	NPV analysis.....	25
4.4.	Option 3: Highest Cyber Security Maturity level (Preferred)	28
4.4.1.	Option 3 costs	28
4.4.2.	NPV analysis.....	29
4.5.	Costing.....	31
5.	RECOMMENDATION	32

5.1.	Recommended solution	32
5.2.	Program delivery risks.....	33
5.3.	Program assumptions	34
5.4.	Program dependencies	34
5.5.	Business area impacts	35
6.	GLOSSARY	36
7.	APPENDICES	38
	Appendix 1 Risk assessment – Option 1 (SP-1).....	38
	Appendix 2 Risk assessment – Option 2 (SP-2) – BASE CASE	42
	Appendix 3 Risk assessment – Option 3 (SP-3).....	45
	Appendix 4 Approach to quantification of project benefits	49
	Appendix 5 Summary – Ausgrid’s Cyber Security Strategy	51
	Appendix 6 Alignment of preferred option to NER	52

1. Document governance

1.1. Purpose of this document

The purpose of this document is to outline the program brief for the proposed cyber security program of work that will form part of our 2024-29 regulatory proposal.

Related documents

Document	Version	Author
2022-29 Technology Strategy	V1.0	Ryan Hewlett
2022-25 Cyber Security Strategy	V1.0	Hank Opdam
Attachment 5.9 – Technology Plan	V3.0	Matthew Erikson
Attachment 5.9.i – Cyber Security – CBA model	V1.0	Alison Gunn
Consolidated Cost Model	V19	Heidi Henderson

Document history

Date	Version	Comment	Person
11/02/2022	V1.01-7	Draft Review	Matthew Erikson
28/07/2022	V1.08	CIO Review	Ryan Hewlett
31/01/2023	V1.09	Final – Initial Proposal	Matthew Erikson
27/10/2023	V2.01	Draft – Revised Proposal	Matthew Erikson
15/11/2023	V2.02	CIO Review	Ryan Hewlett
30/11/2023	V2.03	Final – Revised Proposal	Alison Gunn

Approval(s)

Name	Position	Date
Ryan Hewlett	Chief Information Officer	17/11/2023
Junayd Hollis	Group Executive – Customer, Assets and Digital	30/11/2023

2. Executive summary

Cyber threats are becoming more frequent and sophisticated. Keeping our network safe from cyber intrusions is essential for safe, reliable energy services. A catastrophic cyber-attack on our network would have social, economic, health and even geopolitical ramifications for Australia.

In the worst possible scenario, a complete shutdown of our network (which includes the Sydney CBD) would have catastrophic implications for the community totalling as much as \$120 million per hour or \$2.9 billion over the course of a full day. For our customers, a cyber breach of this magnitude impacting our network, even for a few hours, would severely disrupt lives and livelihoods.

Ausgrid uses the Australian Energy Sector Cyber Security (AESCFS) framework and is rated as a “High” criticality service provider within the AESCSF. In the 2024-29 regulatory period we will seek to achieve best practice maturity Security Profile 3 (SP-3). In addition, under the Security of Critical Infrastructure Act (SLACI), [REDACTED] and therefore we consider SP-3 is the prudent maturity level for Ausgrid.

Implementing SP-3 enables Ausgrid to achieve a Medium (Possible x Moderate) target risk rating for four of seven key risks as opposed to Security Profile 2 (SP-2) that achieves a target risk rating of High (Likely x Major) by 2029 for all key risks

The value proposition for customers with SP-3 control maturity by 2029 is the most effective controls are implemented to protect data and provide continuity of critical services. As opposed to achieving SP-2, where Ausgrid is predicted to retain a larger quantum of residual risk and with less effective controls to reduce the likelihood and impact of cyber incidents occurring when compared to SP-3 control maturity.

An investment of \$70.2 million plus a step change in operational expenditure (opex) of \$18.1 million is required to achieve this level of cyber security maturity with net benefits of \$152.0 million based on our net present value (NPV) modelling. The investment comprises of \$34.8 million capital expenditure (capex) and \$35.4 million of operational expenditure (opex) of which \$47.5 million is non-recurrent and \$22.7 million is recurrent expenditure.

Executive summary	
Key Objective(s) of the program	The objective of the cyber security program for the 2024-29 regulatory control period is to achieve and maintain the highest level of cyber security maturity SP-3 across all cyber control domains within the AESCSF.
Customer benefits	<p>Investing in this level of cyber security, will enable consumers to securely choose from a range of smart technologies, dynamic tariffs, and services to maximise their use of renewable energy while keeping their bills lower. In turn, facilitating faster, lower cost decarbonisation, and lower bills for consumers with cyber security embedded at the core of the future energy system.</p> <p>The key customer benefits from our proposed program are:</p> <ul style="list-style-type: none"> Securely enables digitisation of the future ‘flexible’ energy system to achieve Net Zero emission reduction targets; Greater resilience of network and Information, Communications and Technology (ICT) and Operational Technology (OT) assets, reducing the risk of cyber security-related outages and breaches, consistent

Executive summary						
	<p>with the National Electricity Objective (NEO), which requires us to maintain the security of both the supply of electricity and the distribution network;</p> <ul style="list-style-type: none"> • Reduced risk of a cyber-attack compromising the physical safety of supply and restoration of power for our staff, customers, and the community; • Provide the cyber security capabilities to support our customers to choose and operate smart technologies to maximise their use of renewable energy and keeping their bills low; • Reduced risk of an unplanned outage of critical ICT systems impacting staff productivity and our ability to publish market data and communicate and interact effectively with our customers; and • Securely protect customer data in accordance with the requirements of the Privacy Act 1988, reducing the potential for sensitive customer information to be stolen or inappropriately accessed. <p>Also, by not prudently investing in cyber security capability throughout 2024-29, Customers become limited in their ability to securely uptake low carbon technologies to maximise their use of renewable energy. Bills will also be higher in the longer term caused by deferred investment of appropriate cyber security capability to enable and support the energy transition.</p>					
Compliance requirements	<ul style="list-style-type: none"> • Distribution Network Service Provider (DNSP) License Conditions – keeping our cyber security systems up to date, supported and secured is a key enabler to meet our license conditions; • Security of Critical Infrastructure Act 2018 (SOCI), Security Legislation Amendment (Critical Infrastructure) Act 2021 (SLACI) and Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP) – Keeping our cyber security systems up to date, supported and secured is a key enabler to comply with these Acts; • Privacy Act 1988, Information Privacy Act 2014 – Having up-to-date and supported infrastructure is a key enabler to appropriately securing information and reducing the risk of a data breach; • Electricity Supply Act 1995 (NSW) – Ensuring supporting cyber security systems and end user devices are highly available and secure enables our critical business services to meet obligations in this Act; and • National Electricity Law (NEL) and National Electricity Rules (NER) – Ensuring supporting cyber security systems are highly available and secure enables our critical business services to meet these rules. 					
NPV	\$152.1 million					
Program timings	Program duration	5 years				
	Program start year	2025	Q1 <input checked="" type="checkbox"/>	Q2 <input type="checkbox"/>	Q3 <input type="checkbox"/>	Q4 <input type="checkbox"/>

Executive summary							
Expenditure forecast	\$million	FY25	FY26	FY27	FY28	FY29	Total¹
	Capex	(7.4)	(6.7)	(8.0)	(6.5)	(6.3)	(34.8)
	Opex	(9.7)	(5.8)	(6.4)	(6.8)	(6.7)	(35.4)
	SCS²	(17.0)	(12.4)	(14.5)	(13.4)	(12.9)	(70.2)
	Ongoing new opex	(2.0)	(3.0)	(4.0)	(4.3)	(4.7)	(18.1)
Program type	ICT investment	<input checked="" type="checkbox"/> Yes				<input type="checkbox"/> No	
	Recurrent ICT	<input checked="" type="checkbox"/> Yes				<input type="checkbox"/> No or n/a	
	Non-recurrent ICT	<input checked="" type="checkbox"/> Yes				<input type="checkbox"/> No or n/a	
	One-off SaaS opex	<input checked="" type="checkbox"/> Yes				<input type="checkbox"/> No or n/a	

Table 1 Executive summary

¹ Due to rounding, some totals may not correspond with the sum of the separate figures.

² Cost allocation method (CAM) allocated standard control services (SCS) component.

3. CONTEXT

3.1. Background

This document outlines the case for an investment to achieve the highest maturity in cyber security (**SP-3**) under the AESCSF, including maintaining it as the framework evolves. NPV analysis demonstrates that the public benefits of this level of cyber maturity are highest for Ausgrid [REDACTED]

We are risk averse in the way that we aim to achieve best industry practice to prevent unauthorised access to our critical network control systems, critical infrastructure sites (such as the control rooms) and our critical applications (such as Metering) that could result in unauthorised control of the network or prolonged outages of critical applications so far as is reasonably practical.

3.2. Problem/opportunity

Electricity is an integral part of all modern economies, supporting a range of critical services including health care, the internet and transportation. The secure supply of electricity is thus of paramount importance. Digitisation is rapidly transforming the energy system, bringing many benefits for businesses and consumers. At the same time, increased connectivity and automation raises the risk of a cyber-attack. A successful attack could trigger the loss of control over devices and processes in the electricity systems, in turn causing physical damage and widespread service disruption. *Figure 1* – shows the potential attack pathways that could result in a successful attack.

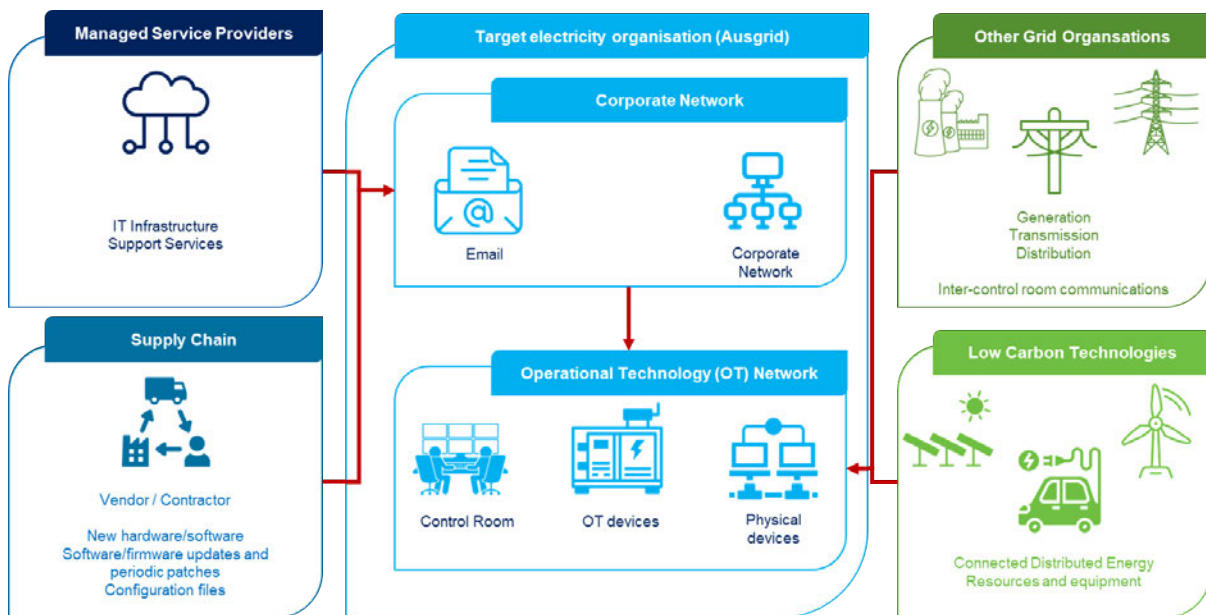


Figure 1 Potential attack pathways an attacker could compromise energy systems.

Cyber-attacks and espionage (illegally gaining access to confidential information) are significant threats to critical infrastructure in Australia due to the country’s geopolitical and economic position. Throughout 2022, cyber-attacks and espionage activity have been directed at the Australian Government, critical infrastructure, and financial services institutions alike. The Australian Cyber Security Centre (**ACSC**) states that approximately one quarter of reported cyber security incidents affected entities associated with Australia’s critical

infrastructure in 2021.³ Cyber-attacks are increasing in frequency, with a 13% increase in cyber-attacks reported by Australian entities to the ACSC in 2020-21.⁴

In March 2022, the ACSC notified Ausgrid that Australian organisations should adopt an enhanced cyber security posture and improve their resilience given the heightened threat environment. It noted that the attack on Ukraine has led to “a heightened cyber threat environment globally, and the risk of cyber-attacks on Australian networks, either directly or inadvertently, has increased”.⁵

Our business strategy to transform into a Distribution System Operator (**DSO**) will result in emerging challenges posed by connected devices, smart grids and Consumer Energy Resources (**CER**). Adopting innovative and secure technologies will be essential to realise the customer benefits presented by this opportunity.

Key drivers shaping cyber security planning in the energy sector include:

1. Increasing digitisation and automation of critical energy systems, increasing the risk of disruption through cyber-attacks;
2. International incidents related to critical infrastructure in the energy sector that have been attributed to cyber threat actors;
3. Increasing level of participation and intervention from Australian Government agencies in relation to cyber threats;
4. Increased usage of CER within the distribution network, introducing new methods of gaining unauthorised access to the electrical network;
5. Increasing ransomware attacks targeted to cause maximum harm to customers and communities;
6. Theft of sensitive data, as the volume of data collected and stored by organisations has increased significantly;
7. Developments in, and increasing adoption of emerging technologies such as robotics, artificial intelligence (**AI**), quantum computing and predictive intelligence; and
8. Increasing challenges in cyber-attack response planning due to the complexity, interconnectedness and interdependence of systems and cloud environments, and third-party hosts and support partners.

There are significant implications of a cyber-attack on Ausgrid and our customers. Our network is critical to the national economy as it services the Sydney CBD and other critical infrastructure businesses which account for 30% of Australia’s gross domestic product (**GDP**).⁶

Figure 2 – Our distribution area and community demonstrates the geography serviced by Ausgrid and indicates the number of consumers, businesses and organisations potentially impacted by a cyber-attack on our distribution network.

³ ACSC, *ACSC Annual Cyber Threat Report 2021*, 15 September 2021

⁴ ACSC, *ACSC Annual Cyber Threat Report 2021*, 15 September 2021

⁵ ACSC, *Australian organisations should urgently adopt an enhanced cybersecurity posture*, 28 March 2022.

⁶ NSW Government, *Sydney Facts*, <https://invest.nsw.gov.au/why-nsw/sydney-facts>, Accessed: 25 February 2022.

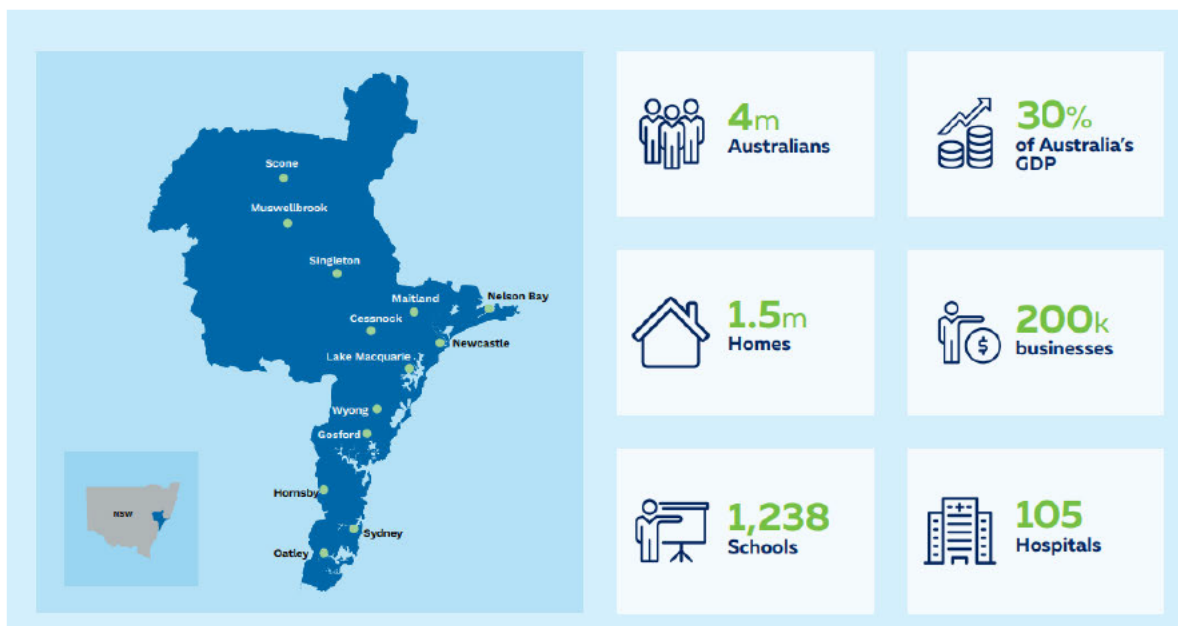


Figure 2 Our distribution area and community

Security controls need to be continually updated to ensure they accommodate new technology developments, threats, and vulnerabilities and to ensure they help us to meet our regulatory obligations. While we have a broad range of controls already implemented at a base level (i.e., implemented, supported, enabled, and configured), these need to be matured to ensure the control capabilities of these tools keep the cyber risk within our risk averse appetite.

3.3. Compliance obligations

We are required to meet the regulatory cyber security obligations as set out below.

Obligation	Description of Requirement
Security of Critical Infrastructure Act 2018 (SOCIA Act)	<p>The SOCIA Act was passed in 2018 and seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia’s critical infrastructure.</p> <p>The Act applies to 22 asset classes across 11 sectors including the energy sector and requires us to comply with the following obligations:</p> <ul style="list-style-type: none"> • Develop a Register of Critical Infrastructure Assets – the register builds a clearer picture of critical infrastructure ownership and control, and supports more proactive management of the risks these assets face; • Mandatory cyber incident reporting – entities for critical infrastructure assets may be required to report critical and other cyber security incidents to the Australian Cyber Security Centre’s online cyber incident reporting portal; • Government Assistance – if we experience a serious cyberattack and has not been able to respond effectively, the Government may provide assistance; • An information gathering power – the Secretary of the Department of Home affairs will have the power to obtain more

Obligation	Description of Requirement
	<p>detailed information from owners and operators of assets in certain circumstances to support the work of the centre; and</p> <ul style="list-style-type: none"> A Ministerial directions power – the Minister for Home Affairs will have the ability to direct an owner or operator of critical infrastructure to do, or not do, a specified thing to mitigate against a national security risk where all other mechanisms to mitigate the risk have been exhausted.

Obligation	Description of Requirement
<p>DNSP License Conditions</p>	<p>License conditions⁷ are imposed under the <i>Electricity Supply Act 1995 (NSW)</i>. The key license conditions relevant to our cyber security program are:</p> <ul style="list-style-type: none"> • Clause 9 requires us to use best industry practice for electricity network control systems to ensure that the distribution system, including all associated ICT infrastructure, can be accessed, operated, and controlled only from within Australia, and that it cannot be connected to any other infrastructure or network which could enable it to be controlled or operated by persons outside of Australia; and • Clause 10 requires us to ensure that information on Operational Technology (OT) and associated ICT infrastructure and personal information is held solely within Australia and accessible only by us (as the license holder) or someone authorised by Ausgrid. • Keeping our ICT systems and network secured against cyber threats is a key enabler to meet these licence conditions.
<p>Australian Energy Sector Cyber Security Framework (AESCSF)</p>	<p>Protecting Australia’s energy sector from cyber threats is of national importance. These protections maintain secure and reliable energy supplies thereby supporting our economic stability and national security. We are obligated to participate annually in an assessment within this framework.</p> <p>Ensuring that ICT infrastructure is kept up to date, supported and secured is a key enabler to meet our AESCSF maturity targets.</p>
<p>National Electricity Law and National Electricity Rules</p>	<p>The National electricity Law (NEL)⁸ requires us to promote efficient investment in, and efficient operation and use of electricity services for the long-term interests of consumers of electricity with respect to price, quality, safety, reliability, and security of supply of electricity as per the National Electricity Objective (NEO).</p> <p>The operating and capital expenditure objectives⁹ set out in the National Electricity Rules (NER) require us to maintain both the quality, reliability, and security of supply of standard control services and the reliability and security of the distribution network.</p>
<p>Privacy Act 1988, and Information Privacy Act 2014</p>	<p>As specified in the <i>Privacy Act 1988</i> and the <i>Information Privacy Act 2014</i>, we are required to maintain strong controls and security on the accessibility of customer data as well as appropriate availability of data.</p>

⁷ The Minister for Resources and Energy issues the DNSP licences. IPART administers compliance with the licence conditions on behalf of the Minister. Licence conditions for Ausgrid are available from IPART’s website: <https://www.ipart.nsw.gov.au/Home/Industries/Energy/Energy-Networks-Safety-Reliability-and-Compliance/Electricity-networks/Licence-conditions-and-regulatory-instruments#:~:text=Operating%20licences%20apply%20to%20Ausgrid%2C%20Endeavour%20Energy%2C%20Essential,to%20be%20read%20in%20conjunction%20with%20...%20>

⁸ The NEL is set out in a schedule to the *National Electricity (South Australia) Act 1996*.

⁹ See clauses 6.5.6(a) and 6.5.7(a) of the NER.

Obligation	Description of Requirement
	Having appropriate controls and cyber security systems in place is a key enabler to appropriately securing information and reducing the risk of a data breach.

Table 2 Summary of compliance obligations

The ongoing security and resilience of critical infrastructure is a shared responsibility of the Australian Government and the owners and operators of the critical assets.

We are required to comply with Commonwealth and State legislation for the protection of assets recognised as critical infrastructure.

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]



3.4. Risk appetite

We are risk averse in the way that we aim to achieve best industry practice to prevent a significant protective security incident so far as is reasonably practical. Refer to *Figure 5 – Ausgrid Risk statement, Risk Appetite and Risk Matrix below* and Appendices, which presents the risk assessment per option.

Risk Appetite Statement

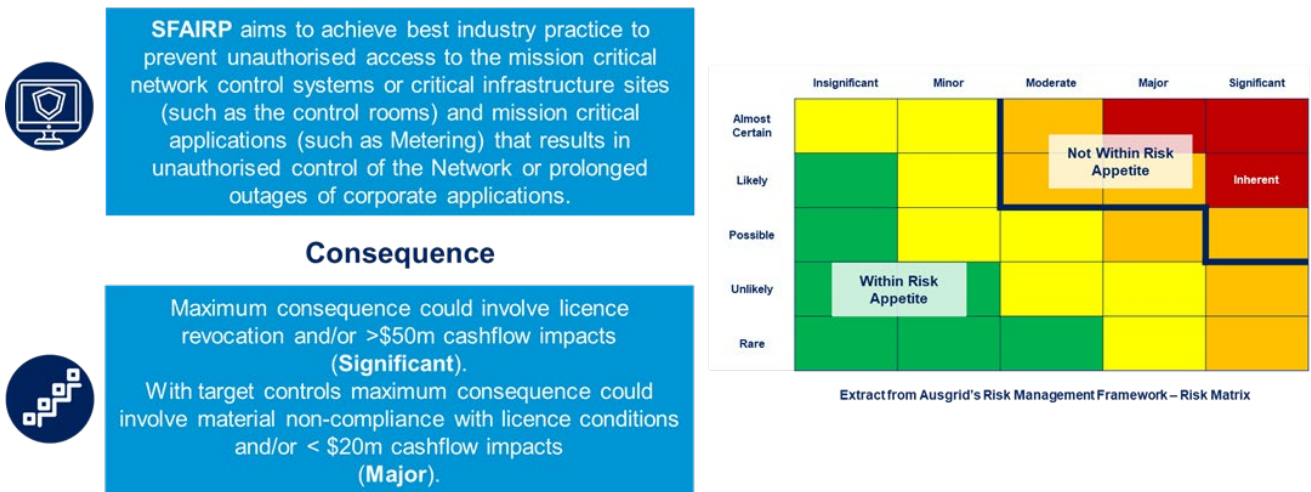


Figure 5 Ausgrid Risk statement, Risk Appetite and Risk Matrix

The proposed cyber security investment program reduces the risk profile of our key cyber risks so that the likelihood and consequence of each of those risks falls within our risk appetite. *Appendix 3 Risk assessment – Option 3 (SP-3)* summarises how achieving the highest level of cyber security maturity under the AESCSF (SP-3) will impact Ausgrid’s cyber risk profile.

Ausgrid assessed the current and predicted Cyber risk position across seven key risks and measured against three levels of control maturity (Security Profile 1 (SP-1) to SP-3)) to demonstrate the reduced likelihood and/or impact from proposed investment. Reducing the likelihood and/or impact of Cyber risk is directly proportionate to the three levels of control maturity (SP-1 to SP-3).

Maintaining a SP-1 control maturity was ruled out as a prudent approach to keep Cyber risk within appetite by 2029. Ausgrid’s chosen option to achieve SP-3 provides to most prudent and effective risk buy-down value for customers when compared against the base case of SP-2 by 2029.

Implementing SP-3 enables Ausgrid to achieve a Medium (Possible x Moderate) target risk rating for four of seven key risks as opposed to SP-2 that achieves a target risk rating of High (Likely x Major) by 2029 for all key risks.

The value proposition for customers with SP-3 control maturity by 2029 is four key risks reducing likelihood and impact and three key risks reducing likelihood, enables critical services to remain protected so far as is reasonably practicable as opposed to achieving SP-2 where a higher likelihood or impact from a Cyber incident is predicted. Unpatched vulnerabilities for critical services causing outages and data loss events impact customers the most. With SP-3 control maturity implemented, this means Ausgrid can implement the most effective controls available to minimise the likelihood and impact of these events occurring and if it does occur, impact from the event is limited.

On the contrary, SP-2 control maturity by 2029 offers customers a lower resilience to Cyber risks and all key risks are predicted to have a higher probability of occurring and increased consequence if the risks materialise due to a lower control effectiveness at managing Cyber risk as opposed to SP-3 control maturity. Key risks that may directly affect customers such as outages from unpatched vulnerabilities for critical services and data loss events are more likely to occur and Ausgrid's ability to effectively manage these risks is weaker in comparison to the effectiveness of SP-3 controls by 2029.

While a 'Possible x Major' Cyber risk position is 'Within Appetite' for Ausgrid in 2022, the residual risk of Ausgrid not achieving SP-3 by 2029 is not tolerable to the business if a Cyber incident occurs and SP-2 does not meet the Board endorsed risk averse risk appetite.

3.5. Cyber Security Strategy

The *Ausgrid Cyber Security Strategy 2022-25* sets out the vision and objectives for our cyber security function to support the delivery of the *Ausgrid Corporate Strategy 2022-35*, to meet our statutory and regulatory obligations and to remain within risk appetite for the risk of a significant protective security incident.

The *Ausgrid Cyber Security Strategy 2022-25* is aligned to the *Ausgrid Technology Strategy 2022-29* which aims to “*improve the delivery of the strategic responses through a flexible and secure technology portfolio, with cost effective and best fit solutions, automated to improve efficiency and with quality data to make better decisions*”.

We initially developed a cyber strategy in 2017 in response to changing ministerially imposed DNSP licence conditions that required minimum cyber security standards to be in place and the introduction of the SOCI Act in 2018. We supported this strategy with a dedicated three-year program to uplift our foundational cyber security services and technology.

The cyber strategy was further revised in 2022, driven by our need to continually enhance our cyber security defensive capability as well as in response to the increased obligations from the Australian Government as a result of SOCI legislation.

The *Ausgrid Cyber Security Strategy 2022-25* aligns to the AESCSF¹⁰. The AESCSF prescribes the target maturity level for practices through the definition of three security profiles: SP-1, SP-2, and SP-3. These security profiles defined by the Australian Cyber Security Centre (ACSC) are a measure of the target state cyber security maturity which industry participants

¹⁰ The AESCSF is based on the NIST CSF, with additional elements relevant to the Australian energy sector. The AESCSF lists 282 cyber security practices under 11 functional domains. The extent of achievement of these practices determines a company's security profile level under the framework. There are 88 practices relating to SP1, a further 112 practices relating to SP2 and a further 82 practices relating to SP3, for a total of 282 practices.

should aim to achieve and maintain. DNSP’s such as Ausgrid are identified as “High” criticality service providers within the AESCSF. Refer to Figure 6 – *AEMO Electricity Criticality Assessment Tool (E-CAT) criteria* below with updated practices for Version 2.

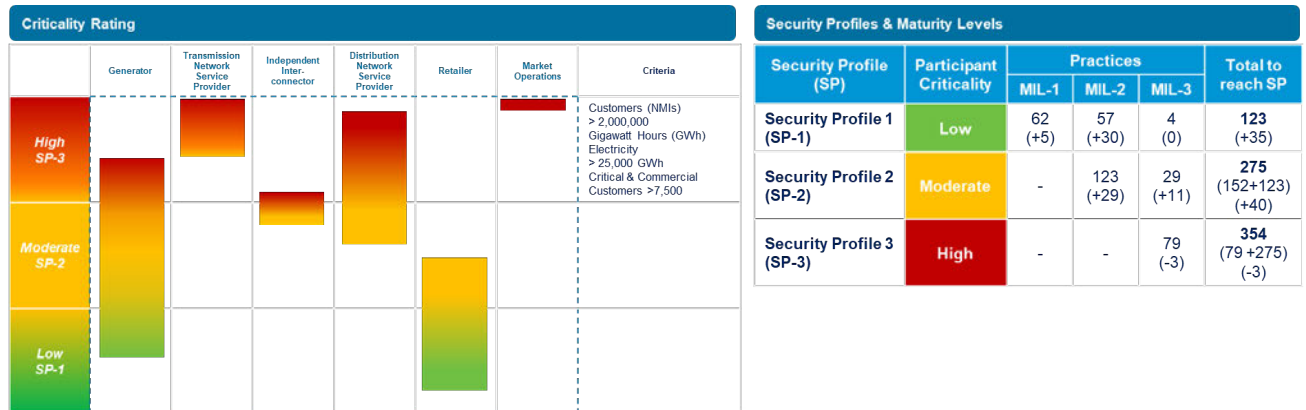


Figure 6 Ausgrid’s interpretation of AEMO Electricity Criticality Assessment criteria (practice numbers updated for AESCF version 2 underneath the original practice totals)¹¹

The E-CAT measures service providers based upon the following attributes:

- Number of Customers (Network Meter Identifiers) Ausgrid supplies electricity to;
- Number of Gigawatt Hours (**GWh**) of electricity transported;
- Number of Critical and Commercial Customers served by Ausgrid; and
- Regions where the provider provides these services.

Based on this, Ausgrid’s criticality is rated as “High”. This rating has been re-affirmed independently.

The *Ausgrid Cyber Security Strategy 2022-25* recognises that our cyber capabilities need to be supported by a range of key enablers to meet the requirements of the AESCSF. These enablers are:

- Strategic organisational engagement;
- Portfolio, strategy, and architecture;
- Skilled cyber security workforce;
- Strategic vendor / supplier partnerships; and
- Cyber security governance risk and compliance.

The *Ausgrid Cyber Security Strategy 2022-25* delivers a set of key outcomes that incrementally increase our cyber security posture and builds capability towards the future state cyber security environment. The initiatives over FY22 to FY24 focus on uplift and enhancements to our cyber security people, processes and technology that will establish and embed baseline capabilities, setting the foundation for achieving SP3 over the 2024-29 regulatory control period.

3.5.1. Inclusion of Version 2 of AESCSF – Revised Proposal

Version 2 of the AESCSF was released by the AER in October 2023. Security Profile 1 increased the volume of practices by 15% with a total practice change of 53%. In addition, SP-2 increased practice numbers by 15% with a total practice change of 58%. Ausgrid has been

¹¹ AEMO, AESCSF Electricity Criticality Assessment Tool (E-CAT), 2022 refresh.

independently assessed against the revised SP-1 practices independently and is now at 94% practice completion as of November 2023.

Refer to **Figure 6 – AEMO Electricity Criticality Assessment Criteria** for updated practices.

3.6. Investment objectives


By investing appropriately, we will enhance our current cyber security controls to prevent and/or detect malicious or unintentional security incidents including ransomware, phishing attacks, insider threats and the exfiltration of sensitive data.

Under the proposed program of work for the 2024-29 regulatory control period, we are aiming to deliver safe, reliant, and secure network services by prudently and efficiently:

- Mitigating assessed, known, emerging and future cyber security risks;
- Countering the increasing cyber threat, we face from multiple threat actors;
- Maintaining control design and effectiveness of implemented cyber security controls;
- Implementing new cyber security controls to mitigate known, unknown risks in the corporate and OT environments; and
- Providing our customers, the assurance that we can identify, detect, protect, and respond to increasing cyber security threats.

3.7. Customer outcomes

Our Corporate Strategy 2022-35 has identified four key themes that will define our business into the future. The cyber security program aligns to the thriving communities, valued people, optimised assets & operations and delivering net zero. Beneath the table, we demonstrate how these themes link to Cyber Security.

Objectives	Actions	Measures
<p>Thriving Communities</p> <p><i>Listen and understand to exceed customer expectations</i></p> 	<ul style="list-style-type: none"> • Support our customers to build resilient communities with a safe and reliable network • Strive to resolve customer issues quickly and meet changing expectations • Support customer choice by providing options and information • Continue to build trust and collaborate with our stakeholders 	<ul style="list-style-type: none"> • Customer confidence score • Partner confidence score • Service ease score • Service resolution score




Objectives	Actions	Measures
<p>Valued People</p> <p><i>Put our people at the heart to make Ausgrid a great place to work</i></p> 	<ul style="list-style-type: none"> • Harness our knowledge and resources to work safely and efficiently • Be inclusive, capable, and informed with our diverse, trusted workforce • Enable our people to work smarter by simplifying processes and systems • Collaborate and support each other 	<ul style="list-style-type: none"> • Zero fatalities • Total Recordable Injury Frequency Rate (TRIFR) • Employee engagement • Female people leaders
<p>Optimised Assets & Operations</p> <p><i>Excel at operations to deliver safe and affordable services</i></p> 	<ul style="list-style-type: none"> • Improve operational efficiency • Lift our digital and data capabilities to make fast, evidence-based decisions • Enhance effectiveness of internal services • Grow revenue by leasing our assets 	<ul style="list-style-type: none"> • Standard Control Services (SCS) opex • Delivery of network CAPEX program
<p>Delivering Net Zero</p> <p><i>Innovate and grow our business to support a net zero future</i></p> 	<ul style="list-style-type: none"> • Demonstrate leadership and facilitate an equitable and affordable transition to net zero • Enable flexibility and support a resilient and secure energy system • Embrace the energy transition to create revenue opportunities • Reduce Ausgrid’s carbon footprint 	<ul style="list-style-type: none"> • Unregulated Earnings before Interest, Tax, Depreciation and Amortization (EBITDA). • Carbon equivalent emissions

Table 3 Summary of customer outcomes

The proposed investment in cyber security capability and controls over the 2024-29 regulatory control period will deliver significant benefits to customers. The key customer benefits from the proposed cyber program are:

- Securely enables digitisation of the future ‘flexible’ energy system to achieve Net Zero emission reduction targets;
- Greater resilience of network and ICT assets, reducing the risk of cyber security-related outages and breaches, consistent with the National Electricity Objective (**NEO**), which requires us to maintain the security of both the supply of electricity and the distribution network;
- Reduced risk of a cyber-attack compromising the physical safety of supply and restoration of power for our staff, customers, and the community;

- Provide the cyber security capabilities to support our customers to choose and operate smart technologies to maximise their use of renewable energy and keeping their bills low;
- Reduced risk of an unplanned outage of critical ICT systems impacting staff productivity and our ability to publish market data and communicate and interact effectively with our customers; and
- Securely protect customer data in accordance with the requirements of the Privacy Act 1988, reducing the potential for sensitive customer information to be stolen or inappropriately accessed.

4. OPTIONS

This section provides an overview of the options which could credibly address the need to uplift and modernise our cyber capabilities. The NPV associated with each option is also noted.

4.1. Overview of options

Three options have been considered, which are listed in the table below. The recommended option for the 2024-29 regulatory control period is Option 3 as it achieves the highest cyber security maturity level to prevent and/or detect malicious or unintentional cyber security incidents. This will also provide cyber capabilities to enable future technologies, such as CER, and to protect against unknown or evolving threats.

Option	Description	NPV
Option 1: Current Minimum Compliance – Maintain cyber security maturity level \$23.7 million (totex)	Maintains Security Profile (SP-1) SP-1 is designed for low-criticality organisations and affects 88 practices within the AESCSF. No significant investments will be undertaken in our cyber security systems and practices in the 2024-29 regulatory control period, with investment deferral until the next period (2030-34). Specifically: <ul style="list-style-type: none"> • Does not extend AESCSF maturity beyond existing activities (i.e. maintain our SP-1 position and undertakes no further activities towards SP-2 and SP-3). 	(\$57.1 million)
Option 2: Base Case – Enhance cyber security maturity level \$73.2 million (totex)	Achieve and perform security practices at AESCSF (SP-2) SP-2 is designed for moderate-criticality organisations and includes 112 additional practices on top of the 88 practices from SP-1 within the AESCSF. We will further extend our cyber security maturity by expanding on the SP-1 level to achieve SP-2. SP-2 tradeoffs include: <ul style="list-style-type: none"> • Level of cyber practice maturity recommended for the criticality for a DNSP deemed high criticality (SP-3); • Highly integrated cyber controls, defence in depth and best in class protection; 	\$23.0 million

	<ul style="list-style-type: none"> • Constrained ability to enable future technologies i.e., CER; and • Constrained ability to protect against unknown or evolving cyber vulnerabilities and threats. 	
<p>Option 3: Target State – Highest cyber security maturity level (Preferred) \$88.3 million (totex) – (including opex step change of \$18.1 million)</p>	<p>Active management of cyber risk expands on SP-2 and enables us to achieve AESCSF (SP-3)</p> <p>SP-3 is designed for high-criticality organisations and includes 82 additional practices on top of the 200 practices from SP-2 within the AESCSF. This equates to the highest level of cyber security management.</p> <p>In response to [REDACTED] the deteriorating geopolitical threat landscape that is increasingly targeting our distribution network and systems., will require a significant investment uplift to achieve and maintain security practices at SP-3.</p> <p>SP-3 enables Ausgrid to realise an estimated \$118 million of avoided costs attributed through risk reduction in contrast to SP-2 (Option 2).</p>	<p>\$152.0 million</p>

Table 4 Overview of options

The principal difference between the three levels of maturity is that each level provides progressively greater maturity and mitigation against potential cyber incidents. We did not consider a “do nothing” case (i.e., nil investment) as the cyber threats are dynamic.

Maintaining current minimum compliance and maturity level SP-1 comes at considerable risk. Failure to maintain current functionality and a minimum capability to adequately address cyber security risks would result in an unacceptable level of risk to our network operations, staff, customers, and the community more broadly.

This would not be prudent as it would fail to maintain the security of both the distribution network and network services. Details of each capability level are provided below.

4.2. Option 1: Maintain Cyber Security Maturity Level

Option 1 maintains security practices at current minimum compliance (SP-1) of the AESCSF maturity without any further investment to move beyond SP-1. [REDACTED]

[REDACTED] SP-1 is not adequate based upon our interdependencies with other critical infrastructure assets and the consequences that would arise for Australia’s social or economic stability, defence, or national security if a hazard were to cause the asset a significant relevant impact.

4.2.1. Option 1 costs

The estimated capital cost of Option 1 is \$8.3 million, of which \$1.0 million is non-recurrent expenditure. There is also operating expenditure of \$7.9 million, of which \$4.8 million is non-recurrent expenditure, over the 2024-29 regulatory control period. This option will result in an uplift of ongoing operational expenditure of \$7.5 million over five years. Further information on the costs of Option 1 is provided in the following tables.

\$ million	FY25	FY26	FY27	FY28	FY29	Total
Direct Labour	(0.4)	(1.3)	(1.7)	(0.5)	(0.2)	(4.2)
Materials	(0.1)	(0.3)	(1.0)	(0.2)	(0.1)	(1.5)
Contractor services	(0.3)	(0.8)	(1.0)	(0.3)	(0.1)	(2.6)
Indirect cost	-	-	-	-	-	-
Other	-	-	-	-	-	-
Contingency	-	-	-	-	-	-
TOTAL CAPEX	(0.8)	(2.4)	(3.7)	(1.0)	(0.4)	(8.3)
Non-recurrent	(0.4)	(0.2)	-	-	(0.4)	(1.0)
Recurrent	(0.4)	(2.2)	(3.7)	(1.0)	-	(7.3)

Table 5 Summary of capital costs

\$ million	FY25	FY26	FY27	FY28	FY29	Total
Direct Labour	(0.9)	(0.6)	(0.8)	(1.2)	(0.6)	(4.2)
Materials	(0.2)	-	(0.2)	(0.3)	(0.2)	(0.9)
Contractor Services	(0.7)	(0.4)	(0.5)	(0.8)	(0.5)	(2.9)
TOTAL INVESTMENT OPEX	(1.8)	(1.0)	(1.6)	(2.2)	(1.2)	(7.9)
Non-recurrent	(1.2)	(1.0)	(0.8)	(0.8)	(1.2)	(4.8)
Recurrent	(0.7)	-	(0.8)	(1.5)	(0.1)	(3.0)
Ongoing new opex	(1.1)	(1.4)	(1.5)	(1.7)	(1.9)	(7.5)

Table 6 Summary of operating costs

4.2.2. NPV analysis

The NPV of Option 1 is driven primarily by the costs incurred. Being a maintenance only option, we do not forecast any reduction in the cyber risk profile. That is, the proposed investment under Option 1 maintains the current risk profile, provided no change in the likelihood or consequence of the cyber risks.

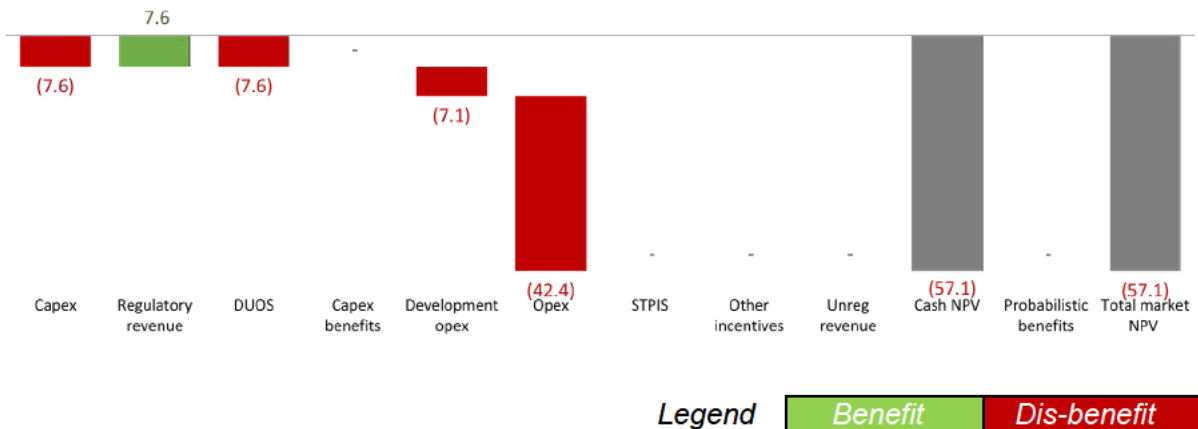


Figure 6 Option 1 – Market NPV (\$' millions, real FY24)

The NPV of Option 1 is (\$57.1) million. As there are no changes in the risk profile under Option 1, there are no quantified benefits. The key benefit of Option 1 is the avoidance of a deterioration in the cyber risk profile, provided there is no change in the threat environment.

4.3. Option 2: Enhanced Cyber Security Maturity Level

Option 2: Base Case – Enhanced Cyber Security Maturity Level moves beyond security practices at SP-1 of the AESCSF maturity and achieves SP-2. SP-2 is designed for moderate-criticality organisations and includes 112 additional practices on top of the 88 practices from SP-1 within the AESCSF.

Ausgrid considered SP-2 as a viable target state for Cyber Security capability. While SP-2 is an appropriate level of Cyber Security capability that is commensurate to Ausgrid’s risk appetite and the level of Cyber threat exposed to Ausgrid, this option was not preferred due to expected material residual risk and the level of cyber threat exposed to Ausgrid by 2029.

SP-2 is an appropriate target state by 2024, however the material risks exposed to Ausgrid and the level of Cyber threat increases the likelihood of a Cyber incident occurring that will require SP-3 capability to counter anticipated cyber threats by 2029.

As a critical infrastructure asset [REDACTED] with a ‘High’ criticality classification per the AESCSF, Ausgrid require to achieve the highest maturity level target state of the AESCSF by the end of 2029.

4.3.1. Option 2 costs

The estimated capital cost of Option 2 is \$28.6 million, of which \$17.4 million is non-recurrent expenditure. There is also operating expenditure of \$27.3 million, of which \$21.7 million is non-recurrent, over the 2024-29 regulatory control period. This option will result in an uplift of ongoing operational expenditure of \$17.3 million over five years. Further information on the costs of Option 2 is provided in the following tables.

\$ million	FY25	FY26	FY27	FY28	FY29	Total
Direct Labour	(3.3)	(3.8)	(3.4)	(2.6)	(2.3)	(15.3)
Materials	(0.7)	(0.5)	(1.5)	(0.2)	(0.5)	(3.4)
Contractor services	(2.0)	(2.3)	(2.2)	(1.7)	(1.6)	(9.8)
Indirect cost	-	-	-	-	-	-
Other	-	-	-	-	-	-
Contingency	-	-	-	-	-	-
TOTAL CAPEX	(6.0)	(6.6)	(7.1)	(4.6)	(4.3)	(28.6)
Non-recurrent	(4.9)	(3.2)	(3.0)	(2.9)	(3.4)	(17.4)
Recurrent	(1.2)	(3.3)	(4.1)	(1.7)	(0.9)	(11.2)

Table 7 Summary of construction costs

\$ million	FY25	FY26	FY27	FY28	FY29	Total
Direct Labour	(4.2)	(2.6)	(2.7)	(2.9)	(2.8)	(15.2)
Materials	(1.2)	(0.3)	(0.3)	(0.5)	(0.2)	(2.4)
Contractor Services	(2.8)	(1.6)	(1.6)	(1.9)	(1.7)	(9.6)
TOTAL INVESTMENT OPEX	(8.2)	(4.5)	(4.7)	(5.2)	(4.8)	(27.3)
Non-recurrent	(7.0)	(3.4)	(3.5)	(3.3)	(4.5)	(21.7)
Recurrent	(1.2)	(1.1)	(1.2)	(1.9)	(0.2)	(5.5)
Ongoing new opex	(1.9)	(2.9)	(3.8)	(4.1)	(4.5)	(17.3)

Table 8 Summary of operating costs

4.3.2. NPV analysis

This NPV analysis is primarily driven by the benefits of avoided cyber security risks, specifically network and systems outages, lost staff productivity and unauthorised use of

personal and network data (see Appendices – Appendix 1 Risk Assessment for an analysis on these risks).

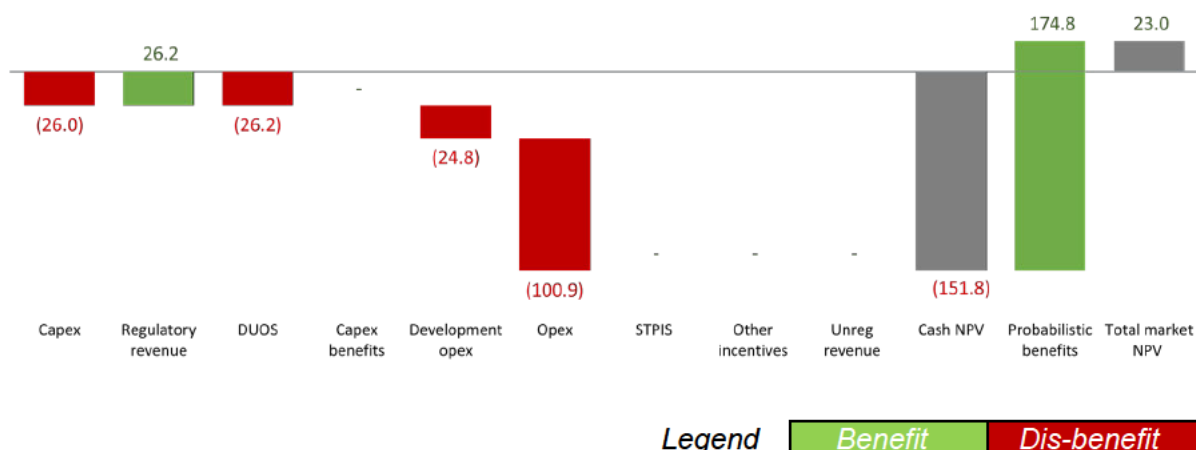


Figure 7 Option 2 – Market NPV (\$' millions, real FY24)

The key benefits of Option 2 relative to Option 1 are the reduction in the quantified risk of a successful cyber-attack, meaning a lower likelihood and / or consequence of the key risks, as set out in the following table.

Risk Scenario	Likelihood		Annual Benefit
	SP-1	SP-2	SP-1 vs SP2 \$ millions
Unauthorised access to, or use of, personal data Theft of personal information about employees and / or customers.	47%	31%	1.83
Increase length of unplanned outage Critical operational systems being compromised or rendered unavailable, potentially leading to increased length of unplanned network outages.	0.44%	0.30%	7.60
Delays to planned maintenance Critical operational systems being compromised or rendered unavailable, potentially leading to reduced staff productivity.	44%	30%	8.38
Delays in being able to publish key data to the market Critical operational systems being compromised or rendered unavailable, potentially leading to an inability to publish key data to the market in a timely fashion.	44%	30%	0.53

Risk Scenario	Likelihood		Annual Benefit
	SP-1	SP-2	SP-1 vs SP2 \$ millions
<p>Lost staff productivity due to reduced access to key corporate or operational systems</p> <p>Critical corporate systems being compromised, potentially impacting operational capacity, employee productivity and our ability to interact with our customers</p>	44%	30%	12.98
<p>Manual control of the grid</p> <p>Field workers required to take direct control of the grid via sub-stations in order to directly restore electricity, resulting in inconsistent ability to provide power and impacting Ausgrid productivity whilst restoration efforts take place.</p>	0.44%	0.30%	0.07

Table 9 Summary of likelihood of key risks

The value of these benefits has been quantified by estimating the changes in the expected consequence cost of the above cyber risks, relative to Option 1 (i.e., the reduction in the expected cost of the risk relative to Option 1 is the benefit attributable to the investment for Option 2). The expected cost has been estimated as the product of the likelihood of the risk (a percentage) and the consequence, i.e., the cost if the risk does eventuate (a dollar value). Further information on our approach to quantifying the risk benefits is provided in *Appendix 1 – Risk Assessments*.

Additional benefits that have not been quantified include:

- Theft of sensitive information about the distribution network, which would be a breach of our licence conditions;
- Employee or public safety being compromised;
- Flow on benefits to broader economy of avoided outages; and
- Avoided negative reputational impacts on Ausgrid resulting from customer personal information breaches and mandatory breach notifications.

We have not quantified the flow on benefits to the broader economy of avoided outages. However, as noted previously, our distribution area accounts for more than 30% of Australia’s GDP. This equates to around \$120 million per hour or \$2.9 billion per day.

4.4. Option 3: Highest Cyber Security Maturity level (Preferred)

Option 3: Target State – Highest Cyber Security maturity level expands on Option 2 and enables us to achieve SP-3. SP-3 is designed for high-criticality organisations and includes 82 additional practices on top of the 200 practices from SP-2 within the AESCSF.

SP-3 is the target maturity level for the 2024-29 period.

4.4.1. Option 3 costs

The estimated capital cost of Option is \$34.8 million, of which \$20.6 is non-recurrent expenditure. There is also operating expenditure of \$35.4 million, of which \$26.9 million is non-recurrent, over the 2024-29 regulatory control period. This option will result in an uplift of ongoing operational expenditure of \$18.1 million over five years, which is driven by the need for resources with specialist skills, further protection through new cyber software capability, and investing in evolving cyber awareness training programs for staff to protect themselves and the organisation from cyber-attacks. Further information on the costs of Option 3 is provided in the following tables.

\$ million	FY25	FY26	FY27	FY28	FY29	Total
Direct Labour	(4.1)	(3.8)	(3.9)	(3.7)	(3.4)	(18.9)
Materials	(0.8)	(0.5)	(1.6)	(0.4)	(0.6)	(3.9)
Contractor services	(2.4)	(2.3)	(2.5)	(2.4)	(2.3)	(12.0)
Indirect cost	-	-	-	-	-	-
Other	-	-	-	-	-	-
Contingency	-	-	-	-	-	-
TOTAL CAPEX	(7.4)	(6.7)	(8.0)	(6.5)	(6.3)	(34.8)
Non-recurrent	(5.6)	(3.3)	(3.1)	(4.0)	(4.5)	(20.6)
Recurrent	(1.7)	(3.3)	(4.9)	(2.5)	(1.8)	(14.2)

Table 10 Summary of construction costs

\$ million	FY25	FY26	FY27	FY28	FY29	Total
Direct Labour	(5.0)	(3.4)	(3.6)	(3.8)	(3.9)	(19.7)
Materials	(1.3)	(0.3)	(0.5)	(0.6)	(0.4)	(3.1)
Contractor Services	(3.3)	(2.1)	(2.3)	(2.5)	(2.4)	(12.5)

\$ million	FY25	FY26	FY27	FY28	FY29	Total
TOTAL INVESTMENT OPEX	(9.7)	(5.8)	(6.4)	(6.8)	(6.7)	(35.4)
Non-recurrent	(8.1)	(4.7)	(4.4)	(4.1)	(5.6)	(26.9)
Recurrent	(1.6)	(1.1)	(2.0)	(2.7)	(1.1)	(8.5)
Ongoing new opex	(2.0)	(3.0)	(4.0)	(4.3)	(4.7)	(18.1)

Table 11 Summary of operating costs

4.4.2. NPV analysis

This NPV analysis is primarily driven by the benefits of avoided cyber security risks, specifically outages, safety and theft of data (see Appendices – Appendix 1 Risk Assessment for an analysis on these risks). We have discussed these risks and our approach to quantify this avoided risk below.

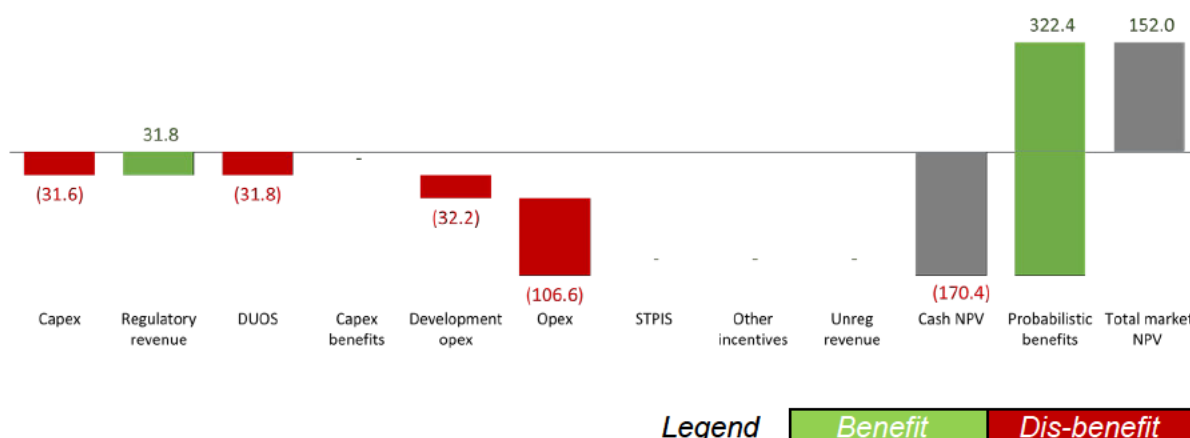


Figure 8 Option 3 – Market NPV (\$' millions, real FY24)

The key benefits of Option 3 relative to Option 1 and Option 2 are the further reduction in the risk of a successful cyber-attack, meaning an even lower probability and / or consequence of the key risk scenarios, as shown below:

Risk Scenario	Likelihood			Annual Benefit	
	SP-1	SP-2	SP-3	SP-1 vs SP-3 \$ millions	SP-2 vs SP-3 \$ millions
Unauthorised access to, or use of, personal data Theft of personal information about employees and / or customers.	47%	31%	8%	4.45	2.62

Risk Scenario	Likelihood			Annual Benefit	
	SP-1	SP-2	SP-3	SP-1 vs SP-3 \$ millions	SP-2 vs SP-3 \$ millions
<p>Increase length of unplanned outage</p> <p>Critical operational systems being compromised or rendered unavailable, potentially leading to increased length of unplanned network outages.</p>	0.44%	0.30%	0.06%	20.63	13.03
<p>Delays to planned maintenance</p> <p>Critical operational systems being compromised or rendered unavailable, potentially leading to reduced staff productivity.</p>	44%	30%	6%	13.59	5.22
<p>Delays in being able to publish key data to the market</p> <p>Critical operational systems being compromised or rendered unavailable, potentially leading to an inability to publish key data to the market in a timely fashion.</p>	44%	30%	6%	1.45	0.91
<p>Lost staff productivity due to reduced access to key corporate or operational systems</p> <p>Critical corporate systems being compromised, potentially impacting operational capacity, employee productivity and our ability to interact with our customers</p>	44%	30%	6%	17.84	4.86
<p>Manual control of the grid</p> <p>Field workers required to take direct control of the grid via sub-stations in order to directly restore electricity, resulting in inconsistent ability to provide power and impacting Ausgrid productivity whilst restoration efforts take place.</p>	0.44%	0.30%	0.06%	0.12	0.04

Table 12 Summary of key risks scenarios

As per Option 2, the value of these benefits has been quantified by estimating the changes in the expected cost of the above cyber risks, relative to Option 1 and Option 2.

Similarly, additional benefits that have not been quantified include:

- Theft of sensitive information about the distribution network;
- Employee or public safety being compromised;
- Flow on benefits to broader economy of avoided outages; and
- Avoided negative reputational impacts on Ausgrid resulting from customer personal information breaches and mandatory breach notifications.

We have not quantified the flow on benefits to the broader economy of avoided outages. However, as noted previously, our distribution area accounts for more than 30% of Australia's GDP. This equates to around \$120 million per hour and \$2.9 billion per day (noting that not all of this would be at risk).

4.5. Costing

The costs of each option have been estimated based on a cost build up for each individual project, based on typical delivery team resource requirements, delivery partner costs and licences.

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

5. RECOMMENDATION

5.1. Recommended solution

Option 3: Highest Cyber Security Maturity level SP-3 is the preferred option as it:

- Delivers the highest benefit - SP-3 \$152.0 million versus SP-2 \$23.0 million;
- Achieves the optimum maturity target state within AESCSF, [REDACTED];
- Is consistent with the NEO;
- Minimises implementation cost and risk;
- Maximises realisation of benefits and
- Aligns to our corporate strategy and risk appetite.

This option will uplift the cyber security controls covering our critical ICT and OT systems and our capability to manage the increasing cyber security threat, both in terms of number of attempted attacks and sophistication of those attacks.

The basis of this recommendations is that the proposed investments under **Option 3** will:

- Ensure that we can continue to deliver safe, reliable, and secure network services for the duration of the 2024-29 regulatory control period;
- Deliver appropriate controls and capabilities to mitigate against increasingly sophisticated cyber-attacks on both our ICT and OT systems, thereby maintaining the security of the distribution network;
- Ensure we meet our Licence Conditions and security obligations under the SOCI, SLACI, SLACIP Acts and the Privacy Act; and
- Deliver the greatest benefit to customers in terms of reduced risk of outages and data breaches.

5.2. Program delivery risks

The following table summarises the risks to the delivery of the proposed cyber risk program over the 2024-29 regulatory control period.

Risk #	Risk Category	Description	Inherent Risk Level	Mitigation Plan	Residual Risk level
01	Cyber Incident	A major cyber incident could occur during program delivery causing impacts to scope, schedule, and costs	Extreme	Maintain existing controls to reduce the impact of a cyber incident occurring and ensure incident responses are updated.	High
02	Scope Expansion	Requests for additional features or capabilities not captured in the originally scope, may extend the timeline of the project.	Medium	Set scope expectations early on and define boundaries.	Low
03	New Technology Support Skills	If new technology is being introduced as part of this program, there may be insufficient skills to support the new technology after the program of work has been completed.	Medium	Put plans in place to develop the required skillset is developed to enable technology to be supported in the future.	Low
04	Costs	Project Costs are estimated based upon market knowledge in FY22, and costs could increase as the project is executed in 2024-29 regulatory control period.	Medium	Develop a Gate 3 Business Case prior to executing the program and revise costs accordingly.	Low
05	ICT Infrastructure Program inter-dependency	Inter-dependencies with the ICT Infrastructure Program could cause impacts to schedule and costs of this program.	High	Ensure prioritization and planning processes adequately capture inter-dependencies and manage appropriately.	Medium

Table 15 overview of program delivery risks

5.3. Program assumptions

The following table summarises the key program-level assumptions underpinning this program brief.

#	Type	Description
01	Resourcing	Cyber security specialists and resources will be available as required during each stage of the project and for ongoing operations..
02	Prioritisation	The cyber program is considered a high priority project due to the nature of the risks and the potential consequences of a cyber-attack. Given the nature of the risks and the potential consequences of failures or disruptions to business operations, this program will be prioritised accordingly (see Appendices – Appendix 1 Risk Assessment for an analysis on these risks).
03	Scope	The scope identified is based on current control assessments and the Ausgrid technology plan. If the control environment changes the scope will need to be modified.
04	Supply Chain	Delayed delivery of equipment from suppliers is possible and contingency has been incorporated into project scheduling.

Table 16 Overview of program assumptions

5.4. Program dependencies

The following table summarises the key dependencies with other programs.

#	Program Name	Description
01	ICT Infrastructure Program	ICT Infrastructure initiatives may impact scheduling of Cyber Security initiatives throughout the program. Inability to deliver on the renewal and upgrades of ICT infrastructure within acceptable asset lifecycle periods may cause exposures to cyber security risks. This includes vulnerabilities within legacy and unsupported technologies, and this may have a direct impact on the goals and targets of the Cyber Security Program. This may require elevated cyber security monitoring and services to manage these risks.

Table 17 Overview of program dependencies

5.5. Business area impacts

The following table summarises the key business area impacts.

#	Impacted Group	Description
01	All Ausgrid	Where possible the program initiatives will be managed with go-lives that minimise the amount of (or any) disruption to business operations due to technology transition downtimes (e.g., planned out of hours etc.) Training on cyber awareness and extent of cyber campaigns.
02	All Ausgrid	Several SP-3 practices are going to impact all staff and contractors. These include introducing new policies and procedures and assigning roles and responsibilities.
03	ICT / Cyber team	The ICT/Cyber team will be involved in the successful delivery of the project and the ongoing maintenance.

Table 18 Overview of business area impacts

6. GLOSSARY

Shortened Form	Extended Form
ACSC	Australian Cyber Security Centre
AESCSF	Australian Energy Sector Cyber Security Framework
AI	Artificial Intelligence
Capex	Capital Expenditure
CER	Consumer Energy Resources
DNSP	Distribution Network Service Provider
DSO	Distribution System Operator
EBITDA	Earnings before Interest, Tax, Depreciation and Amortization
E-CAT	Electricity Critically Assessment Tool
FY25-29	Financial Year 2025 to Financial Year 2029
GDP	Gross Domestic Product
ICT	Information, Communications and Technology
NEL	National Electricity Law
NEO	National Electricity Objective
NER	National Electricity Rules
Opex	Operating Expenditure
OT	Operational Technology
SCS	Standard Control Services
SLACI	Security Legislation Amendment (Critical Infrastructure) Act 2021
SLACIP	Security Legislation Amendment (Critical Infrastructure Protection) Act 2022
SOC	Security Operation Centre
SOCI Act	Security of Critical Infrastructure Act 2018

Shortened Form	Extended Form
SP-1	Security Profile 1
SP-2	Security Profile 2
SP-3	Security Profile 3
TRIFR	Total Recordable Injury Frequency Rate

Table 19 Glossary of terms used throughout the document.

7. APPENDICES

Appendix 1 Risk assessment – Option 1 (SP-1)

Table 20 – Option 1 (SP1) – Key risks and residual position by 2029 summaries the inherent risks which could be experienced by the end of the coming regulatory control period of (2029).

Option 1 does not reduce the likelihood or impact of Group Risk 4.1 – Significant Protective Security Incident and below risk scenarios materialising. By 2029, Group Risk 4.1 – Significant Protective Security Incident will be **Not Within Appetite**.

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

Risk Description	Nature of Mitigation	Residual Risk 2029 – Not Within Appetite	
		Risk Rating	Likelihood x Consequence
<p>R1 – Ransomware attacks Compromise of critical ICT / OT services caused by a ransomware attack resulting in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	Extreme	Almost Certain x Significant
<p>R2 – Compromise via unpatched applications (Vulnerability Management) Unauthorised access to corporate / OT networks caused by physical and/or logical access control failures or limited control effectiveness may result in data loss, loss of control of relevant network and unplanned outages.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	Extreme	Almost Certain x Significant

<p>R3 – Data Loss</p> <p>Data exfiltration from organisation caused by data security control failure or limited control effectiveness to protect data that may result in potential revocation of network license and substantial fines and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	<p>Extreme</p>	<p>Almost Certain x Significant</p>
<p>R4 – Insider attack – intentional and unintentional</p> <p>Compromise of critical ICT / OT services caused by an insider attack may result in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	<p>Extreme</p>	<p>Almost Certain x Significant</p>
<p>R5 – External attack on Ausgrid assets/network</p> <p>Compromise of critical ICT / OT services caused by an external attack may result in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	<p>Extreme</p>	<p>Almost Certain x Significant</p>
<p>R6 – Supply chain/ vendor compromise</p> <p>Compromise of critical ICT / OT services caused by a supply chain attack may result in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	<p>Extreme</p>	<p>Almost Certain x Significant</p>

<p>and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>			
<p>R7 – Non-compliance to regulatory requirements Non-compliance to regulatory requirements and other legal obligations caused by a cyber incident resulting in potential revocation of network license, unplanned outages, substantial fines and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	<p>Extreme</p>	<p>Almost Certain x Significant</p>

Table 20 Option 1 (SP1) – Key risks and residual position by 2029

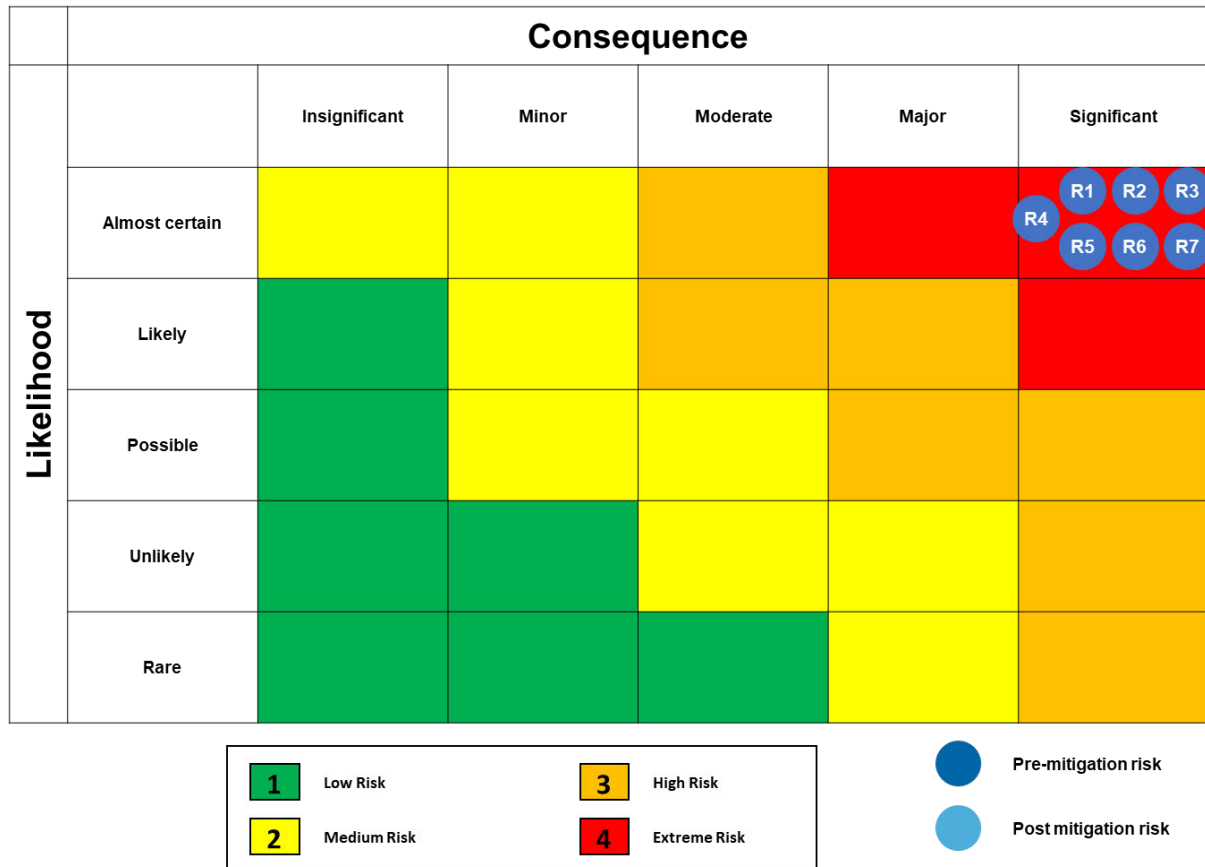


Figure 9 Change in risk position with Option 1 – (SP1) by 2029

Appendix 2 Risk assessment – Option 2 (SP-2) – BASE CASE

Table 21 – Option 2 (SP2) – Key risks and residual position by 2029 summaries the inherent risks which are reduced by the end of the coming regulatory control period of (2029) if option 2 is selected. This assessment has been undertaken in alignment with the Ausgrid Group’s Risk Management Framework.

Option 2 reduces the likelihood or impact of Group Risk 4.1 – Significant Protective Security Incident and below risk scenarios materialising. By 2029, Group Risk 4.1 – Significant Protective Security Incident will be **Not Within Appetite**.

Risk Description	Nature of Mitigation	Residual Risk 2029 – Not Within Appetite	
		Risk Rating	Likelihood x Consequence
<p>R1 – Ransomware attacks</p> <p>Compromise of critical ICT / OT services caused by a ransomware attack resulting in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	High	Likely x Major
<p>R2 – Compromise via unpatched applications (Vulnerability Management)</p> <p>Unauthorised access to corporate / OT networks caused by physical and/or logical access control failures or limited control effectiveness may result in data loss, loss of control of relevant network and unplanned outages.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	High	Likely x Major
<p>R3 – Data Loss</p> <p>Data exfiltration from organisation caused by data security control failure or limited control effectiveness to protect data that may result in potential revocation</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	High	Likely x Major

<p>of network license and substantial fines and delays to the safe supply and restoration of energy.</p>			
<p>R4 – Insider attack – intentional and unintentional Compromise of critical ICT / OT services caused by an insider attack may result in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	<p>High</p>	<p>Likely x Major</p>
<p>R5 – External attack on Ausgrid assets/network Compromise of critical ICT / OT services caused by an external attack may result in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	<p>High</p>	<p>Likely x Major</p>
<p>R6 – Supply chain/ vendor compromise Compromise of critical ICT / OT services caused by a supply chain attack may result in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	<p>High</p>	<p>Likely x Major</p>
<p>R7 – Non-compliance to regulatory requirements</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s</p>	<p>High</p>	<p>Likely x Major</p>

<p>Non-compliance to regulatory requirements and other legal obligations caused by a cyber incident resulting in potential revocation of network license, unplanned outages, substantial fines and delays to the safe supply and restoration of energy.</p>	<p>threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>		
---	---	--	--

Table 21 Option 2 (SP2) – Key risks and residual position by 2029

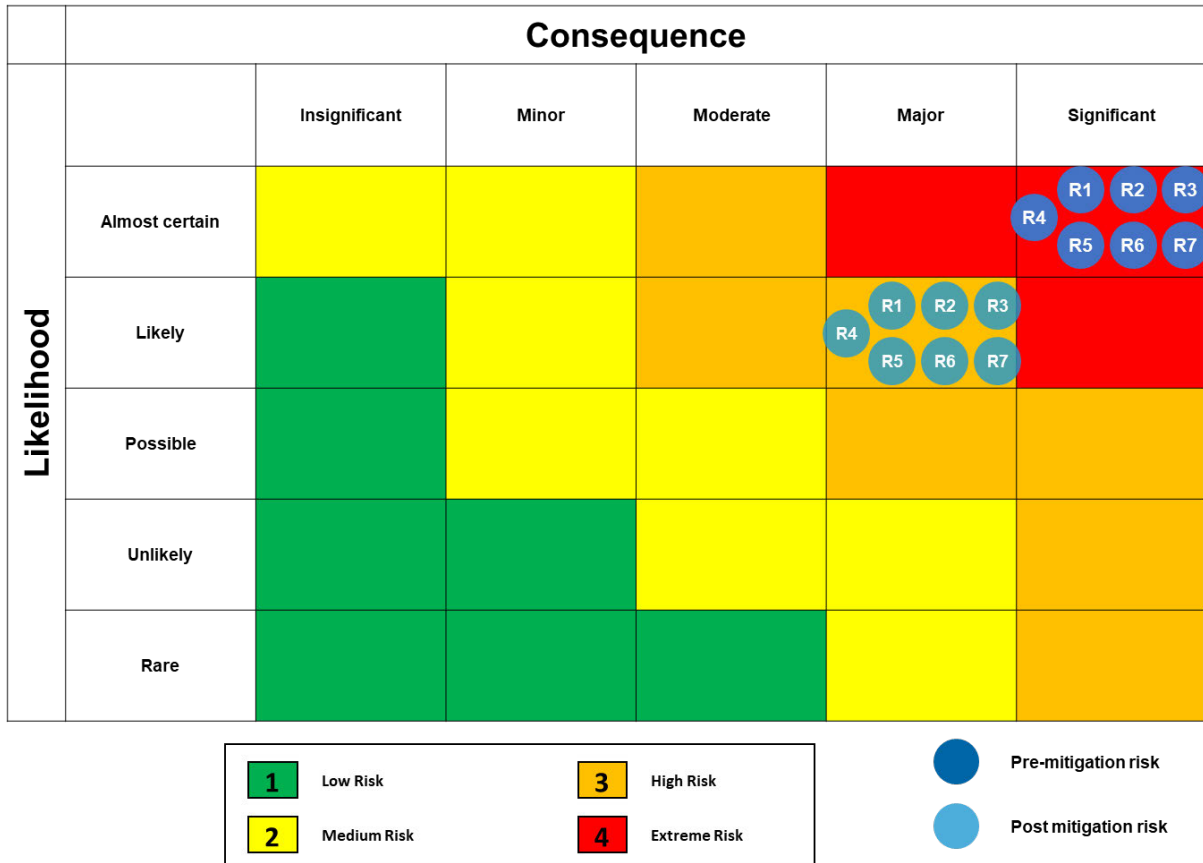


Figure 10 Change in risk position with Option 2 – (SP2 to SP3) by 2029

Appendix 3 Risk assessment – Option 3 (SP-3)

Table 22 – Option 3 (SP-3) – Key risks and residual position by 2029 summaries the inherent risks which are reduced by the end of the coming regulatory control period of (2029) if option 2 is selected. This assessment has been undertaken in alignment with the Ausgrid Group’s Risk Management Framework.

Option 3 reduces the likelihood or impact of Group Risk 4.1 – Significant Protective Security Incident and below risk scenarios materialising. By 2029, Group Risk 4.1 – Significant Protective Security Incident will be **Within Appetite**.

Risk Description	Nature of Mitigation	Residual Risk 2029 – Within Appetite	
		Risk Rating	Likelihood x Consequence
<p>R1 – Ransomware attacks Compromise of critical ICT / OT services caused by a ransomware attack resulting in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	High	Major x Possible
<p>R2 – Compromise via unpatched applications (Vulnerability Management) Unauthorised access to corporate / OT networks caused by physical and/or logical access control failures or limited control effectiveness may result in data loss, loss of control of relevant network and unplanned outages.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	Medium	Possible x Moderate

Risk Description	Nature of Mitigation	Residual Risk 2029 – Within Appetite	
		Risk Rating	Likelihood x Consequence
<p>R3 – Data Loss</p> <p>Data exfiltration from organisation caused by data security control failure or limited control effectiveness to protect data that may result in potential revocation of network license and substantial fines and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	High	Possible x Moderate
<p>R4 – Insider attack – intentional and unintentional</p> <p>Compromise of critical ICT / OT services caused by an insider attack may result in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	High	Possible x Moderate
<p>R5 – External attack on Ausgrid assets/network</p> <p>Compromise of critical ICT / OT services caused by an external attack may result in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	High	Possible x Major

Risk Description	Nature of Mitigation	Residual Risk 2029 – Within Appetite	
		Risk Rating	Likelihood x Consequence
<p>R6 – Supply chain/ vendor compromise</p> <p>Compromise of critical ICT / OT services caused by a supply chain attack may result in leakage/theft/manipulation of Personally Identifiable Information, Australian Electricity Market Data and/or Metering data, unplanned outages and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	High	Possible x Major
<p>R7 – Non-compliance to regulatory requirements</p> <p>Non-compliance to regulatory requirements and other legal obligations caused by a cyber incident resulting in potential revocation of network license, unplanned outages, substantial fines and delays to the safe supply and restoration of energy.</p>	<p>Maintaining current SP-1 control effectiveness will not keep pace with Ausgrid’s threat profile and SP-1 controls will not detect, prevent the sophistication of Cyber threat actors by 2029.</p>	Medium	Unlikely x Moderate

Table 22 Option 3 (SP3) – Key risks and residual position by 2029

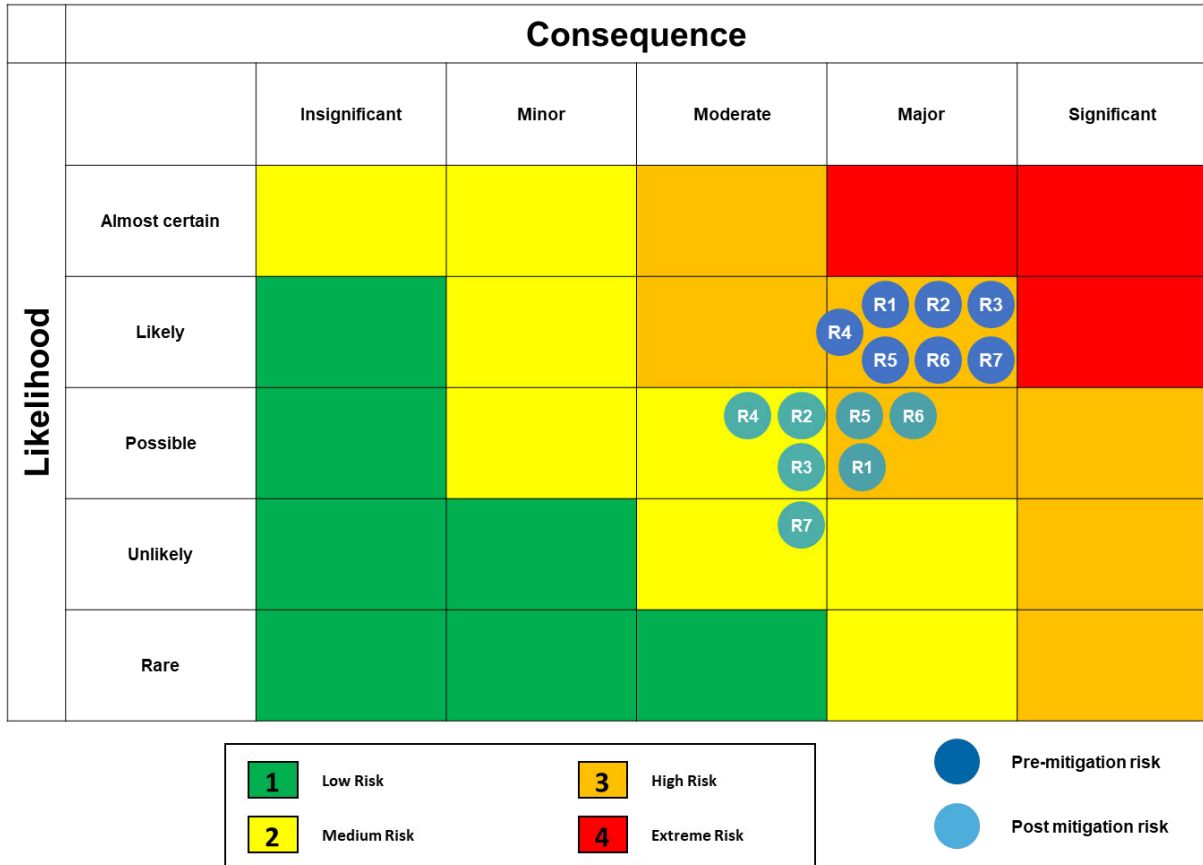


Figure 11 Change in risk position with Option 3 – (SP2 to SP3) by 2029

Appendix 4 Approach to quantification of project benefits

Ausgrid has identified four potential categories of benefits and has quantified these benefits wherever feasible and practicable.

The following table details the benefits categories and our approach to quantifying the value of each type of benefit. Benefits that cannot be readily quantified are described qualitatively.

Benefit category	Description	Quantification approaches
Operational benefits to Ausgrid and / or customers	Direct improvements in the operations and / or services supplied by Ausgrid because of an investment. These benefits are typically reflected in reduced costs (efficiencies), such as direct cost savings for Ausgrid in delivering SCS or time savings for customers.	<ul style="list-style-type: none"> • Cost savings are quantified through: <ul style="list-style-type: none"> – Cost build up (e.g., hours of labour saved <i>times</i> average cost of labour per hour); and / or – Benchmarks (e.g., typical % costs savings for similar projects or external benchmarks) • Customer time savings are quantified based on value of time saved (e.g., minutes saved <i>times</i> average wages (\$ / minute))
IT risk benefits	Changes in risks relating to IT systems and functionality because of an investment. For example, a reduction in the risk that an IT system will fail.	<ul style="list-style-type: none"> • Risk based benefits are quantified by estimating the change in the expected cost of the risk, where the expected cost of the risk is estimated as the likelihood of the risk (%) <i>times</i> the consequence of the risk (\$)
Enterprise risk benefits	Changes in risks relating to Ausgrid’s ability to perform tasks required by regulation or contract because of an investment. For example, a reduction in the risk that Ausgrid will not meet compliance obligations under the SOCI Act.	<ul style="list-style-type: none"> • For some risk-based benefits (for example safety) we will use a risk monetization framework which allocates a monetary cost to the associated risk level. • For example, assume a risk has a consequence of \$10 million and 10% chance (i.e., likelihood) of occurring without the project. With the project, the consequence does not change but the likelihood falls to 8%. <ul style="list-style-type: none"> – The quantified risk benefit is then the change in likelihood <i>times</i> consequence, which is (10% - 8%) x \$10m = \$200,000
Community risk benefits	Changes in risks to the community at large because of an investment. For example, a reduction in safety risks for the public.	<ul style="list-style-type: none"> • The consequence costs may comprise different elements, such as: <ul style="list-style-type: none"> – Loss of supply, which is measured using an estimate of the unserved energy and the value of customer reliability

		<p>(VCR) for Ausgrid’s distribution area</p> <ul style="list-style-type: none"> - Rectification costs, which are measured using an estimate of the resource effort required (e.g., hours times \$/hour for ICT resources).
--	--	---

Table 23 Approach to quantification of project benefits

Appendix 5 Summary – Ausgrid’s Cyber Security Strategy

The following table details how the preferred option aligns to Ausgrid’s 2022-25 Cyber Strategy and allows us to achieve a target state maturity of SP-3.

Cyber Security Goal	Outcomes and how this investment contributes
1. Achieve and Maintain SP-3 AESCSF maturity level	<ul style="list-style-type: none"> • Capability uplift to implement all 282 practices of SP-3 per the AESCSF with additional risk buy-down to further protect our systems from emerging cyber threats based upon our unique attributes (geographic location and customer quantities).
2. Drive the cyber risk for the business to within risk appetite	<ul style="list-style-type: none"> • Enhancing governance, risk management capabilities and attestation to capture, manage and report on cyber risks and issues. • Expansion of data security capabilities to identify, classify and protect operational, customer and personal data. • Alignment of architecture across Cyber Security and ICT & OT to ensure consistent direction and reusable security patterns. • Development and implementation of Cloud Security Governance with controls to manage compliance.
3. Trusted and connected organisational partner	<ul style="list-style-type: none"> • Resourcing the cyber security team to optimise existing controls and support the uplift in technologies and monitoring capabilities. • Delivering and measuring annual cyber plans which are aligned to core ICT and Business values and represented in team KPIs. • Developing and maintaining cyber driven focus groups in the business (e.g. Data Security Governance) to ensure business concerns and issues are being addressed
4. Evolve and enhance cyber defenses and resiliencies	<ul style="list-style-type: none"> • Developing, enhancing, and testing security response capabilities in line with the changing external threats. • Developing a cyber skill register to improve cyber staff capabilities. • Applying a security vulnerability management framework to all inhouse and vendor managed software, appliances, and platforms.
5. Enhancing and accelerating security uplift and performance	<ul style="list-style-type: none"> • Maturing access management capabilities to minimize inappropriate access. • Investing in security orchestration, automation, and response to increase detection of threats and attacks in real-time. • Enhancing Security Assurance capabilities to regularly test controls.

Table 24 Alignment summary of Ausgrid’s Cyber Security Strategy and SP-3.

Appendix 6 Alignment of preferred option to NER

The following table details how the preferred option aligns to the NER expenditure objectives.

NER requirement	How this investment aligns to the NER requirement
<p>6.5.7 (a)(2)</p> <p>The forecast capital expenditure complies with all applicable regulatory obligations or requirements associated with the provision of standard control services.</p>	<p>The proposed investment under Option 3 is designed to ensure that we meet our obligations under relevant regulatory instruments, including our license conditions, the SOCI Act and the Privacy Act.</p>
<p>6.5.7 (a)(3)(iv)</p> <p>The forecast capital expenditure maintains the reliability and security of the distribution system through the supply of standard control services.</p>	<p>The proposed investment under Option 3 provides the strongest controls to protect us from potential cyber-attacks, to ensure the availability and integrity of critical systems are maintained. This, in turn, ensures that we can continue to maintain the quality, reliability and security of supply of standard control services.</p>
<p>6.5.7 (a)(4)</p> <p>The forecast capital expenditure maintains the safety of the distribution system through the supply of standard control services.</p>	<p>Any cyber-attack that takes control of network assets presents a clear and immediate safety risk to both workers and the public, and our cyber program mitigates growth in this risk.</p>
<p>6.5.7 (c)(1) (i)</p> <p>The total of the forecast capital expenditure reasonably reflects the efficient costs of achieving the capital expenditure objectives.</p>	<p>A detailed cost build up has been prepared to estimate the capital and incremental operating costs for Option 3. This has been based on historical costs, knowledge of recent market procurement for equivalent capability and services, as well as specialist advice and internal subject matter expertise.</p> <p>We undertake competitive market procurement to ensure cost efficiencies in project deliverables.</p>
<p>6.5.7 (c)(1) (ii)</p> <p>The total of the forecast capital expenditure reasonably reflects the costs that a prudent operator would require to achieve the capital expenditure objectives.</p>	<p>The proposed investments have been selected to achieve SP-3 against the AESCSF as per Ausgrid's independent assessment and to meet our regulatory obligations, and maintain the cyber risk profile within Ausgrid's risk appetite. A more detailed internal business case will be prepared and subject to our internal governance procedure prior to any investment is undertaken.</p>
<p>6.5.7 (c)(1) (iii)</p> <p>The total of the forecast capital expenditure reasonably reflects a realistic expectation of the demand</p>	<p>A detailed cost build up has been prepared to estimate the capital and incremental operating costs for the preferred option. This has been based on historical costs, knowledge of recent market procurement for equivalent capability and</p>

NER requirement	How this investment aligns to the NER requirement
forecast and cost inputs required to achieve the capital expenditure objectives.	<p>services, as well as specialist advice and internal subject matter expertise.</p> <p>We undertake competitive market procurement to ensure cost efficiencies in project deliverables.</p>

Table 25 Alignment of preferred option to NER.