



31 January 2023

Attachment 5.8.d: Operational technology security program

Ausgrid's 2024-29 Regulatory Proposal

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



Table of Contents

1. Document governance	4
1.1. Purpose of this document	4
2. Executive summary	5
3. CONTEXT	7
3.1. Background	7
3.1. Problem/opportunity	8
3.2. Compliance obligations	11
3.3. Risk appetite	15
3.4. Security management approach for OT	16
3.5. Operational Technology Security Program	18
3.6. Investment objectives	19
3.7. Customer outcomes	20
4. OPTIONS	22
4.1. OVERVIEW OF OPTIONS	22
4.2. OPTION 1: MAINTAIN OPERATIONAL TECHNOLOGY SECURITY	24
4.2.1. Description	24
4.2.2. Option 1 Assumptions	24
4.2.3. Option 1 – Risk Outcomes	25
4.2.4. NPV analysis	25
4.3. OPTION 2: LIMITED PROACTIVE SECURITY UPLIFT	26
4.3.1. Description	26
4.3.2. Option 2 Assumptions	27
4.3.3. Option 2 – Risk Outcomes	27
4.3.4. NPV analysis	28
4.4. OPTION 3: PROACTIVE & FULLY COMPLIANT SECURITY UPLIFT	28
4.4.1. Description	28
4.4.2. Option 3 Assumptions	29
4.4.3. Option 3 – Risk Outcomes	29
4.4.4. NPV analysis	30
4.5. OPTION 4: PROACTIVE & HIGHLY RESILIENT SECURITY UPLIFT	31
4.5.1. Description	31
4.5.2. Option 4 Assumptions	31
4.5.3. Option 4 – Risk Outcomes	32

4.5.4. NPV analysis	32
5. RECOMMENDATION	34
5.1. Recommended solution	34
Recommended Solution	34
5.2. Alignment to strategy	34
5.3. Program delivery risks.....	35
5.4. Program assumptions	36
5.5. Program dependencies	36
5.6. Business area impacts	36
APPENDIX A: PROPOSED OT SECURITY PROJECTS FOR 2025-29.....	37
APPENDIX B: APPROACH TO QUANTIFICATION OF PROJECT BENEFITS	38
APPENDIX C – INDUSTRY BEST PRACTICE FOR OPERATIONAL TECHNOLOGY	39
APPENDIX D – BEST PRACTICE IN OT – REFERENCE STANDARDS	45

1. Document governance

1.1. Purpose of this document

The purpose of this document is to outline the Operational Technology (OT) Security program for a continuation of the program of work that forms part of Ausgrid's 2024-29 regulatory proposal.

Related documents

Document	Version	Author
Attachment 5.2.a – Network Strategy	January 2023	Ausgrid
Attachment 5.9 – Technology Plan 2024-29	January 2023	Ausgrid
Attachment 5.9.e – Cyber Security Program	January 2023	Ausgrid
Ausgrid distributors license – Consolidated Licence Conditions – December 2017	December 2017	IPART
Attachment 5.5.a – Resilience Implementation Plan	January 2023	Ausgrid
Attachment 5.7 – CER Integration Program	January 2023	Ausgrid

2. Executive summary

“Operational technology” (OT) is the term used to describe hardware and software that detects or causes a change, through the direct monitoring and/or control of industrial equipment, assets, processes, and events¹. At Ausgrid this makes up the majority of the tools used to monitor and manage the electricity network in real-time.

This brief describes the initiatives necessary for us to protect and manage Ausgrid’s OT against known and likely future cyber threats. It describes a necessary increase in capability to meet the increasing level and severity of threats with the objective of maintaining the same outcome of our current capability: cyber resilience. Consistent with our IT cyber brief, we identify the most efficient means of delivering this higher level of capability, with the highest economic benefit for customers, as our proposed approach.

This program is a sub-component of Ausgrid’s overall Cyber Security protections and relates only to Ausgrid’s OT. The table below provides a summary of the OT Security program discussed in this business case. It demonstrates that the program of work, if approved, would strengthen Ausgrid’s security posture in defending against significant cyber security threats to Ausgrid’s OT systems and deliver net benefits of \$29.0 million based on our net present value (NPV) modelling.

The program of works has been established from the investment option (option 3 of 4) that presents the most favourable NPV for customers as it includes a portfolio of projects (largely related to technology-based controls) that deliver the highest net benefits and is able to demonstrate compliance with Ausgrid’s obligations for management of OT so far as is reasonably practicable (SFAIRP).

This program option will proactively reduce cyber risk within the OT domain to mitigate all known risks SFAIRP and within Ausgrid’s appetite while fully meeting licence conditions requiring the management of OT with ‘best practice’. The program will also seek to implement process controls enabling the organisation to achieve security profile level 3 as defined in the Australian Energy Sector Cyber Security Framework.

Executive summary	
Key Objective(s) of the program	<p>The purpose of the OT Security program for the 2024-29 regulatory control period is to strengthen Ausgrid’s OT resilience and to maintain a secure environment in defending against cyber threats, both remote and local, known, and unknown, and mitigate risks associated with known vulnerabilities.</p> <p>This program will also enable Ausgrid to maintain industry best practice for operational technology security as required in its Electricity Distribution Licence Conditions, maintain compliance with Security of Critical Infrastructure (SOCI) Act 2018 and other more recent amendments, and will meet Ausgrid’s risk appetite with respect to cyber risks and resiliency of OT systems [REDACTED].</p> <p>To achieve this objective a range of ‘best practice’ technology controls (as per critical infrastructure protection clauses of Ausgrid’s licence conditions), specific to the utilities industry, will be implemented within the electricity network control system and processes established to maintain these controls in alignment with security level 3 of the Australian Energy Sector Cyber Security Framework (AESCSF).</p>

¹ <https://www.gartner.com/en/information-technology/glossary/operational-technology-ot>.

Customer benefits	<ul style="list-style-type: none"> Adapt Ausgrid's OT environment so that it is current and secure for the critical role in distributing energy to customers and is capable of safely facilitating energy flows in the future energy mix and providing customers with greater choice and control of their energy use. Ensure the safe and secure operation and control of Ausgrid's electricity network, reducing the risk of cyber security-related outages and breaches, consistent with the national electricity objective (NEO), which requires Ausgrid to maintain the security of both the supply of electricity and the distribution network. Reduced risk (reduced frequency and recovery time from cyber events) of supply loss to customers and economic impacts from large scale loss of energy supply to customers following a cyber security related network outage. Reduced risk of significant disruption to critical infrastructure due to cyber security related network outages/interference. 						
Regulatory requirements	<ul style="list-style-type: none"> Ausgrid's Distribution Network Service Provider (DNSP) Ministerially Imposed Licence Conditions – Clause 9 & 10 – Critical Infrastructure National Electricity Rules Section 4.3.4I – articulates the requirement for secure and available systems in order to support responding to Australian Energy Market Operator (AEMO) direction. Security of Critical Infrastructure Act 2018, Security Legislation Amendments 2021 and 2022 Electricity Supply Act 1995 (NSW) Privacy Act 1988 						
NPV calculations	This program results in a net economic benefit of \$29.0m, largely driven by probabilistic benefits associated with reduced likelihood of unserved energy from a malicious cyber-attack on the OT environment						
Expenditure forecast (FY24 Real \$)	(\$m)	FY25	FY26	FY27	FY28	FY29	Total
	CAPEX	\$5.64	\$3.46	\$5.48	\$5.23	\$6.17	\$25.98
	OPEX	\$0.28	\$0.71	\$0.85	\$1.02	\$1.15	\$4.02
	Total	\$5.93	\$4.18	\$6.32	\$6.25	\$7.32	\$30.00

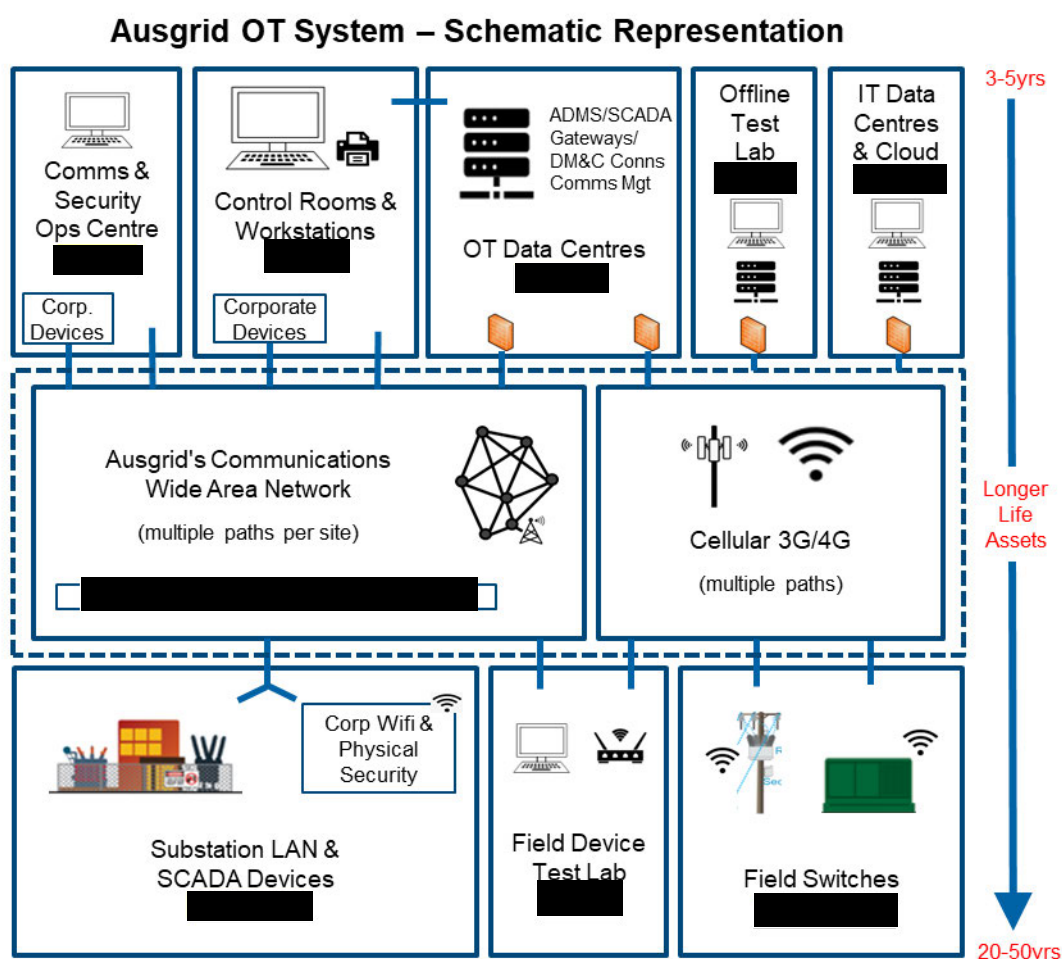
3. CONTEXT

3.1. Background

This document outlines the case for investment to strengthen Ausgrid's OT resilience and to maintain a secure environment in defending against cyber threats, both remote and local, and mitigate risks associated with known vulnerabilities.

Ausgrid's OT system is used to monitor and control the flow of electricity by operating network switches and intelligent devices across the grid. The OT system includes a large number of long-lived field devices, connected to our control centres via wide-area communications networks. The field devices and communications networks are complex and expensive to replace.

Figure 1- Schematic Representation of Ausgrid's OT System



This security program will also enable Ausgrid to maintain industry best practice as required in its Electricity Distribution Licence Conditions, maintain compliance with Security of Critical Infrastructure (**SOCI**) Act 2018, and regulatory obligations, and will meet Ausgrid's risk appetite with respect to cyber risks and resiliency of OT systems [REDACTED].

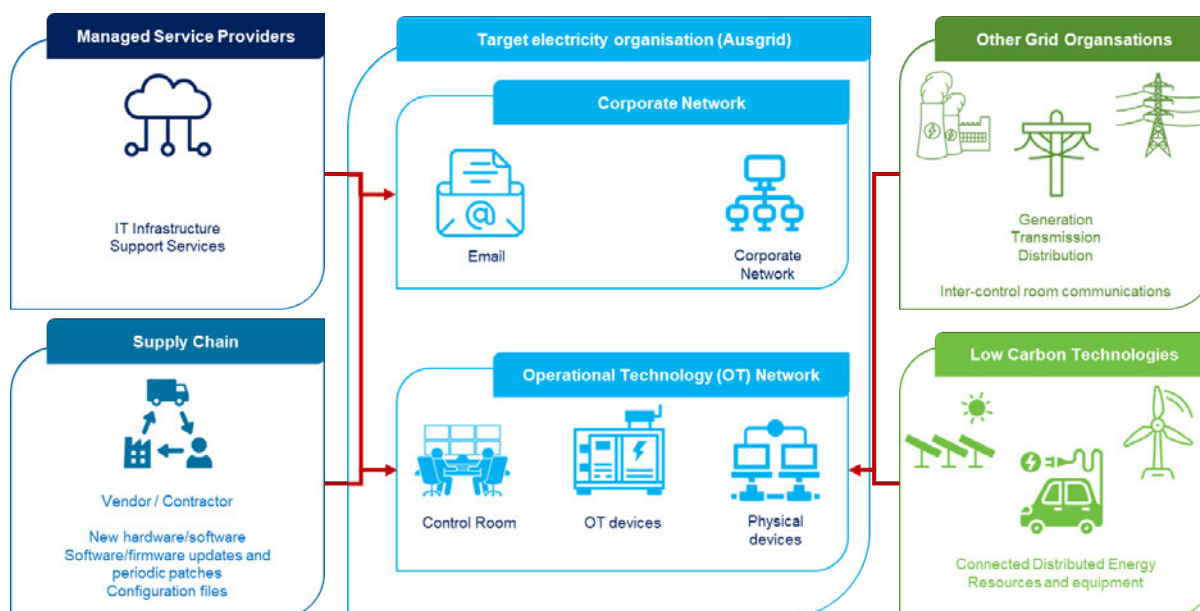
To achieve this objective a range of technology controls, specific to the utilities industry, will be implemented within the electricity network control system and processes established to maintain these controls in alignment with security level 3 of the Australian Energy Sector Cyber Security Framework (**AESCSF**). This approach will achieve the greatest NPV for customers.

3.1. Problem/opportunity

Electricity is an integral part of all modern economies, supporting a range of critical services including health care, transportation, communications, banking and gas and water utilities. The secure supply of electricity is of paramount importance.

Digitalisation is rapidly transforming the energy system, bringing many benefits for businesses and consumers. At the same time, increased connectivity (to both the electricity grid and IT system) and automation raises risks to cyber security and the threat of cyber-attacks. 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 and community disruption.

Figure 2 - Potential ways 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. Cyber-attacks are increasing in frequency, with a 13% increase in cyber-attacks reported by Australian entities to the ACSC in 2020-21.

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. 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”.²

Our strategy to transform into a Distributed Systems Operator (**DSO**) will result in emerging challenges posed by connected devices, smart grids and DER. 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:

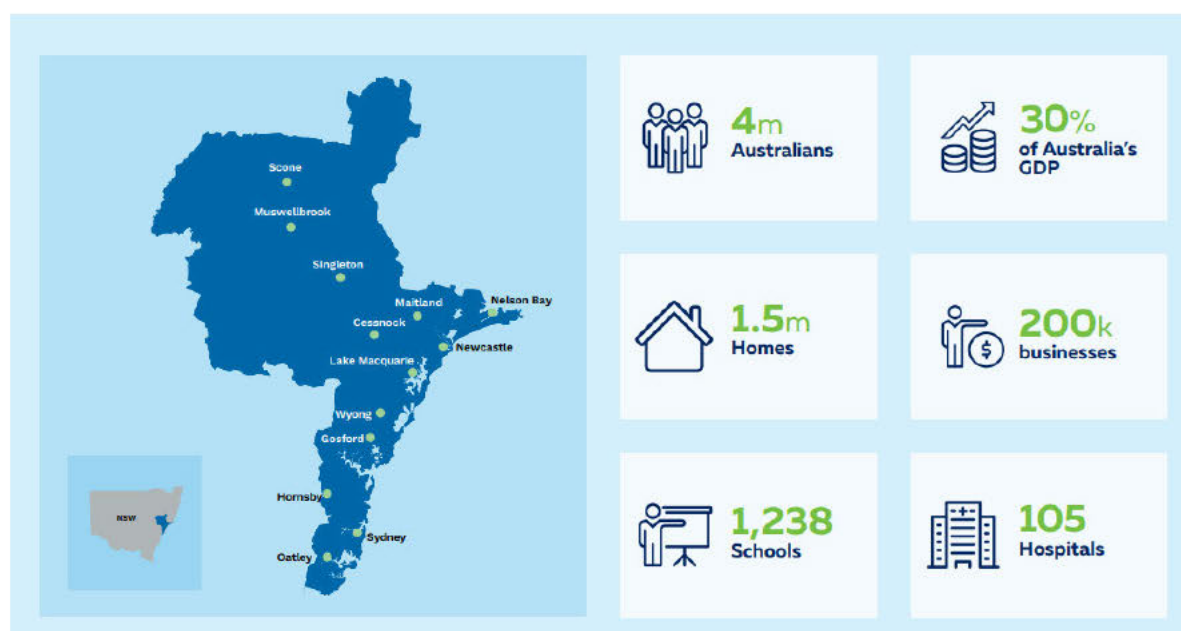
1. Increasing digitisation and automation of critical energy systems, increasing the risk of disruption through cyber-attacks;
2. International incidents related to critical infrastructure in the energy sector that have been attributed to cyber threat actors;
3. Increasing level of concern and urgency from Australian Government agencies in relation to cyber threats;
4. Increased usage of DER 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, quantum computing and predictive intelligence; and
8. Increasing complications 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**)³. Figure 3 below shows the geography serviced by Ausgrid and indicates the number of consumers, business and organisations potentially impacted by a cyber-attack on our distribution network.

² ACSC, *Australian organisations should urgently adopt an enhanced cybersecurity posture*, 28 March 2022.

³ NSW Government, *Sydney Facts*, <https://invest.nsw.gov.au/why-nsw/sydney-facts>, Accessed: 25 February 2022.

Figure 3 - 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 tolerable and within our risk averse appetite.

Electricity distribution businesses rely on a number of key OT applications and systems to safely and efficiently manage the flow of electricity across the distribution network, and also an essential role in the day-to-day delivery of planned augmentation, maintenance and unplanned work resulting from events such as faults or storms.

These OT applications and systems are integral to performing key network functions and are categorised into key domains for ensuring the distribution of electricity to Ausgrid's customers. The domains are:

- Central control system
- Communications to substation/field devices
- Substation and field devices

To continue to safely and securely manage the distribution of electricity to customers all three domains must remain operational with uncompromised integrity.

3.2. Compliance obligations

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

Table 1 – Cyber Security Obligations

Obligation	Description of Requirement
DNSP License Conditions	<p>License conditions⁴ 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 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. <p>Keeping our systems and network secured against cyber threats is a key enabler to meet these licence conditions. How this obligation relates to OT is detailed in Appendix D & E.</p>
Security of Critical Infrastructure Act 2018 (SOCI Act)	<p>The SOCI Act outlines specific requirements for owners and operators of critical infrastructure assets. This legislation directs the Commonwealth to establish and maintain a critical infrastructure asset register. It is this register that provides the foundation with which to identify, understand and manage the national security risks of espionage, sabotage and coercion. The Act 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"> • Critical Infrastructure Asset Register - As a critical infrastructure operator, we are to ensure the accuracy of asset information reported in the critical infrastructure register and provide annual reports to ensure the currency of the register. • Mandatory Reporting of Cyber Security Incidents - Subsequent amendments in December 2021 established requirements for mandatory reporting of cyber security incidents where there has been exploitation of our OT or IT systems.

⁴ 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>

Obligation	Description of Requirement
	Ausgrid has additional obligations under the SOCI Act which it is prohibited by law from disclosing.
AESCSF	<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 both ICT and OT infrastructure is kept up to date, supported and secured is a key enabler to meet our AESCSF maturity targets.</p>

Obligation	Description of Requirement
National Electricity Law and National Electricity Rules	<p>The National Electricity Law (NEL)⁵ 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 objectives⁶ 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>
Privacy Act 1988 & Information Privacy Act 2014	<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. 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.</p>

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.



⁵ The NEL is set out in a schedule to the *National Electricity (South Australia) Act 1996*.

⁶ See clauses 6.5.6(a) and 6.5.7(a) of the NER.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

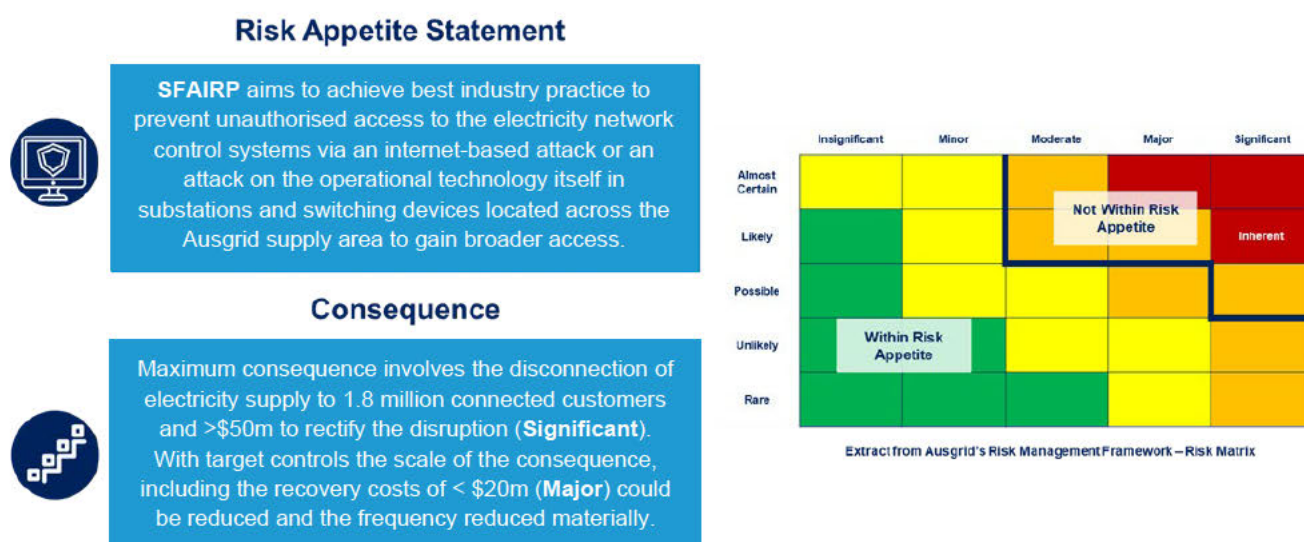
[REDACTED]

[REDACTED]

3.3. Risk appetite

We are risk averse in the way that we aim to prevent a successful cyber-attack on the electricity grid. We are continuing to apply best industry practice controls to prevent a significant protective security incident So Far As Is Reasonably Practical (**SFAIRP**). Refer to Figure 6 below.

Figure 5 - Ausgrid Risk statement, Risk Appetite and Risk Matrix



The proposed OT Security program seeks to reduce the risk profile of our key OT security risks so that the likelihood of each of those risks falls to within our risk appetite. The key OT security risks relate to the loss of supply of electricity to a small region of Ausgrid's supply area or to the total loss of supply of electricity to the whole supply area. These risks have consequences that are a major or significant classification respectively and the OT Security program seeks reduce the likelihood to within appetite SFAIRP.

The application of the SFAIRP approach to OT Security investments is demonstrated through detailed cost benefit analysis supporting the options and recommended investments outlined in this document.

A risk assessment of the OT environment demonstrates that Ausgrid is not within risk appetite without proactive and ongoing investment in security controls and mitigations. Ausgrid's detailed risk analysis supports this classification and has the following assessed outcomes:

- Without the current program of works to strengthen controls, the likelihood of a material event would manifest in up to 1 occurrence per year (**Possible**). With controls currently being delivered, the expected likelihood of this risk manifesting is less than 1 in 10 years (**Unlikely/Rare**), however will degrade if not continually upgraded and supplemented as cyber-attack sophistication increases,
- Major and widespread customer interruptions, high cost of response and/or extended time of impact to customers is **Significant** from a malicious breach of OT services, and

- The mitigative controls and plan of works are targeting a reduction of the consequence to **Major** by reducing the extent of impact to customers by segregating OT services and providing faster restoration

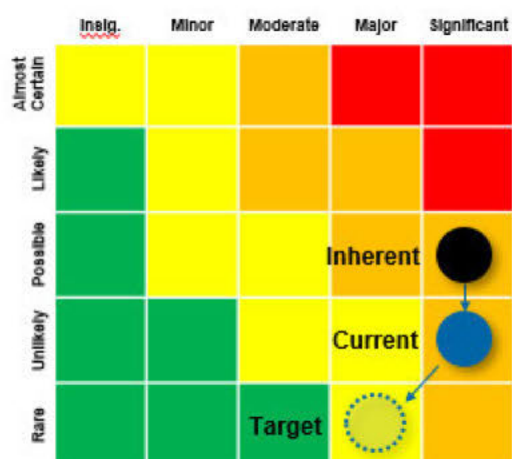
The direction of risk management associated with Ausgrid's OT environment is described in Figure 7 demonstrating our proposed approach to achieve and maintain compliance with regulatory requirements for *best practice* and manage the security risks to within appetite.

The likelihood of an event occurring is a balance between security controls and sophistication of a malicious attacker. As cyber security attacker capability grows the likelihood of a successful attack increases moving the *Current* risk towards the *Inherent* risk position in Figure 7.



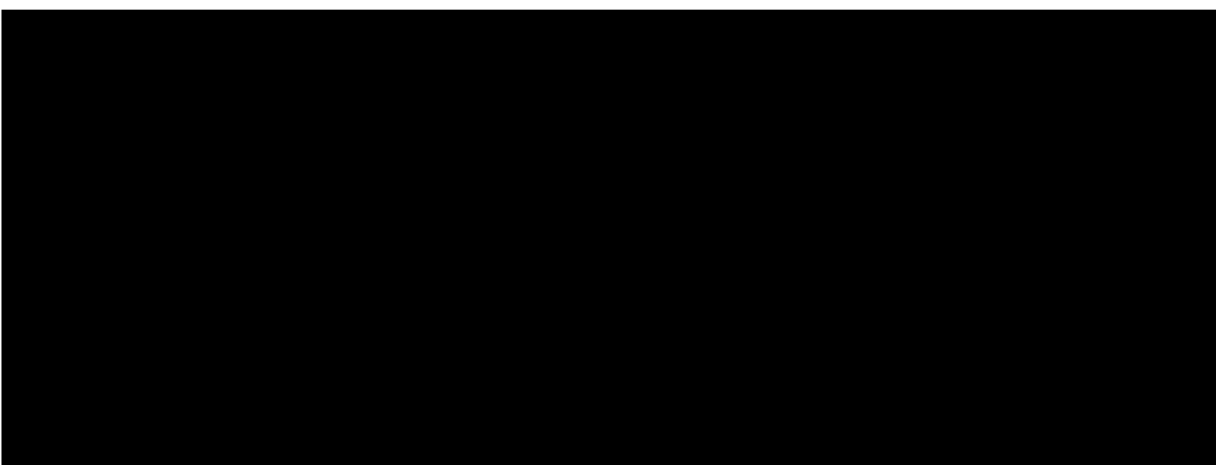
The OT Security program seeks to maintain and uplift security controls to combat the increasing sophistication of attackers and reduce the potential impact of a successful attack as indicated in the *Target* state in Figure 7.

Figure 6 - Ausgrid Proposed Risk Appetite for OT

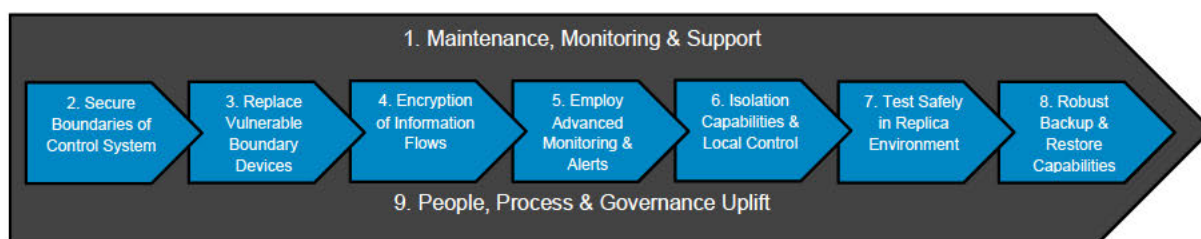


3.4. Security management approach for OT

OT security management takes a risk-based approach to focus resources in a sustainable way on the most critical and vulnerable assets. Compensating controls are designed and introduced to mitigate any vulnerabilities where this cannot be reasonably achieved.



Security management of the OT system can be characterised by the following key themes with each focused on a specific set of activities.



Each of these OT security themes is described in further detail below.

1. **Maintenance, monitoring & support** – ongoing operations to monitor, maintain the integrity of OT devices and systems, including support updates as required.
2. **Replacement of vulnerable boundary devices** – Targeting boundary devices with known vulnerabilities due to their lack of support and obsolescence that could be exploited to provide an entry point into the OT environment where further inherent vulnerabilities can be exploited.
3. **Securing the boundaries of the control system** – Implement new technologies to improve access control, reduce points of entry with the use of data diodes, modern firewall functionality, router updates and further separation of IT and OT networks.
4. **Encryption of information flows** – securing communication in transit so that it cannot be intercepted without access to communication end points, reducing dependence on communications technologies for security.
5. **Test safely in replica environment** – maintaining a replica OT environment that can be used to scan and test new devices and applications for vulnerabilities without risking the live OT environment.
6. **Advanced monitoring & alerts** – implementation of traffic monitoring on both data centre and key substations to monitor device health and correlate events and traffic patterns to detect & alert administrators to unusual system behaviour.
7. **Isolation capability and local control** – Implement points of isolation that enable at-risk segments of the network to be isolated & execute manual controls.
8. **Robust backup & restore capabilities** – Establish routine and automated backups of all components of the OT environment with playbooks to rapidly restore to a known operational state.
9. **People, process & governance uplift** – Physical security of major substations is ineffective from a coordinated and planned attack and OT security aims to limit impacts to only that site.

Each of these key themes has a distinct focus on particular phases of the security lifecycle and subsequent activities with coverage across all phases required to minimise impacts from a cyber-attack on the OT system. The applicable security phases are shown in *Table 2* for each key theme.

Table 2 – Key Investment & Operational Areas of Focus for OT Security

Key Investment & Operations Areas	Security Phase				
	Identify	Protect	Detect	Respond	Recover
Maintenance, monitoring & support	Y	Y	Y		
Replacement of vulnerable boundary devices		Y			
Securing the boundaries of the control system		Y			
Encryption of information flows		Y			
Test safely in replica environment	Y	Y	Y		
Advanced monitoring & alerts	Y		Y		
Isolation capability & local control		Y		Y	Y
Robust backup & restore capabilities					Y
People, process & governance uplift	Y	Y	Y	Y	Y

3.5. Operational Technology Security Program

This program has been developed to mitigate the risks of a cyber security attack on the OT applications and systems SFAIRP. This approach will also continue to maintain and enhance Ausgrid's control system security posture and maintain compliance with NSW Distributors Licence, specifically the Critical Infrastructure Licence Conditions, and broader Commonwealth Government cyber security legislation and guidelines.

It has also been developed in the context of Ausgrid's obligations to maintain the quality, reliability and security and maintain the safety of the distribution system through the supply of standard control services as required in the NER (6.5.7 (a) 3 & 4).

There is an increasing need to deploy new operational technologies to management the electricity network and a subsequent need to increasingly interface OT and IT environment for dynamic network management. Combined with an increasing threat sophistication and these changes create an ever increasing need to apply additional compensating controls to the OT environment to manage the related cyber risks SFAIRP.

The OT Security Program includes projects to maintain existing security controls and uplift or deploy new controls across three key domains. The domains are:

- Central control system
- Communications to substation/field devices
- Substation and field devices



Ausgrid's core control system is currently being replaced by a modern Advanced Distribution Management System (ADMS). The ADMS application will enable the retirement of some legacy core infrastructure components.



As required by critical infrastructure licence conditions, Ausgrid must use best industry practice for management of electricity network control systems and ensure that operation and control of its distribution system, including all associated infrastructure, can only be accessed, operated and controlled from within Australia.

These OT applications and systems are integral to performing key network functions and ensuring the distribution of electricity to Ausgrid's customers. Asset lives increase as deployment of these devices or communications becomes further from central locations limiting access, specifically in substations, on pole top structures, or communications assets connecting these sites.

Security controls need to be continually updated to ensure they accommodate new technology developments, threats and vulnerabilities. To minimise the cost of replacing long lived assets at a shorter period due to the need to maintain modern security features, the program aims to deploy solutions through a range of projects to minimise the impact to the overall electricity network control system from the use of legacy network control devices. This requires appropriate communications segregation and central control system protections. Where this cannot be achieved legacy field devices are required to be replaced or sophisticated monitoring installed.

Ausgrid will continue to invest in a number of systems to increase the resilience of the OT and enable the remote control and management of associated secondary systems which provide protection, control and monitoring of the electrical network. This investment is in addition to enterprise cyber security controls that protect against a malicious attacker utilising the internet or corporate applications or systems to compromise the integrity of the IT environment.

3.6. Investment objectives

This program is designed to achieve the following specific objectives:

- Mitigate assessed, known, emerging and future cyber security risks to the OT environment;
- Maintain compliance with regulatory obligations and work towards SP3 process compliance and security control obligations as the SOCI Act evolves;
- Counter the increasing attention Ausgrid faces from threat actors;
- Maintain control design and effectiveness of implemented OT security controls;
- Implement new OT security controls to mitigate known, unmanaged risks in the OT environment;
- Provide Ausgrid and its customers the confidence that Ausgrid can identify, detect, protect and respond to increasing cyber security threats;
- Develop the capability to securely integrate new technology into the network to drive efficiency in energy distribution over the long term;
- Modernise the OT security functionality to keep pace with external cyber capability and facilitate the adoption of new capabilities, technology and equipment to prevent breaches of the OT environment;
- Improve the resilience of customer energy supply in the face of a changing external threat landscape and increasing societal dependency on electricity; and

- Deploy enabling technology, devices and systems to facilitate the safe and secure transition towards a less carbon intensive energy system including customer preferences to incorporate DER such as solar generation, electric vehicles and household batteries.

To achieve these objectives, the OT Security Program comprises a range of investments which may evolve over time as technology matures. To manage the uncertainty associated with investment of this nature, Ausgrid will continue to prioritise the projects in line with our approach in the 2019-24 regulatory reset period.

We have included an operational expenditure component to address the maintenance and support of the new capabilities and will continually seek to find efficiencies to reduce this ongoing operational uplift.

The program is structured to consider a range of technology focused as reducing the risk from a malicious cyber-attack on the OT environment through a layered defence approach.

To ensure the greatest economic value from the investments Ausgrid utilises quantitative risk assessment to measure the expected risk reduction prior to determining to invest in each project within the program.

3.7. Customer outcomes

Through a co-design process with customer advocates, we identified six key topics that will define our business into the future. Of these, the OT security program is particularly aligned to Resilient theme in maintaining the safety and security of the network, also with a direct impact on Improved Customer Experience and Value for Money.

Table 3 – Themes Identified to Define the Business into the Future

Theme	Overview
Fair	<ul style="list-style-type: none"> • Intergenerational equity • No one left behind, where practical
Sustainable	<ul style="list-style-type: none"> • Lowering Ausgrid's carbon footprint • Facilitating the transition to net zero by 2050
Future network	<ul style="list-style-type: none"> • Creating shared value in the community • Encouraging DER across different geographic and customer segments
Customer experience	<ul style="list-style-type: none"> • Digitalisation of services • Quality of service and bespoke experiences and outcomes
Resilient	<ul style="list-style-type: none"> • Respond to climate change and changing community needs • Maintain safety, reliability and network security
Value for money	<ul style="list-style-type: none"> • Unlock additional value while keeping bills stable • Benefits from investments exceed the costs which will be incurred

The proposed investment in OT security will deliver:

- Resilient outcomes for customers, by maintaining safety, reliability and network security;
- Improve Customer Experience by reducing the risk of cyber-attacks resulting in network outages and disruptions, and theft of, or unauthorised access to OT design data;
- Value for Money, with the expected benefits (i.e. reduced investment in replacing legacy electricity network technologies) being lower than otherwise required to maintain our regulatory obligations.

The benefits of this program are largely focused on avoiding disruptions to customers from a malicious cyber intrusion into the operational technology systems of Ausgrid where the attacker could disrupt or compromise the safe and reliable operation of the electricity network. This consequence has not been experienced within Ausgrid previously and therefore must utilise the experiences of other Australian

businesses and international electricity utilities to fully appreciate the significant consequences on both the supply of electricity to consumers and also the economic impact to Australians.

These impacts are listed in the table below to better understand the detailed linkages between the impacts to customers and the investments within the OT security program.

Table 4 – Key Customer Benefits from the OT Security Program

Benefit	Overview
Avoid Large Scale Disruptions	Reduce exposure of control system – greater protections from malicious actors and rapid response to eliminate threat before disruption occurs
Quicker Response to Disruptions	Rapid event response – Improvements to isolation and restoration of power supply following an authorised operation of the grid
Improved Customer Safety	Rapid and remote network intervention – improve availability of remote operability during an attack or heightened threat level to isolate hazards to customers and the public
Efficient Customer Connections	Reduced complexity and cost – establishing pre-approved secure methods of communicating between customer and grid assets
Long Term Affordability	Modest and targeted investment – select investments in compensating security controls will maintain affordability rather than wholesale replacement of legacy devices where they become vulnerable



4. OPTIONS


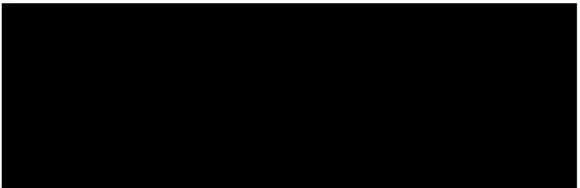
This section provides an overview of a select number of options which could credibly address the need to uplift and modernise Ausgrid's cyber function. The NPV associated with each option is also noted.

4.1. OVERVIEW OF OPTIONS

Four options have been considered, which are listed in the table below. The recommended option for the 2025-29 period is option 3 based on quantitative analysis demonstrating that it will unlock the most net economic benefits while maintain compliance and alignment with critical infrastructure licence conditions and good industry practice for OT systems.

Table 5 – Overview of OT Security Program Options

Option	Description	NPV
Option 1: Maintenance of Existing Protections Only	<p>No significant investments in Ausgrid's OT security will be undertaken in the 2025-29 regulatory control period, with investment focused only on maintaining current protections.</p> <p>Continue to replace existing security controls only at end of life to maintain services in an environment with security risk escalation. This will demonstrate compliance with the current Critical Infrastructure Act and pose a risk of non-compliance to the critical infrastructure clauses of the existing NSW Government licence conditions.</p> <p>Security Profile 1 (SP-1) level process controls to complement technology-based security controls.</p> 	\$10.4m
Option 2: Limited Proactive Uplift	<p>Ausgrid will further extend its OT security process maturity by expanding on SP1 compliance and move towards SP2 based on risks and threats.</p> <p>Proactive uplift of OT technology-based security controls to mitigate key risks, with the ability to demonstrate compliance to licence conditions requiring the management of OT with 'best practice'</p> <p>Security Profile 2 (SP-2) level process controls to complement technology-based security controls.</p> 	\$26.1m

Option 3: Proactive & Fully Compliant Uplift	<p>Ausgrid will further extend its OT security process maturity by expanding on SP1 compliance and move towards SP3.</p> <p>This option adopts the majority of the initiatives identified through the review of Ausgrid's OT security program. This option provides the highest economic value and a high level of protection / mitigation against potential cyber attacks to OT systems.</p> <p>Proactive uplift of OT technology-based security controls to mitigate all known risks SFAIRP while fully meeting licence conditions requiring the management of OT with 'best practice'.</p> <p>Security Profile 3 (SP-3) level process controls to complement technology-based security controls.</p> 	\$29.0m
Option 4: Proactive & Highly Resilient Uplift	<p>Ausgrid will further extend its OT security process maturity by expanding on SP1 compliance and move towards SP3.</p> <p>This option adopts all the initiatives identified through the review of Ausgrid's OT security program. This option provides the second highest economic value and a very high level of protection / mitigation against potential cyber attacks to OT systems.</p> <p>Aggressive uplift of OT technology-based security controls to further strengthen separation of OT and IT networks, mitigating all known risks SFAIRP and meeting licence conditions.</p> <p>Security Profile 3 (SP-3) level process controls to complement technology-based security controls.</p> 	\$20.6m

The principal difference between the four options is the level of protections employed within the OT system, with technology and process maturity increases to at minimum keep pace with the growing capability of malicious actors seeking to disrupt network operations and supply of electricity to consumers.

- Option 1 maintains the existing level of OT system protections;

- Option 2 introduces additional controls for communication security and advanced monitoring;
- Option 3 expands on option 2, incorporating further replacement of legacy and vulnerable field devices;
- Option 4 expand on option 3, incorporating further separation and reduced dependence upon third parties for critical control system communications.

We did not include a “do nothing” option as this was not considered a credible option. Failure to adequately address OT security risks would result in an unacceptable level of risk.

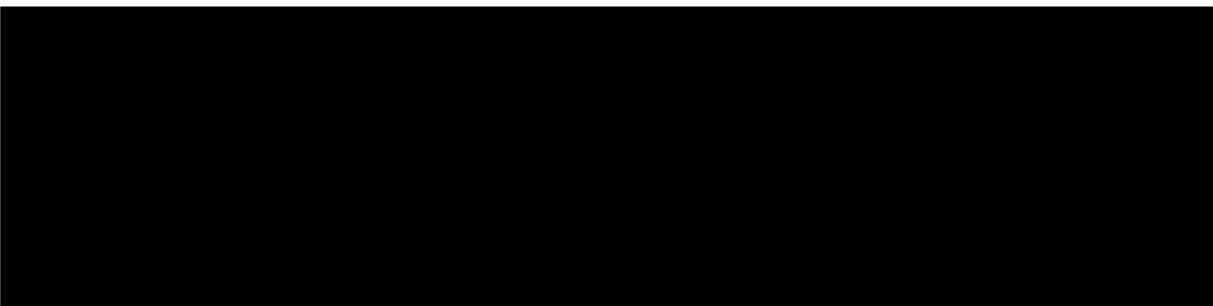
4.2. OPTION 1: MAINTAIN OPERATIONAL TECHNOLOGY SECURITY

4.2.1. Description

This option involves the maintenance and replacement of existing technology-based security controls within the OT environment and uplift of security controls only where they are known to be highly vulnerable to attack.

No significant investments in Ausgrid's OT security will be undertaken in the 2025-29 regulatory control period, with investment focused only on maintaining current protections and continue to replace existing equipment only at end of life to maintain services in an environment with security risk escalation. This will demonstrate compliance with the current Critical Infrastructure Act and pose a risk of non-compliance to the critical infrastructure clauses of the existing NSW Government licence conditions.

Security Profile 1 (SP-1) level process controls will be maintained to complement technology-based security controls.



4.2.2. Option 1 Assumptions

Option1 has been estimated based on the following assumptions:

1. Threat escalation has been modelled at 13% pa in line with recent announcements from the Australian Cyber Security Centre (ACSC);
2. The largest consequence from an intentional and educated breach of the OT environment will result in widespread power outages for 12 hours (capped);
3. A proliferation of an IT or OT breach is modelled in 10% of occasions; and
4. The boundaries of the OT environment include field/substation devices, communications channels, OT and IT data centres and the internet.

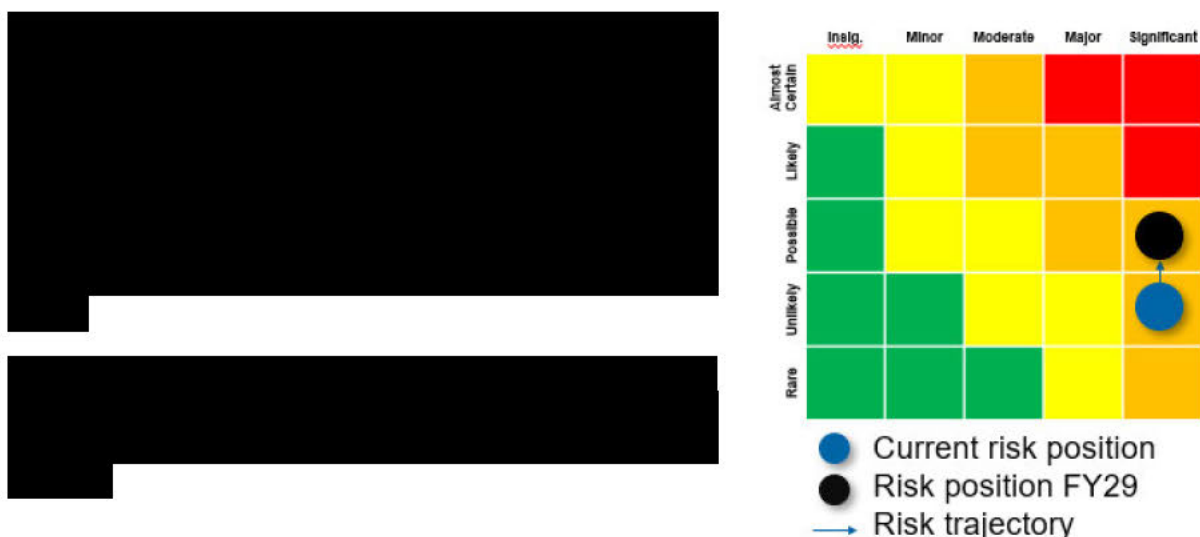
The investment is separated into recurrent and non-recurrent expenditure

- Recurrent expenditure is associated with maintaining existing functions and capacity and would refer to investments that are made on a frequent periodic basis.

- Non-recurrent expenditure refers to major (one off, infrequent, or non-periodic) investments related to replacing existing ICT assets or the acquisition of new ICT assets, functions, or capability that is driven by a specific need.

The costs of this option have been estimated based on initial estimates of each project, based on historical expenditure in similar equipment and associated labour and contracted services.

4.2.3. Option 1 – Risk Outcomes



Capital Cost and Scope Assumptions

\$ million	FY25	FY26	FY27	FY28	FY29	Total
CAPEX	\$1.63m	\$1.29m	\$0.54m	\$0.81m	\$1.19m	\$5.46m

Operating Cost Assumptions

\$ million	FY25	FY26	FY27	FY28	FY29	Total
OPEX	\$0.15m	\$0.14m	\$0.15m	\$0.15m	\$0.15m	\$0.59m

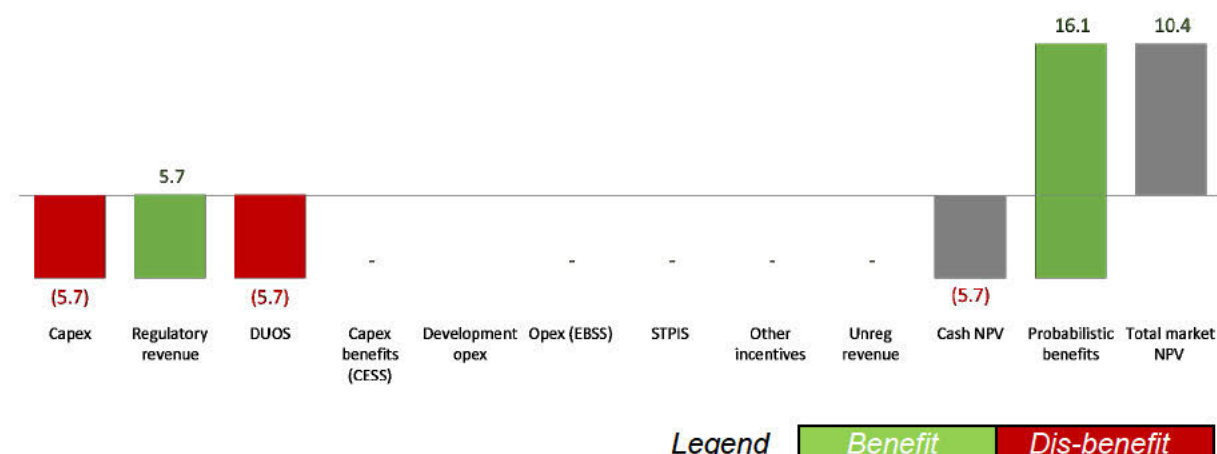
Additional opex has not been included as a step change in the 2024-29 regulatory submission.

4.2.4. NPV analysis

The NPV analysis considered benefits across a broad value framework considering:

- Capex avoided from repex expenditure based on damage of equipment
- Some opex and capex loss of productivity benefits in field response and incident management
- Market benefits primarily from customer unserved energy triggered by a cyber attack

These benefits were applied based on expected risk reductions from development and deployment of the various projects within this program option.

Market NPV of option (\$' millions, real FY22)

The investment only in maintenance of current risks, and subsequent lack of positive probabilistic benefits in a climate of increasing external threats were the primary driver for the negative NPV outcomes.

4.3. OPTION 2: LIMITED PROACTIVE SECURITY UPLIFT

4.3.1. Description

Under this option, Ausgrid will further extend its OT security maturity with a proactive uplift of security controls where they are known to be highly vulnerable to attack and also where it is reasonably foreseeable that an attack could be mitigated with next controls, including the maintenance and replacement of existing security controls within the OT environment and uplift of security controls only.

Ausgrid will further extend its OT security process maturity by expanding on SP1 compliance and move towards SP2 based on risks and threats. A proactive uplift of OT security technology controls to mitigate key risks, with the ability to demonstrate compliance to licence conditions requiring the management of OT with 'best practice'.

Security Profile 2 (SP-2) level process controls will be deployed and maintained to complement technology-based security controls.



4.3.2. Option 2 Assumptions

Option 2 has been estimated based on the following assumptions:

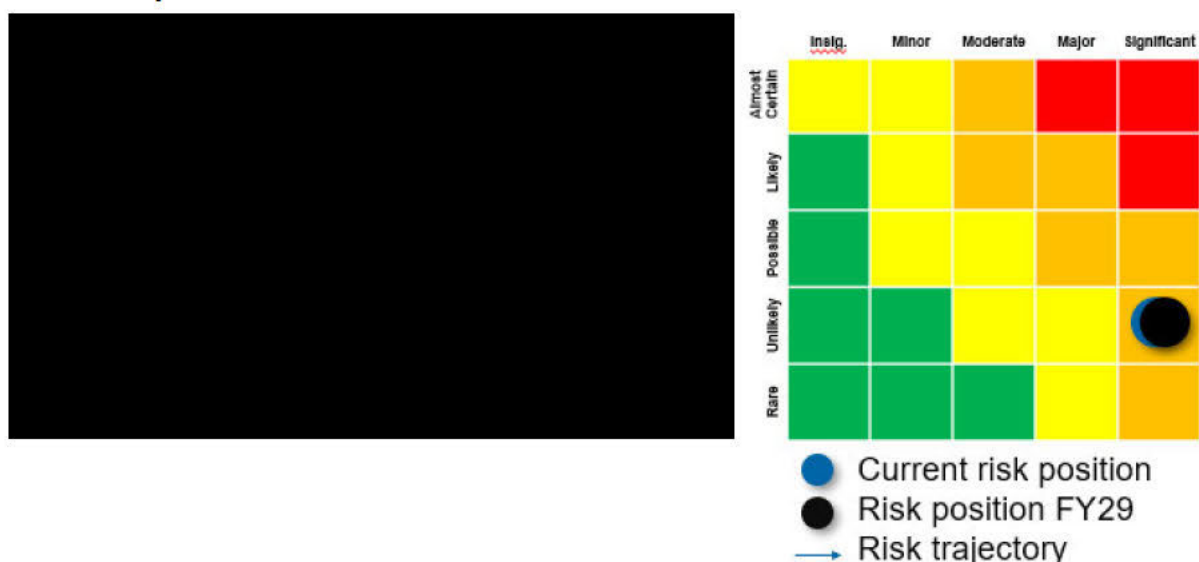
1. Threat escalation has been modelled at 13% pa in line with recent announcements from the Australian Cyber Security Centre (ACSC);
2. The largest consequence from an intentional and educated breach of the OT environment will result in wide spread power outages for 12 hours (capped);
3. A proliferation of an IT or OT breach is modelled in 10% of occasions; and
4. The boundaries of the OT environment include field/substation devices, communications channels, OT and IT data centres and the internet.

The investment is separated into recurrent and non-recurrent expenditure

- Recurrent expenditure is associated with maintaining existing functions and capacity and would refer to investments that are made on a frequent periodic basis.
- Non-recurrent expenditure refers to major (one off, infrequent, or non-periodic) investments related to replacing existing ICT assets or the acquisition of new ICT assets, functions, or capability that is driven by a specific need.

The costs of this option have been estimated based on initial estimates of each project, based on historical expenditure in similar equipment and associated labour and contracted services.

4.3.3. Option 2 – Risk Outcomes



Capital Cost and Scope Assumptions

\$ million	FY25	FY26	FY27	FY28	FY29	Total
CAPEX	\$3.09m	\$1.91	\$3.33m	\$4.69m	\$6.07m	\$19.09m

Operating Cost Assumptions

\$ million	FY25	FY26	FY27	FY28	FY29	Total
OPEX	\$0.27	\$0.26	\$0.38	\$0.38	\$0.38	\$1.66

Additional opex has not been included as a step change in the 2024-29 regulatory submission.

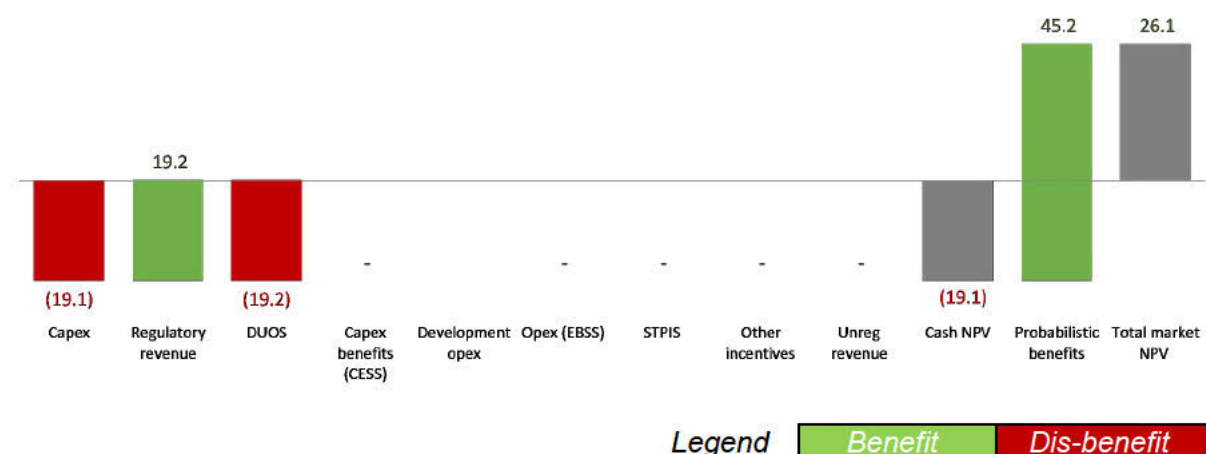
4.3.4. NPV analysis

The NPV analysis considered benefits across a broad value framework considering:

- Capex avoided from repex expenditure based on damage of equipment
- Some opex and capex loss of productivity benefits in field response and incident management
- Market benefits primarily from customer unserved energy triggered by a cyber attack

These benefits were applied based on expected risk reductions from development and deployment of the various projects within this program option.

Market NPV of option (\$' millions, real FY22)



Probabilistic benefits were the primary driver for the positive NPV outcomes, particularly driven by reduced likelihood of unserved energy value from a malicious cyber-attack on the OT environment.

4.4. OPTION 3: PROACTIVE & FULLY COMPLIANT SECURITY UPLIFT

4.4.1. Description

Under this option, Ausgrid will further extend its OT security maturity with a highly proactive uplift of security controls where they are known to be highly vulnerable to attack and also where it is reasonably foreseeable that an attack could be mitigated with next controls with advanced functionality. This option also includes the maintenance and replacement of existing security controls within the OT environment and uplift of security controls only.

Ausgrid will further extend its OT security process maturity by expanding on SP1 and SP2 compliance and move towards SP3 based on risks and threats. This option adopts the majority of the initiatives identified through the review of Ausgrid's OT security program. This option provides the highest economic value and a high level of protection / mitigation against potential cyber-attacks to OT systems.

Proactive uplift of OT security to mitigate all known risks SFAIRP while fully meeting licence conditions requiring the management of OT with 'best practice'

Security Profile 3 (SP-3) level process controls will be deployed and maintained to complement technology-based security controls.



4.4.2. Option 3 Assumptions

Option 3 has been estimated based on the following assumptions:

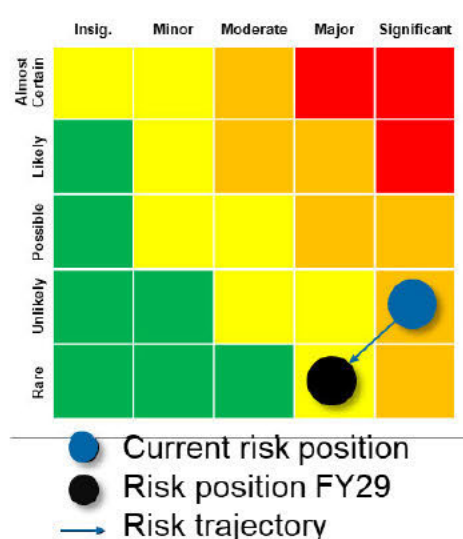
1. Threat escalation has been modelled at 13% pa in line with recent announcements from the Australian Cyber Security Centre (ACSC);
2. The largest consequence from an intentional and educated breach of the OT environment will result in widespread power outages for 12 hours (capped);
3. A proliferation of an IT or OT breach is modelled in 10% of occasions; and
4. [REDACTED]

The investment is separated into recurrent and non-recurrent expenditure

- Recurrent expenditure is associated with maintaining existing functions and capacity and would refer to investments that are made on a frequent periodic basis.
- Non-recurrent expenditure refers to major (one off, infrequent, or non-periodic) investments related to replacing existing ICT assets or the acquisition of new ICT assets, functions, or capability that is driven by a specific need.

The costs of this option have been estimated based on initial estimates of each project, based on historical expenditure in similar equipment and associated labour and contracted services.

4.4.3. Option 3 – Risk Outcomes



Capital Cost and Scope Assumptions

\$ million	FY25	FY26	FY27	FY28	FY29	Total
CAPEX	\$5.64m	\$3.46m	\$5.48m	\$5.23m	\$6.17m	\$25.98m

Operating Cost Assumptions

\$ million	FY25	FY26	FY27	FY28	FY29	Total
OPEX	\$0.28m	\$0.71m	\$0.85m	\$1.02m	\$1.15m	\$4.02m

Additional opex has not been included as a step change in the 2024-29 regulatory submission.

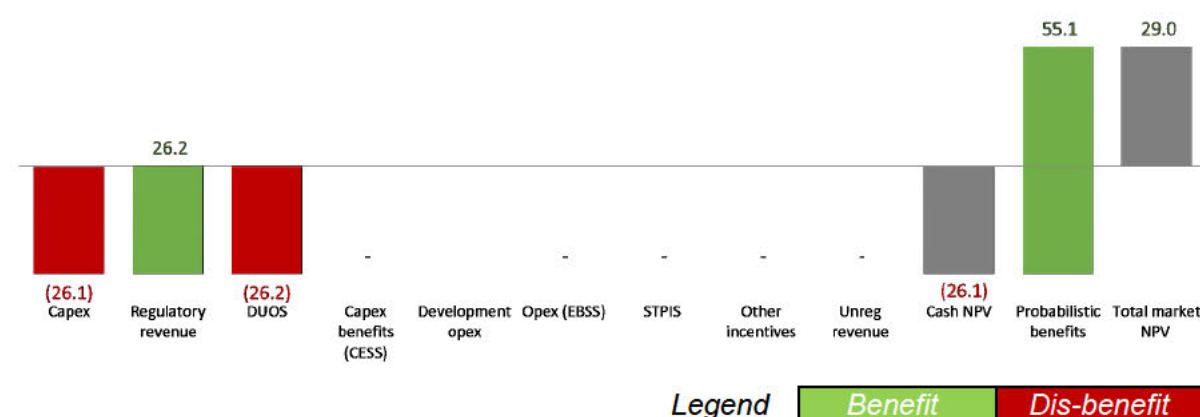
4.4.4. NPV analysis

The NPV analysis considered benefits across a broad value framework considering:

- Capex avoided from repex expenditure based on damage of equipment
- Some opex and capex loss of productivity benefits in field response and incident management
- Market benefits primarily from customer unserved energy triggered by a cyber attack

These benefits were applied based on expected risk reductions from development and deployment of the various projects within this program option.

Market NPV of option (\$' millions, real FY22)



Probabilistic benefits were the primary driver for the positive NPV outcomes, particularly driven by reduced likelihood of unserved energy value from a malicious cyber attack on the OT environment. The opex supporting this options a significant driver of the NPV outcome and would increase significantly if licence cost efficiencies could be found.

4.5. OPTION 4: PROACTIVE & HIGHLY RESILIENT SECURITY UPLIFT

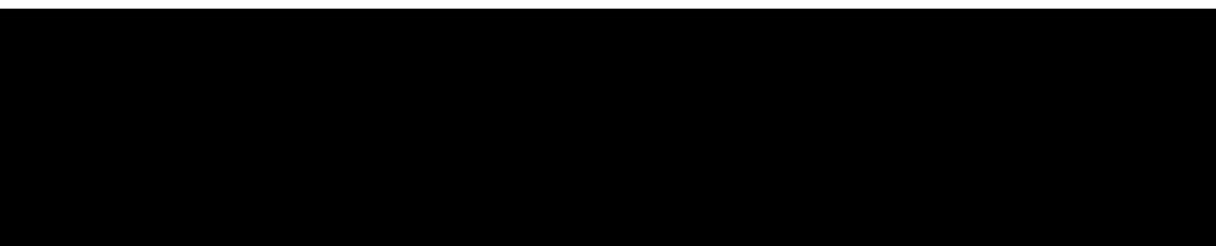
4.5.1. Description

Under this option, Ausgrid will further extend its OT security maturity by adopting all the initiatives identified through the review of Ausgrid's OT security program. This includes an aggressive uplift of security controls where they are known to be highly vulnerable to attack and also where it is reasonably foreseeable that an attack could be mitigated with next controls with advanced functionality. This option also includes the maintenance and replacement of existing security controls within the OT environment and uplift of security controls only.

Ausgrid will further extend its OT security process maturity by expanding on SP1 and SP2 compliance and move towards SP3 based on risks and threats. This option provides the second highest economic value and a very high level of protection / mitigation against potential cyber-attacks to OT systems. This includes an aggressive uplift of OT security to further strengthen separation of OT and IT networks, mitigating all known risks SFAIRP and meeting licence conditions.

This option will proactively uplift of OT security to mitigate all known risks SFAIRP while fully meeting licence conditions requiring the management of OT with 'best practice'

Security Profile 3 (SP-3) level process controls will be deployed and maintained to complement technology-based security controls



Option 4 provides the enhanced capabilities of Option 3, however, also includes the full physical separation of the OT Environment onto different communications of that to IT. This project provides marginal security improvement in providing greater IT/OT isolation, however the cost and complexity of this key project in Option 4 presents a significant delivery risk.

4.5.2. Option 4 Assumptions

Option 3 has been estimated based on the following assumptions:

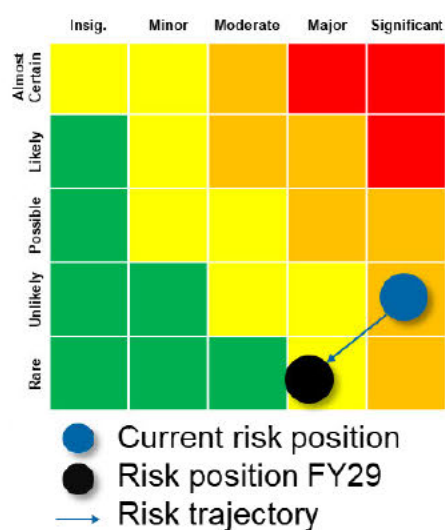
1. Threat escalation has been modelled at 13% pa in line with recent announcements from the Australian Cyber Security Centre (ACSC);
2. The largest consequence from an intentional and educated breach of the OT environment will result in widespread power outages for 12 hours (capped);
3. A proliferation of an IT or OT breach is modelled in 10% of occasions; and
4. The boundaries of the OT environment include field/substation devices, communications channels, OT and IT data centres and the internet.

The investment is separated into recurrent and non-recurrent expenditure

- Recurrent expenditure is associated with maintaining existing functions and capacity and would refer to investments that are made on a frequent periodic basis.
- Non-recurrent expenditure refers to major (one off, infrequent, or non-periodic) investments related to replacing existing ICT assets or the acquisition of new ICT assets, functions, or capability that is driven by a specific need.

The costs of this option have been estimated based on initial estimates of each project, based on historical expenditure in similar equipment and associated labour and contracted services.

4.5.3. Option 4 – Risk Outcomes



Capital Cost and Scope Assumptions

\$ million	FY25	FY26	FY27	FY28	FY29	Total
CAPEX	\$5.86m	\$7.91m	\$7.73m	\$7.49m	\$6.17m	\$35.16m

Operating Cost Assumptions

\$ million	FY25	FY26	FY27	FY28	FY29	Total
OPEX	\$0.28m	\$0.71m	\$1.06m	\$1.24m	\$1.36m	\$4.66m

Additional opex has not been included as a step change in the 2024-29 regulatory submission.

4.5.4. NPV analysis

The NPV analysis considered benefits across a broad value framework considering:

- Capex avoided from repex expenditure based on damage of equipment
- Some opex and capex loss of productivity benefits in field response and incident management
- Market benefits primarily from customer unserved energy triggered by a cyber attack

These benefits were applied based on expected risk reductions from development and deployment of the various projects within this program option.

Market NPV of option (\$' millions, real FY22)

Probabilistic benefits were the primary driver for the positive NPV outcomes, particularly driven by reduced likelihood of unserved energy value from a malicious cyber-attack on the OT environment with significant impact from the opex required to support this option.

5. RECOMMENDATION

5.1. Recommended solution

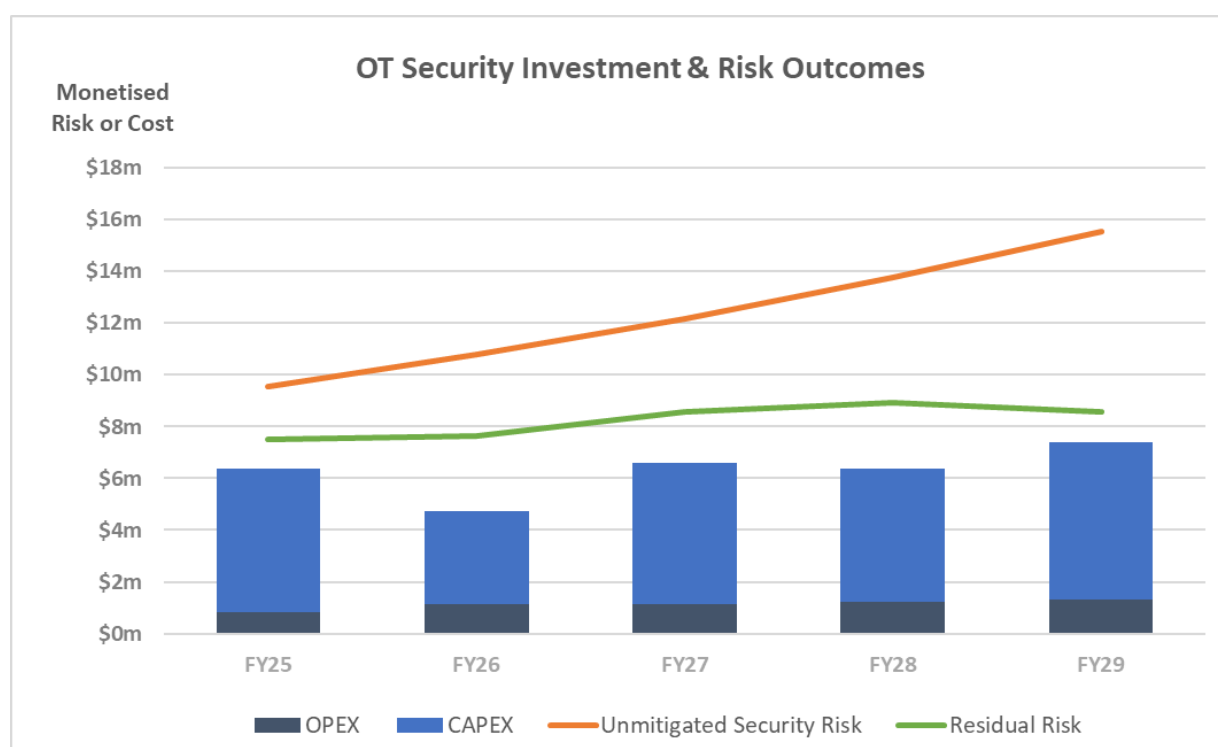
Recommended Solution

- Option 3 is the recommended OT security program as it includes a portfolio of projects that delivers the highest net benefits and seeks to achieve full compliance with regulatory obligations for management of Operational Technology
- This program option will proactively reduce cyber risk within the OT domain to mitigate all known risks SFAIRP and within Ausgrid's appetite while fully meeting licence conditions requiring the management of OT with 'best practice'
- The program will also seek to implement process controls to achieve security profile level 3 as defined in the Australian Energy Sector Cyber Security Framework.

The risk outcomes from the program are shown below in **Figure 8** where the benefits from the investment in the 2024-2029 period continue to accrue into the longer term with limited expenditure to maintain controls.

The benefits (difference between the unmitigated and residual risk) shown in **Figure 8** below continue beyond the period shown resulting in a positive NPV outcome. I.e. Benefits continue to accrue beyond the date at which the investment is concluded and will continue until the assets supporting the risk mitigation reaches end of life and are replaced or upgraded.

Figure 7 – OT Security Program Risk Outcomes



5.2. Alignment to strategy

The recommended option is included in Ausgrid's business plan and aligns to the current Corporate, Network, Asset Management and Cyber Security strategies. It also meets the NER expenditure objectives, criteria and factors relating to prudence and efficiency of expenditure.

5.3. Program delivery risks

The key risks of the program relate to delivery risk and technology selection. The program structure is designed to mitigate these risks by allowing for engagement at various stages throughout the program and associated project lifecycles, enabling the projects to be selected and adapted to the best available information and resources within industry.

Risk #	Risk Category	Description	Inherent Risk Level	Mitigation Plan	Residual Risk level
01	Key Resources	Key resources not available to assist in design of future state or in testing the end product.	Medium	Plan and ensure that resources are available or that resources are backfilled.	Low
02	New Technology	If new technology is being introduced as part of this upgrade, the skillset might not be there to sufficiently support it after the program of work has completed.	Medium	Plan and ensure that skillset is developed to ensure that technology can be supported in the future.	Low
03	Scope Expansion	Expectation that the scope might include features that were not originally planned for might extend the timeline of the project.	Medium	Set scope expectations early on and define boundaries. If additional requirements arise, scope will be discussed through the appropriate investment governance mechanism.	Low
04	Costs	Project Costs are estimated based upon market knowledge in FY22 and costs could increase as the projects are executed in FY25-29.	Medium	Undertake Gate 3 Business Cases prior to executing each project within the program and revise costs with costs at the time of execution.	Low
05	Key Resources	Availability of SME resources within local market - After effects of the COVID19 pandemic have caused a skill shortage locally and specialist resources may not be readily available.	Medium	Define resource requirements early and leverage existing relationships with strategic partners where the required skills cannot be found internally within the organisation.	Low

5.4. Program assumptions

The key assumption is that project selection will remain dynamic prior to and throughout the FY25-29 period.

#	Type	Description
01	Resourcing	Appropriate resources will be sourced and available to deliver the selected projects. Specialist resources will also be identified to maintain the OT security functionality in a business-as-usual context.
02	Commitment	Ausgrid Distribution Licence Conditions have specific requirements for OT, including the use of 'best practice', which will persist for the foreseeable future. Subsequently business focus will remain on delivering the identified projects
03	Priority	Moderate to High
04	Scope	Projects will continue to be evaluated and reprioritised based on at a least an annual planning cycle to achieve the greatest risk reduction from investment in each project as part of the overall program. Each potential project is assessed against the core Industrial Control System Security Standards to determine if it aligns to industry direction and 'best practice' to support existing compliance requirements as part of Ausgrid's licence conditions [REDACTED]
05	Threats	External threats will continue to increase as described in recent announcements from the Australian Cyber Security Centre (ACSC).

5.5. Program dependencies

A number of currently selected projects in the program require modern integrations to core Ausgrid IT and OT systems. A program dependency is that these systems remain available to successfully complete the projects and leverage inherent functionality in these systems to avoid additional activities to replicate functionality.

5.6. Business area impacts

[REDACTED]

[REDACTED]

APPENDIX A: PROPOSED OT SECURITY PROJECTS FOR 2025-29

The following table summarises the OT security projects Ausgrid proposes to undertake in the 2024-29 period.

OT Security Program Workstream	Project	2025-29 ⁸ Capex (\$m)	Recurring?	Option 1	Option 2	Option 3 (Preferred)	Option 4

⁸ Refers to the expenditure for the preferred option 3.

APPENDIX B: APPROACH TO QUANTIFICATION OF PROJECT BENEFITS

Ausgrid has identified three 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 (loss of OPEX productivity and loss of CAPEX productivity)	<p>Direct improvements in the operations and / or services supplied by Ausgrid as a result of an investment. These benefits are typically reflected in avoided time reacting to an event or equivalent reduced costs (efficiencies), such as direct cost savings for Ausgrid.</p> <p>These costs will be passed on to customers in the longer term through reduced costs for energy.</p>	<ul style="list-style-type: none"> Cost savings are quantified through cost build up (e.g. hours of labour saved <i>times</i> average cost of labour per hour). These costs saved or inefficiencies avoided are quantified in monetary terms were related to a direct event causing this cost. The likelihood of an event considers the likelihood of a malicious actor succeeding in penetrating through the layers of defence in the OT systems. This is calculated as the multiplication of the likelihood of passing each defence from the point of entry.
Reduced capital required to replace damaged equipment (avoided capex)	The cost avoided if a malicious actor were to succeed in gaining control inside the OT environment and damaging hardware or irrevocably changing the hardware into an inoperable state	<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 event (%) multiplied by the consequence of the event (\$) The likelihood of an event considers the change in likelihood of a malicious actor succeeding in penetrating through the layers of defence in the OT systems following an investment. This is calculated as the multiplication of the new likelihood minus the old likelihood of passing each defence from the point of entry.
Customer benefit related to avoided unserved energy	The customer impact from a supply of electricity interruption for a particular duration as a result of a OT security breach and the acts of that malicious actor.	<ul style="list-style-type: none"> The consequence is calculated as the loss of supply, which is measured using an estimate of the unserved energy and the value of customer reliability (VCR) for Ausgrid's distribution area. I.e. multiplying the value of customer reliability by the duration of the supply interruption and the number of customers without supply for each scenario.

APPENDIX C – INDUSTRY BEST PRACTICE FOR OPERATIONAL TECHNOLOGY

Purpose

This appendix outlines the recent history regarding the cyber security uplift to Ausgrid's Operational Technology (OT) domain, including a summary of obligations and background to the introduction of the Critical Infrastructure Licence Conditions, the Critical Infrastructure Act 2018 and associated implications to Ausgrid's Operational Technology environment. This document also outlines Ausgrid's interpretation of 'best industry practice for electricity network control systems' as referenced in Ausgrid's Licence Conditions.

Background

The industrial control systems within the electrical network industry, known as OT, are defined as the application of information technology systems for the purpose of directly operating or managing devices on the electricity network, including the integration of remote devices (field and substation) with supervisory control and data acquisition (SCADA) systems using communications links to provide a platform that is used to monitor and operate the underlying asset.

It includes any hardware or software which detects or causes a change to network operation through the direct monitoring and/or control of physical devices, processes and events in the distribution system. This is often referred to as the 'cranking path' by practitioners in determining what action could related to a change in the configured electricity network state.

Historically, industrial control systems utilised specialised, bespoke hardware and dedicated communication channels. However, in the last 25 years, SCADA systems have moved away from bespoke hardware to utilising similar or identical Information Technology (IT) platforms. These platforms provide improved functionality, flexibility and redundancy for lower cost, however, require different skills and capability to manage. Importantly these systems share some security vulnerabilities that can affect corporate IT systems that bespoke industrial systems were not exposed to historically. Management of these security vulnerabilities in the OT environment is a fast-evolving area and has become a significant focus of utilities and governments around the world.

Challenges of OT/IT Convergence

The term OT/IT convergence reflects patterns of similarity between the two environments. There are two common industry trends that are reflective of OT/IT convergence but are quite different in their impacts on cyber security. The first is the use of IT hardware systems within the OT environment. As systems rely on more commonplace technologies, we witness OT hardware being similar to that which is employed in the IT space. The systems might appear the same but have quite different purpose and function. The second trend is business enablement which sees the controlled interaction between OT and IT systems to support operational activities and business insight.

Whilst the benefits of this convergence exist, there remain a number of important differences in the architecture, configuration and purpose between the two domains. Traditional IT security objectives (heavily influenced by the banking and financial sectors) typically follow the priorities of confidentiality, integrity and availability. In the case of control systems, and particularly electricity networks, the consequences of a security breach are very different and therefore the priorities are different.

The combined importance of safety, availability and integrity within an OT system mean that nothing must be done on the active control system network that would interfere or disrupt the time-critical operations of the system where there are potentially adverse safety outcomes. In the control systems environment, the security objectives of the IT world are replaced by human health and safety, availability of the system, and timeliness and integrity of the data.

Table 1 illustrates the key differences in the priority of various system objectives and the key consequences from the loss of system function from a cyber security intrusion. This is exaggerated by

the difference in non-time critical applications/systems compared to those with time criticality with direct implications to people and infrastructure.

Table 1 - IT / OT Cyber Security Differences

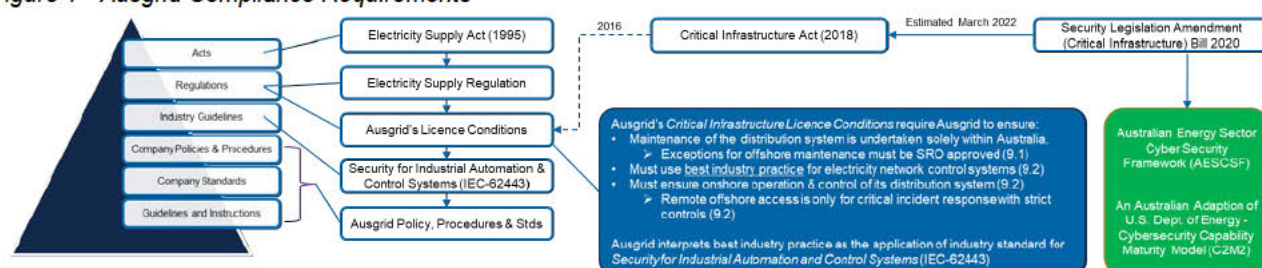
IT / OT Cyber Differences	Operational Technology	Information Technology
Objectives: Information & Operational Technology systems and processes have differing objectives given their differing purposes	Objectives by priority 1. System Availability 2. System Integrity 3. Information Confidentiality	Objectives by priority 1. Information Confidentiality 2. System Integrity 3. System Availability
Consequences: The criticality and type of realised consequences differ between information and operational systems for a failure or potential cyber intrusion.	<ul style="list-style-type: none"> Power Outages Damage to Assets Injury / Death Secondary impacts: <ul style="list-style-type: none"> Reputational Damage Regulatory Fines Work Cover Investigations Court actions and/or Coroner's court directions 	<ul style="list-style-type: none"> Loss of Privacy Loss of Productivity Financial Loss Reputational Damage Loss of Data Regulatory Fines Court Actions

Due to these differences, while the OT and IT domains often use similar or identical technology, differences in focus between the two domains drives the need for specific industry-aligned approaches appropriate to cyber security for the OT domain.

Ausgrid's Regulatory Environment

Ausgrid operates in a highly regulated environment. Ausgrid's cyber security governance, at a high level, is shown below in Figure 1.

Figure 1 - Ausgrid Compliance Requirements



Ausgrid's Critical Infrastructure Licence Conditions

Ausgrid has key obligations in its Distributor's Licence to operate a distribution system under the Electricity Supply Act 1995 (NSW). The NSW Minister for Industry, Resources and Energy grants the distribution licence under section 14 of the Electricity Supply Act 1995 (NSW). The Minister also imposes on Ausgrid a schedule of Licence Conditions for the Operator (Ausgrid) of a Transacted Distribution System.

On 1 December 2016 Ausgrid transitioned to a 50.4% long term lease with private ownership. As part of the lease transaction, the NSW Minister updated the schedule of Licence Conditions for the Operator (Ausgrid).

A key change at this point in time was the introduction of additional 'Critical Infrastructure Licence Conditions' (Conditions 9, 10 and 11). These requirements describe the significance of infrastructure being managed by Ausgrid, as described in the excerpt below:

CRITICAL INFRASTRUCTURE LICENCE CONDITIONS

... the assets which the Licence Holder operates may constitute "critical infrastructure" being those physical facilities, supply chains, information technologies and communication networks which, if destroyed, degraded or rendered unavailable for an extended period, would significantly impact on the security, social or economic wellbeing of the State of New South Wales ... These licence conditions will be reviewed by the Minister from time to time (and where necessary) in consultation with responsible Ministers of the Commonwealth ...

The Critical Infrastructure Licence Conditions included in the schedule of Licence Conditions were developed by NSW Government and Commonwealth agencies. This review included Foreign Investment Review of the Licence Condition provisions. The licence conditions require a:

- Substantial presence must be held in Australia and prevent operation or control of the control systems or the supporting ICT from outside of Australia (Condition 9); and
- Data Security must be maintained that prevents access to operational technology, ICT or bulk load and customer information from outside of Australia or from unauthorised persons (Condition 10).

Condition 9 contains clear requirements for Ausgrid to use industry best practice. As industry best practices are evolving, Ausgrid interprets best industry practice in a manner consistent with industry participants, such as AEMO. This includes adoption of a hierarchy of industry standards, guidelines and advice as outlined in Table 2 – *Hierarchy of reference material representing industry best practice*, and the best practice reference list attached in Appendix 1.

Condition 9 also recognised that compliance with the requirements involved a significant uplift in the Cyber Security capabilities of the OT domain. This condition allowed for a ministerially approved implementation plan that provided a 12 month program of works to uplift the OT infrastructure, capability, policies and procedures. Ausgrid's implementation plan focused on key areas including:

- Control System Isolation and Segregation;
- Control System Distribution Network Management System Improvements;
- Control System Security Architecture; and
- Security Information and Event Management (**SIEM**).

The implementation plan required an investment of around \$10m in 2017 to achieve the required uplift in the infrastructure, capability, policies and procedures in the OT domain.

In the last regulatory period, Ausgrid has continued to uplift the maturity of OT security to further align with Licence Conditions requirement to use best industry practice. An annual plan is developed to maintain compliance in line with the evolving frontier of industry best practice. Ausgrid consults with industry participants and bodies continuously and incorporates feedback into each annual planning cycle.

Ausgrid's Critical Infrastructure Licence Conditions were revised and re-issued in December 2017 following the first IPART audit against the conditions in 2017, and subsequent detailed engagement with IPART, the NSW Minister for Industry, Resources and Energy, and relevant Commonwealth agencies.

The key revisions to the Critical Infrastructure Licence Conditions were:

- Introduction of the Remote Access Protocol; and
- Adjustment of Data Security requirements and definitions.

The Remote Access Protocol was originally developed and agreed between the Commonwealth Representative and Ausgrid and was based on the CERT – ICS Remote Access Protocol⁹. Ausgrid Specific adaptations have been identified and agreed in the ‘Ausgrid Industrial Control System Remote Access Protocol Agreement’ agreed in June 2022.

The CERT – ICS Remote Access Protocol was developed to allow specific external parties (vendors) to securely remotely connect to critical infrastructure control networks. This includes design principles for the technology to enable secure remote access, implementation principles to provide guidance on approaches for satisfying the design principles and the specified protocol, or procedure, for remote access.

Further work has been undertaken between Ausgrid and the Commonwealth agencies to refine the required Remote Access Protocol for Ausgrid and significant work has been undertaken to commence deployment of this capability.

Critical Infrastructure Act 2018 and Amendments in 2021 and 2022

The Security of Critical Infrastructure Act 2018 commenced in July 2018, to provide a framework for managing risks to national security relating to critical infrastructure through:

- improving the transparency of the ownership and operational control of critical infrastructure in Australia in order to better understand those risks; and
- facilitating cooperation and collaboration between all levels of government, and regulators, owners and operators of critical infrastructure, in order to identify and manage those risks.

A critical Infrastructure asset is defined to include critical electricity assets, which are defined broadly to include a network, system, or interconnector, for the transmission or distribution of electricity. Ausgrid’s distribution system is a critical electricity asset and its entire network is captured by the definition within the Act.

The Act includes powers of direction and information provision.

The Critical Infrastructure Centre has been formed to administer the Act and carry out the following high-level activities:

- Conduct national security risk assessments to support the Foreign Investment Review Board;
- Develop and implement targeted mitigations in concert with industry, states and territories; and
- Develop improved best practice guides for industry.

Ausgrid has closely engaged with the Critical Infrastructure Centre during the development of the Act, the 2017 revision to the Ministerial Distributor’s Licence Conditions and the Advanced Distribution Management System (**ADMS**) project. All of these engagements have informed and refined Ausgrid’s understanding of what constitutes industry best practice for electricity network control systems.

This engagement has continued with the energy sector co-design working groups and the proposed Security Legislation Amendment (Critical Infrastructure) Bill 2021. The aim of the Bill is to provide a framework for managing risks to national security relating to critical infrastructure. On advice from the Parliamentary Joint Committee on Intelligence and Security (**PJCIS**) in September 2021, this bill was broken into two complimentary smaller bills to pass in sequence. The first bill aims to support Govt involvement and intervention in the event of a major cyber incident affecting critical infrastructure. The second is responsible for guiding the security and resilience uplift among identified operators of critical infrastructure and national significance.

During Energy Sector co-design working groups for the Critical Infrastructure Bill (2021), the use of Australian Energy Sector Cyber Security Framework (**AESCSF**) or other equivalent standard to drive the intended risk management framework was well supported by the Energy Sector participants. While not accurately reflected in the first Bill and associated rules, Commonwealth agencies have indicated that there is an appetite to introduce requirements for Critical Infrastructure Operators to comply with AESCSF SP-2 and SP-3 requirements at a future time likely inside the 2025-29 regulatory period. It is expected this will be in the form of the rules associated with this second bill.

⁹ https://www.cert.gov.au/sites/g/files/net3281/f/remote_access_protocol.pdf

Ausgrid is uplifting the OT Cyber governance framework to align to AESCSF SP-2 and SP-3 capability and maturity where there is demonstrable value in doing so.

In support of this approach is the Risk Management Program Rules provided with the Bill, including the requirement to identify and mitigate the risks and hazards associated with a cyber attack resulting in prolonged outages to the electrical network. These various risks are to be managed in accordance with industry best practise.

Industry Best Practice

In 2016 Ausgrid developed an OT / Control System Security Strategy which was further refined with the introduction of the Critical Infrastructure Licence Conditions and its subsequent revision. This strategy has informed the Operational Technology Security approach and the cyber security program.

This strategy references current good and best practice in SCADA systems and, where applicable, IT Cyber Security practices from the following key reference material outlined in the best practice reference list attached in Appendix 2. This approach is in alignment with Ausgrid's obligations under Critical Infrastructure Licence Condition 9.2.

A hierarchy of reference material has been developed with the most relevant and authoritative source being IEC-62443 – Security for Industrial Automation and Control Systems as depicted in Table 2 – *Hierarchy of reference material representing industry best practice*. In cases where the primary reference offers no (or insufficient) guidance, secondary and more detailed reference materials are utilised.

In addition to using IEC-62443, Ausgrid has adopted the use of the Australian Energy Sector Cyber Security Framework (AESCSF) to assist in assessing Ausgrid's OT cyber security capability and maturity and identifying further areas for improvement.

Table 2 – *Hierarchy of reference material representing industry best practice*

Hierarchy of Preferred Best Practice Standards	Applicable Standard
Primary Reference Standards <ul style="list-style-type: none"> International standard for control systems Widely accepted across energy sector to protect critical infrastructure from cyber threats 	IEC-62443 – Security for Industrial Automation and Control Systems
Governance framework standard	Australian Energy Sector Cyber Security Framework (AESCSF).
Secondary Reference Standards <ul style="list-style-type: none"> Authoritative (US Government) guide for control systems 	NIST SP800-82 – Guide to Industrial Control Systems (ICS) Security
Detailed References <ul style="list-style-type: none"> Authoritative Government guide for specific issues and where relevant vendor recommendations 	Generic Cyber Security Government Guides and Standards <ul style="list-style-type: none"> NIST Special Publications ASD Strategies & Guidance Vendor Recommendations <ul style="list-style-type: none"> Recommended configurations Reference architectures Support notices

Note, the above list represents a current view of industry OT cyber best practice and will be refined as the cyber threat landscape continues to evolve and industry and general cyber security best practice changes. In support of continuous improvement and supported by IEC62443 standard, Ausgrid will

continue to monitor and update this reference list during the periodic review of policy, procedures and standards.

APPENDIX D – BEST PRACTICE IN OT – REFERENCE STANDARDS

International		
ISA	International Society for Automation	<ul style="list-style-type: none"> TR99.00 01-2007 Security Technologies for Industrial Automation and Control Systems, TR99.00 02-2004 Integrating Electronic Security Into The Manufacturing And Control Systems Environment
IEC	International Electrotechnical Commission	<ul style="list-style-type: none"> 62443-1-1 Security for Industrial Automation and Control Systems – Models and Concepts, formerly ISA-TR99.00.01 IEC 62351 (TC57, WG15) – Security standards for the power system information infrastructure
ISO	International Organization for Standardization	<ul style="list-style-type: none"> Common Criteria for Information Technology Security Evaluation
Australia		
ASD	Australian Signals Directorate Formerly Defence Signals Directorate (DSD)	<ul style="list-style-type: none"> Strategies to Mitigate Targeted Cyber Intrusions ASD Top 35 Mitigation Strategies ASD Top 4 extending to the Essential 8 CERT – Industrial Control System Remote Access Protocol
AEMO	Australian Energy Market Operator	<ul style="list-style-type: none"> Australian Energy Sector Cyber Security Framework (AESCSF).
TISN	Trusted Information Sharing Network	<ul style="list-style-type: none"> Generic SCADA Risk Management Framework For Australian Critical Infrastructure Risk Management for Industrial Control Systems (ICS) And Supervisory Control Systems (SCADA) Information For Senior Executives SCADA Security Good Practice Guide - Hardening of SCADA ICT Systems
AGD	Attorney Generals Department	<ul style="list-style-type: none"> Critical Infrastructure and Protective Security Policy
	Edith Cowan University Research Online	<ul style="list-style-type: none"> Safeguarding Australia from Cyber-terrorism: A Proposed Cyber-terrorism SCADA Risk Framework for Industry Adoption
United States of America		
NERC	North American Electric Reliability Corporation	<ul style="list-style-type: none"> NERC-1200 - North American Electric Reliability Corporation Cyber Security Standards NERC 1300 – Cyber Security <ul style="list-style-type: none"> C P-002 –Critical Cyber Assets C P-003 –Security Management Controls C P-004 –Personnel and Training C P-005 –Electronic Security C P-006 –Physical Security C P-007 –Systems Security Management C P-008 –Incident Reporting & Response Management C P-009 –Recovery Plans
NIST	National Institute of Standards and Technology	<ul style="list-style-type: none"> SP 800-82, Guide to Industrial Control Systems (ICS) Security SP 800-77, Guide to Psec VPNs SP 800-30, Risk Management Guide for Information Technology Systems SP 800-40, Creating a Patch and Vulnerability Management Program
SANS	SANS Institute - Escal Institute Of Advanced Technologies, Inc	<ul style="list-style-type: none"> Security for Critical Infrastructure SCADA Systems
DOE	U.S Department of Energy	<ul style="list-style-type: none"> 21 Steps to Improve Cyber Security of SCADA Networks Lessons Learned from Cyber Security Assessments of SCADA and Energy Management Systems The Department of Energy (DOE) developed the Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)
DHS	U.S. Department of Homeland Security	<ul style="list-style-type: none"> Recommended Practice: Improving Industrial Control Systems Cybersecurity with Defence-In-Depth Strategies Good Practice Guide: Cyber Security Assessments of Industrial Control Systems
DISA	Defense Information Systems Agency	<ul style="list-style-type: none"> The Security Technical Implementation Guides (STIGs)
CIS	Center for Internet Security	<ul style="list-style-type: none"> Cyber Security Procurement Language for Control Systems
EEI	Edison Electric Institute	<ul style="list-style-type: none"> Patch management strategies for the Electric Sector
United Kingdom		
CPNI	Centre for the Protection of National Infrastructure	<ul style="list-style-type: none"> Good Practice Guide on Patch Management Configuring and Managing Remote Access for Industrial Control Systems Cyber security assessments of industrial control systems Process control and SCADA security - General Guidance Firewall deployment for SCADA and process control networks Process Control and SCADA Security Guides 1- 7