Cyber Security Baseline

Regulatory Business Case (RBC) 2024-29

PowerWater

Contents

1. Summary

This business case has been prepared to support the 2024-29 Regulatory Proposal. The business case demonstrates that Power and Water has undertaken appropriate analysis of the need and identified a full suite of credible options that will resolve the need, to ensure that Power and Water continues to meet the National Electricity Objectives and manage the network prudently and efficiently.

The proposed expenditure identified in this business case will undergo further assessment and scrutiny through Power and Water's normal governance processes prior to implementation and delivery.

This business case addresses the risks posed by unauthorised access to sensitive information and systems and that operate essential service networks and as such Power and Water needs to protect them from illegal access.

1.1 Business need

Power and Water's cyber security maturity is not adequate to comply with the obligations under the amended Critical Infrastructure Act nor robust enough in the face of the worsening cyber-attack landscape. This business case supports achievement of Security Profile level 2 (per the Australian Energy Sector Cyber Security Framework, 'AESCSF') by the end of the 2024-29 regulatory control period ('the next RCP').

1.1.1 Worsening cyber security threat landscape

The cyber security threat landscape has worsened over the last few years as evidenced by recent cyber-attacks on Optus and Medibank Private[1] and by the latest report by the Australian Cyber Security Centre (ACSC), in which it states it received 76,000 cybercrime reports last financial year, up 13% from the previous period.[2] The ACSC reports that state actors continued to engage in malicious cyber operations:[3]

- *'Russia's invasion of Ukraine has increased the cyber threat globally*
- *Malicious state actors continue to seek sensitive information, including by targeting Australian small businesses and individuals.*
- *Most compromises identified by the ACSC used relatively simple tradecraft which could have been prevented by enhanced cyber security.'*

1.1.2 Amendments to the Security of Critical Infrastructure Act

As observed by the ACSC:

> *'The consequences of a prolonged and widespread failure in the energy sector, for example, could be catastrophic to our economy, security and sovereignty, as well as the Australian way of life…'*[4]

During 2021–22, the ACSC received 95 cyber incidents affecting critical infrastructure.

Recognising the increased threat of cyber-attacks, the Australian government introduced the Security Legislation Amendment (Critical Infrastructure) Act 2021 (SLACI Act) on 2 December 2021 which amended

[1] Reuters.com/world/asia-pacific/Australia - 5 Nov 2022

[2] ACSC, Annual Cyber Threat Report, 2022

[3] *Ibid*

[4] *Ibid,* page 51

the SOCI Act. Since the implementation of the amendments in April 2022, the ACSC has notified 5 critical infrastructure entities of cyber incidents and vulnerabilities on their networks.

The reforms introduce a Positive Security Obligation[5] and Systems of National Significance (SoNS). SoNS are a small subset of critical infrastructure assets that are most crucial to the nation, by virtue of their interdependencies across sectors and potential for cascading consequences to other critical infrastructure assets and sectors if disrupted. SoNS are subject to enhanced cyber security obligations (ESCO).[6]

1.1.3 SP-2 is likely to be the prudent cyber security level for Power and Water

Given the range and nature of Power and Water's services, localities and customer base, combined with the guidance from the AESCSF that medium criticality network service providers should be operating with Security Profile level 2 ('SP-2')[7] and considering the practices required to be in place to achieve SP-2, it is clear that the minimum target for Power and Water should be SP-2 within the next RCP.

1.1.4 Power and Water's current cyber security maturity

The inputs in assessing Power and Water's cyber security strategy include:

- Self-assessed coverage and maturity against AESCSF and C2M2[8]
- Ernst and Young SCADA Security Review against AESCSF, ISA/IEC 62443[9] and ISO27001:2013[10]
- An internal audit of Power and Water's cyber security practices
- Cross-referencing and consolidating the above against NIST[11] and the AESCSF framework for SP-1 and SP-2[12] to identify key practices which require uplift and to what level to address the above obligations and risks
- Sequencing and timing informed by the DRAFT Risk Management Program Guidance for the Security of Critical Infrastructure Act 2018 Reforms.
- InfoTech.com Security Pressure, Security Requirements and Security Program Gap Analysis.

Power and Water intends to use the AESCSF framework as its anchor model and cyber risk management framework for all cyber risk-related investment planning. The other frameworks and standards that offer guidance on how to implement these elements will also be used and aligned to AESCSF, including NIST and relevant ISO standards for IT, IoT, and OT.

[5] Extends the provision of information for the Register of Critical Infrastructure Assets for entities not previously captured by the SOCI Act and mandatory cyber incident reporting.

[6] Part 2C of the SOCI Act

[7] The AESCSF has been updated with the emphasis on Security Profiles SP-1, SP-2, SP-3 (with the latter being the highest level) rather than the previous version's emphasis on Maturity Indicator Level (MIL-1, MIL-2, MIL-3) although they are similar

[8] Cyber Maturity Capability Maturity Model produced by the US Department of Energy

[9] The ISA/IEC 62443 series of standards define requirements and processes for implementing and maintaining electronically secure industrial automation and control systems (IACS)

[10] ISO/IEC 27001 – Information technology — Security techniques — Information security management systems — Requirements which is a part of a set of internationally recognised ISO-27000 standards for managing information security

[11] National Institute of Standards and Technology which is part of the US Department of Commerce

[12] Security Profile 1 is the lowest level of cyber security maturity in the AESCSF and represents achievement of 88 practices and anti-patterns; SP-2 is the next of three levels and is attained if 200 specified practices and anti-patterns are achieved

Power and Water's current cyber security maturity level has been assessed at [redacted] The combination of the increased cyber threat landscape, the obligations under the amended Security of Critical Infrastructure Act ('SOCI Act') and associated Bills, and Power and Water's current cyber security maturity level, makes it clear that Power and Water's overall IT and OT cyber security posture is well short of the required level.

1.1.5 Cyber security strategy

Given Power and Water's low cyber security maturity level and its capacity to undertake the necessary work required to achieve SP-2,[14] the strategy is based on a staged approach to across three sets of progressively comprehensive cyber initiatives as shown below:

- Foundations and Framework - in line with the ACSC Priority Practices set within 6 months (i.e. by mid-2023)
- AESCSF SP-1 - within 12 months of the Foundations (i.e. by the end of FY24)
- AESCSF SP-2 - within 42 months of achieving SP-1.

A set of 18 initiatives has been designed and prioritised and sequenced to progressively achieve the required practices. All initiatives are mapped directly to the practices and anti-patterns within the AESCSF for clarity of intent and outcome as part of the overall structure of the associated Risk Management Program for Cyber Security as required under the SOCI Act reforms.

1.2 Options analysis

Three options have been considered for achieving SP-2 maturity level within the next RCP. The common features of the options are:

- The maturity level target by the end of the next RCP is SP-2
- Maturity Level SP-1 is required to be achieved within 18 months of the Risk Management Program Rules[15] commencing - which is assumed to be January 2023
- It may be prudent and efficient for Power and Water to implement some of the 88 SP-3 practices due to emerging risks throughout the course of the project lifecycle , however no contingency amount has been allowed for SP-3 practices
- Given the activities required to achieve SP-1 and SP-2, and the variability of the nature of the solutions covering people, process, information and technology, the options are described in terms of overall approach; the individual solutions (resources, products and services) will be refined during the detailed design and implementation phases of the project lifecycle; each initiative will be subject to Power and Water's standard investment governance process.

1.2.1 Option 1: Blended resource model to achieve SP-2

Option 1 is based on prioritising or targeting investments to address the highest risks first, using a combination of internal and external resources. Necessary investments in new or enhanced technology will be used to optimise the delivery-risk (schedule and cost) for the project. The project is expected to be completed in FY29 at a cost of $28.3 million (totex, whole of business).

[13] Ernst and Young, OT review for Cyber capabilities, 2022

[14] Which involves achieving *and* sustaining 200 practices and anti-patterns

[15] Australian Department of Home Affairs, and CISC, Draft Risk Management Program Rules, Rule 1, page 7

The main differences between Option 1 and the other two options is the resource and technology assumptions. Option 1 appropriately balances risk and cost – it is deliverable cognisant of (i) the competition for scarce internal subject matter experts and experienced external resources, (ii) the cost of external resources, and (iii) the benefits of using new technology to avoid operational cost and risk.

1.2.2 Option 2: Internal resource model to achieve SP-2

The key differentiators of Option 2 are (i) reliance on recruiting people with the requisite skill sets, and (ii) minimal or no new infrastructure, software or supporting technology.

Whilst this option may be less expensive than the preferred Option 1, it is unlikely to be achievable because of (i) the challenges with recruiting and retaining the suitable skills, and (ii) the limited capability of current platforms required to implement the initiatives necessary to achieve SP-1 by the end of the current RCP and achieve SP-2 by no later than the end of the next RCP.

1.2.3 Option 3: Fully out-source to achieve SP-2

The key differentiator of Option 3 is the use of external resources to deliver the initiatives, including project management. Project governance, procurement and contract management would be undertaken by Power and Water. This option is not preferred due to the cost and risk.

1.2.4 Summary of credible options

Table 1: Summary of credible options

Option No.	Option name	Description	Recommended
1	Blended resource model to achieve SP-2	Under this model we will recruit a limited number of internal resources, train selected existing internal resources, and supplement the internal team with external resources. We will utilise tools that will assist in finding network vulnerabilities.	**Yes**
2	Internal resource model to achieve SP-2	Additional recruitment to enable all capability improvements to be achieved with existing technologies. No or minimal new infrastructure, software or supporting technology.	No
3	Fully out-source to achieve SP-2	Seek to out-source operational elements whilst maintaining in-sourced governance across the processes in scope. Heavy use of security services, with positive vetting of compliance required by internal resources.	No

The table below summarises the option analysis parameters and outcomes of the analysis.

1.3 Recommendation

Option 1 - Blended resource model to achieve SP-2, is the recommended option at a total estimated cost of $28.3 million (real 2021/22) across IT and OT domains. The project commences in the current regulatory period with an estimated cost of $6.21 million to achieve SP-1 and continues into the next regulatory period to achieve SP-2 at an estimated cost of $22.10 million to achieve SP-2.

Option 1 is the only option which provides the flexibility to address emergent risks, accept and offset the resourcing challenges for Power and Water, provide an acceptably low delivery risk, and ensure coverage of IT and OT to incrementally establish, operate, mature and sustain SP-2 levels of performance.

The estimated and forecast expenditure by regulatory period is outlined in Table 2.

Table 2: Estimated and forecast capital and operational expenditure – by regulatory period ($m, real 2021/22)

Item	Current regulatory period FY20 - FY24	Next regulatory period FY25 – FY29	Total
Capex	3.65	13.00	16.65
Opex	2.56	9.1	11.66
Total	**6.21**	**22.10**	**28.31**

The estimated and forecast expenditure by regulatory period that has been allocated to Standard Control Services as per the CAM is outlined in Table 3.

Table 3: Estimated and forecast capital and operational expenditure – allocated to SCS ($m, real 2021/22)

Item	Current regulatory period FY20 - FY24	Next regulatory period FY25 – FY29	Total
Capex	2.85	10.16	13.02
Opex	1.27	4.51	5.78
Total	**4.12**	**14.67**	**18.80**

The estimated and forecast expenditure by regulatory period that has been allocated to recurrent and non-recurrent categories is outlined in Table 4.

Table 4: Estimated and forecast capital expenditure – recurrent and non-recurrent ($m, real 2021/22)

Item	Current regulatory period FY20 - FY24	Next regulatory period FY25 – FY29
Recurrent	0%	35%
Non-recurrent	100%	65%

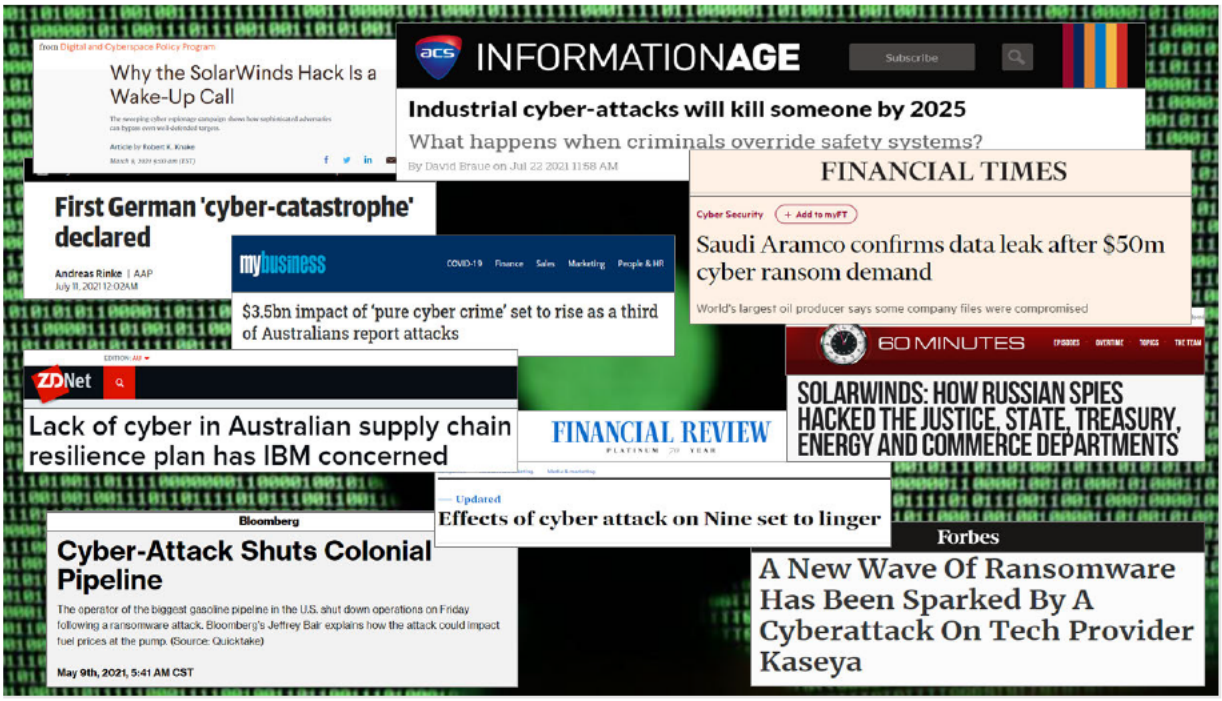
2. Identified need

This section provides the background and context to this business case, identifies the issues that are posing increasing risks to Power and Water and its customers, describes the current mitigation program and its delivery status, and provides a risk assessment of the inherent risk if no investment is undertaken.

2.1 Critical infrastructure trends

All Australians rely on critical infrastructure to deliver essential services that are crucial to our economic prosperity, including electricity. Critical infrastructure is increasingly interconnected and interdependent. The ACSC reports that in the 2021–22 financial year, 95 cyber incidents affected critical infrastructure and that in the six months since April 2022, the ACSC has notified five critical infrastructure entities of cyber incidents and vulnerabilities on their networks.[16] Figure 1 below shows recent headlines from around the world and Australia which anecdotally support the position that the cyber-attack threat landscape is worsening. The ACSC further notes in its Annual Cyber Threat Report, 2022 that *'globally, critical infrastructure has been increasingly targeted by malicious actors.'* Two successful attacks of Optus and Medibank Private in Australia within the last few months have reinforced this position.

Figure 1 - The threat landscape is continuously evolving, with increased severity and frequency across government and utilities



from Digital and Cyberspace Policy Program

Why the SolarWinds Hack Is a Wake-Up Call

The sweeping cyber espionage campaign shows how sophisticated adversaries can bypass even well-defended targets.

Article by Robert K. Knake

March 8, 2021 6:50 am (EST)

INFORMATIONAGE

Industrial cyber-attacks will kill someone by 2025

What happens when criminals override safety systems?

By David Braue on Jul 22 2021 11:58 AM

FINANCIAL TIMES

Cyber Security

Saudi Aramco confirms data leak after $50m cyber ransom demand

World's largest oil producer says some company files were compromised

First German 'cyber-catastrophe' declared

Andreas Rinke | AAP

July 11, 2021 12:02AM

mybusiness

$3.5bn impact of 'pure cyber crime' set to rise as a third of Australians report attacks

60 MINUTES

SOLARWINDS: HOW RUSSIAN SPIES HACKED THE JUSTICE, STATE, TREASURY, ENERGY AND COMMERCE DEPARTMENTS

ZDNet

Lack of cyber in Australian supply chain resilience plan has IBM concerned

FINANCIAL REVIEW

Updated

Effects of cyber attack on Nine set to linger

Bloomberg

Cyber-Attack Shuts Colonial Pipeline

The operator of the biggest gasoline pipeline in the U.S. shut down operations on Friday following a ransomware attack. Bloomberg's Jeffrey Bair explains how the attack could impact fuel prices at the pump. (Source: Quicktake)

May 9th, 2021, 5:41 AM CST

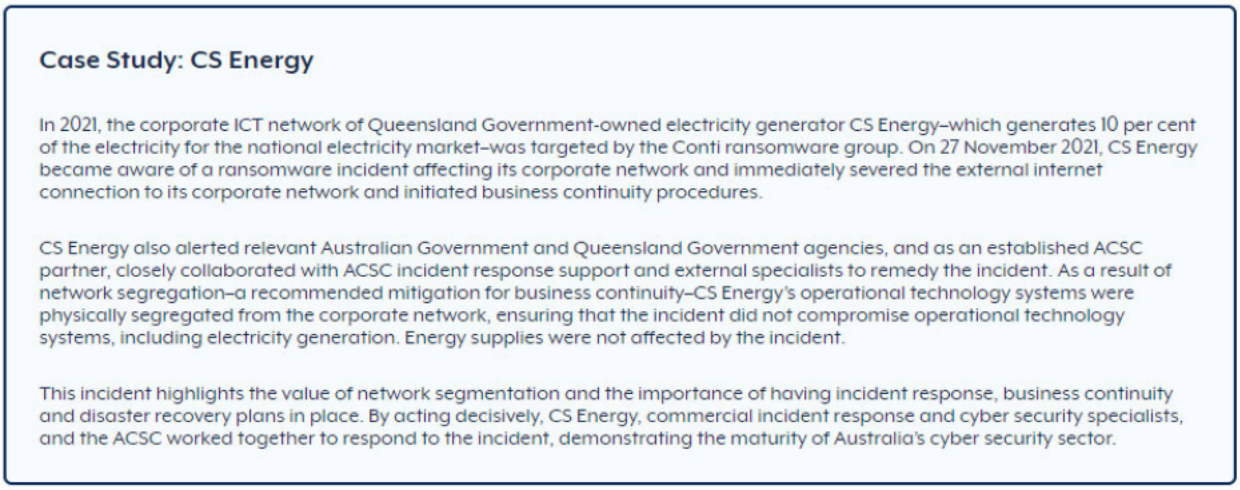
Forbes

A New Wave Of Ransomware Has Been Sparked By A Cyberattack On Tech Provider Kaseya

The ACSC's annual report also includes the case study included in the figure below of a cyber-attack on CS Energy.

[16] ACSC Annual Cyber Threat Report 2022

Figure 2 – Case study : CS Energy



Case Study: CS Energy

In 2021, the corporate ICT network of Queensland Government-owned electricity generator CS Energy–which generates 10 per cent of the electricity for the national electricity market–was targeted by the Conti ransomware group. On 27 November 2021, CS Energy became aware of a ransomware incident affecting its corporate network and immediately severed the external internet connection to its corporate network and initiated business continuity procedures.

CS Energy also alerted relevant Australian Government and Queensland Government agencies, and as an established ACSC partner, closely collaborated with ACSC incident response support and external specialists to remedy the incident. As a result of network segregation–a recommended mitigation for business continuity–CS Energy's operational technology systems were physically segregated from the corporate network, ensuring that the incident did not compromise operational technology systems, including electricity generation. Energy supplies were not affected by the incident.

This incident highlights the value of network segmentation and the importance of having incident response, business continuity and disaster recovery plans in place. By acting decisively, CS Energy, commercial incident response and cyber security specialists, and the ACSC worked together to respond to the incident, demonstrating the maturity of Australia's cyber security sector.

The ACSC identified the following key cyber security trends in the 2021–22 financial year:[17]

> **'Cyberspace has become a battleground –** *cyber is increasingly the domain of warfare, as seen in Russia's use of malware designed to destroy data and prevent computers from booting in Ukraine….In July 2021, the Australian Government publicly attributed exploitation of Microsoft Exchange vulnerabilities to China's Ministry of State Security… Regional dynamics in the Indo-Pacific are increasing the risk of crisis and cyber operations are likely to be used by states to challenge the sovereignty of others.*
>
> **Australia's prosperity is attractive to cybercriminals** - *In 2021–22, cybercrimes directed at individuals, such as online banking and shopping compromise, remained among the most common, while Business Email Compromise (BEC) trended towards targeting high value transactions like property settlements.*
>
> **Ransomware remains the most destructive cybercrime** - *ransomware groups have further evolved their business model, seeking to maximise their impact by targeting the reputation of Australian organisations… The cost of ransomware extends beyond the ransom demands, and may include system reconstruction, lost productivity, and lost customers.*
>
> **Worldwide, critical infrastructure networks are increasingly targeted** - *both state actors and cybercriminals view critical infrastructure as an attractive target. The continued targeting of Australia's critical infrastructure is of concern as successful attacks could put access to essential services at risk.*
>
> **The rapid exploitation of critical public vulnerabilities became the norm** - *Australian organisations, and even individuals, were indiscriminately targeted by malicious cyber actors. Malicious actors persistently scanned for any network with unpatched systems…'.*

[17] ACSC Annual Cyber Threat Report 2022

2.2 SOCI Act amendments

2.2.1 SLACI and SLACIP Acts

Amendments to the SOCI Act have strengthened the security and resilience of critical infrastructure, by:

- Expanding the scope of the Act from applying to four sectors to eleven sectors
- Providing a regime for the Commonwealth to receive reports in relation to cyber security incidents
- Providing a regime for the Commonwealth to respond to serious cyber security incidents.

The Security Legislation Amendment (Critical Infrastructure) Act 2021 ('SLACI Act') has amended the SOCI Act to build upon the existing framework and aims to strengthen the security and resilience of critical infrastructure. The obligations under the SLACI Act include:

- Register of Critical Infrastructure Assets
- Mandatory Cyber Security Reporting.

The Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 ('SLACIP Act') amends the SOCI Act also to strengthen the existing framework for managing risks to critical infrastructure, including by:[18]

- Introducing a requirement for owners and operators of critical infrastructure assets to establish, maintain, and comply with a risk management program to manage the material risk of a hazard occurring, which could impact the availability, integrity, reliability or confidentiality of the critical infrastructure asset
- Establishing a mechanism for the declaration of Systems of National Significance (SoNS)– those being the assets most interconnected, interdependent, and essential to Australia's social or economic stability, defence or national security
- Establishing a framework of Enhanced Cyber Security Obligations (ESCO), which may apply to SoNS
- Enhancing the framework for the use and disclosure of protected information.

2.2.2 Risk management Program Rules - rule 1 – Cyber and information security hazards[19]

Responsible entities for critical infrastructure assets must, within 6 months of the commencement of this rule, ensure that their risk management program includes details of a risk-based plan that outlines strategies and security controls as to how cyber and information security threats are being mitigated.

Responsible entities for critical infrastructure assets must, within 18 months of the commencement of this rule, ensure that their risk management program includes details of how the responsible entity complies with at least one of the following standards and frameworks:

'a) The Australian Cyber Security Centre's Essential Eight Maturity Model at maturity level one;

b) AS ISO/IEC 27001:2015;

c) The National Institute of Standards and Technology (NIST) Cybersecurity Framework;

[18] Australian Department of Home Affairs and the Cyber and infrastructure Security Centre, Draft Risk Program Management Rules

[19] Australian Department of Home Affairs and the Cyber and infrastructure Security Centre, Draft Risk Program Management Rules

d) The Cybersecurity Capability Maturity Model (C2M2) at Maturity Indicator Level 1;

e) Security Profile 1 of the Australian Energy Sector Cyber Security Framework; or

f) An equivalent standard.'

2.2.3 Enhanced Security Obligations

The ECSO that the Secretary may apply to a SoNS will vary between each SoNS, depending on the specific role and function of that asset. The obligations include:

- *'Developing cyber security incident response plans to prepare for a cyber security incident*
- *Undertaking cyber security exercises to build cyber preparedness*
- *Undertaking vulnerability assessments to identify vulnerabilities for remediation, and/or*
- *Providing system information to develop and maintain a near-real time threat picture.'*

2.3 AESCSF Framework

The Australian Energy Market Operator (AEMO) in collaboration with the Australian Cyber Security Centre (ACSC), Cyber and Infrastructure Security Centre (CISC), and the Cyber Security Industry Working Group (CSIWG), developed and are responsible for driving the AESCSF to provide the energy sector appropriate guidance to secure CI.

The AESCSF leverages existing better practices for cyber security and safety, from Australia and overseas including recognised industry frameworks such as the US Department of Energy's Cybersecurity Capability Maturity Model (ES-C2M2) and the National Institute of Standards and Technology (NIST) Cyber Security Framework.

2.4 SP-2 is Power and Water's target

As discussed above, the Draft Risk Management Program Rules, 'Responsible Entities' for critical infrastructure assets:

"must, within 18 months of the commencement of this rule, ensure that their risk management program includes details of how the responsible entity complies with at least one of the following standards and frameworks..."

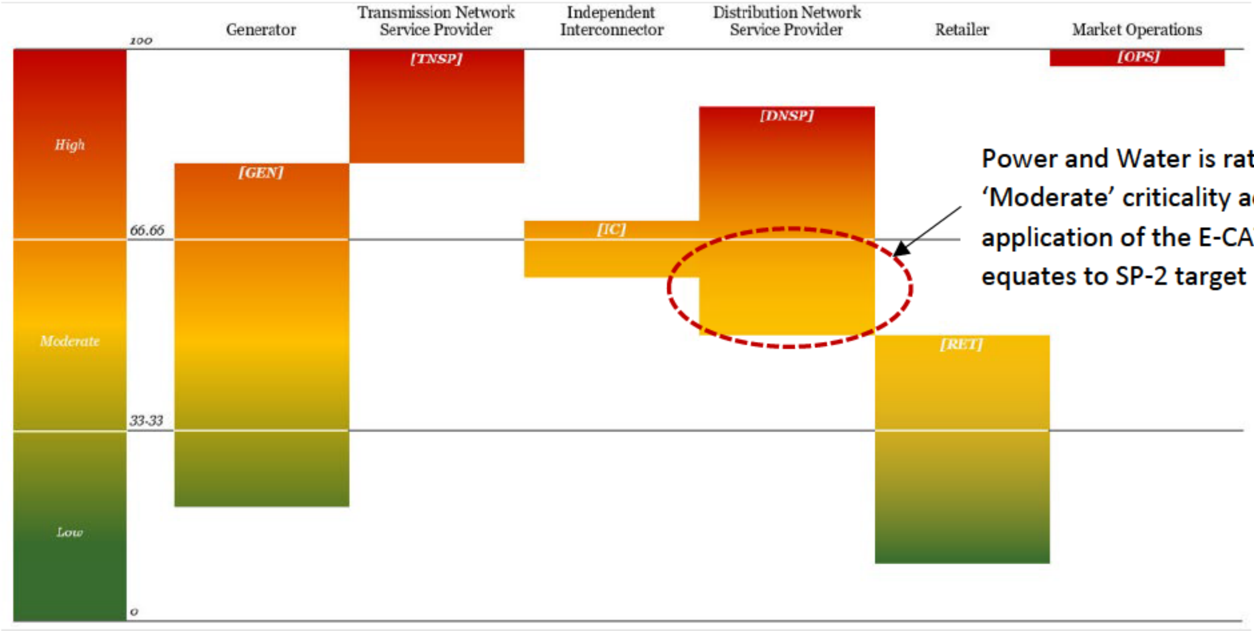
The AESCSF SP-1 is one of these standards and frameworks. However, there are other factors which Power and Water consider combine to support the conclusion that achieving SP-2 within the next RCP is consistent with the actions of a prudent operator in our case:

- The worsening threat landscape, discussed in section 2.1
- The introduction of SONS, which are subject to enhanced cyber security obligations, and which require practices to be in place that go beyond SP-1
- The AER's previous assessment of the prudent level of cyber security as part of its recent Determinations of NSP resets, which in each case has been higher than SP-1 in recognition that a higher level is consistent with the actions of a prudent operator[20]
- The fourth factor is AEMO's assessment of cyber security risk in the electricity sector through the AESCSF - as the figure below shows, AEMO has assessed electricity distribution to straddle the high and

[20] For example, in the AER's AusNet Services Determination 2021-26

moderate criticality bands from a cyber risk perspective. Given Power and Water's relative size as a DNSP to others, the reasonable assumption is that Power and water's electricity assets are of Moderate criticality. As shown in Figure 2, this aligns with a SP-2 target (whereas SP-3 is the appropriate target for TNSPs and, arguably, the large DNSPs). Given Power and Water's responsibility for Market Operations (and Water services), arguably an even higher SP level may be appropriate.

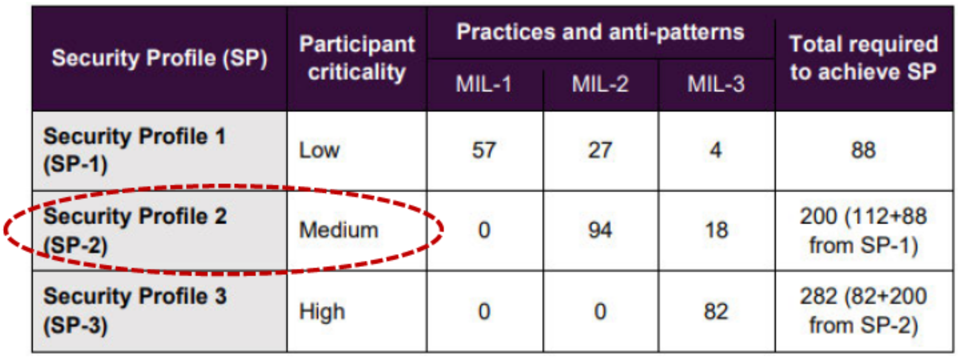
Figure 2: AESCSF electricity sector criticality bands by market role



Power and Water is rated as a 'Moderate' criticality according to application of the E-CAT which equates to SP-2 target

Source: AESCSF Electricity Criticality Assessment Tool (E-CAT) - 2022 Program

Table 5 AESCSF target state maturity and Security Profiles



Security Profile (SP)	Participant criticality	Practices and anti-patterns			Total required to achieve SP
		MIL-1	MIL-2	MIL-3	
Security Profile 1 (SP-1)	Low	57	27	4	88
Security Profile 2 (SP-2)	Medium	0	94	18	200 (112+88 from SP-1)
Security Profile 3 (SP-3)	High	0	0	82	282 (82+200 from SP-2)

Source: AESCSF Overview – 2022 Program, Table 1, page 9

3. Options analysis

This section describes the various options that were analysed to address the Business Need, and specifically the best means of achieving and sustaining the target SP-2 level. The options are analysed based on ability to address the identified needs, prudency and efficiency, commercial and technical feasibility, deliverability, benefits and an optimal balance between long term asset risk and short-term asset performance.

3.1 Comparison of credible options

Credible options are identified as options that address the identified need, are technically feasible and can be implemented within the required timeframe. The following options have been identified:

- Option 1[21] – Blended resource model to achieve SP-2. This option proposes prioritised investments with blended resource model to adequately meet SOCI obligations, demonstrate SP-2 compliance, and address known and emergent risks.
- Option 2[22] – Internal resource model to achieve SP-2. This option proposes additional recruitment to enable all capability improvements to be achieved with existing technologies. No or minimal new infrastructure, software or supporting technology.
- Option 3[23] – Outsourced resource model to achieve SP-2. This option proposes to seek to out-source operational elements whilst maintaining in-sourced governance across the processes in scope. Heavy use of security services, with positive vetting of compliance required by internal resources.

A comparison of the three identified credible options and the issues they address in the identified need is depicted in Table 6.

These options are described and assessed in detail in the sections below.

Table 6 Summary of options analysis outcomes

Assessment metrics	Option 1	Option 2	Option 3
NPV ($m, real 2022)	-20.82	-15.41	-26.95
BCR[24]	Not applicable	Not applicable	Not applicable
Capex ($m, real 2022)	16.65	4.00	15.00
Opex ($m, real 2022)	11.66	16.00	20.00
Totex ($m, real 2022)	28.30	20.00	35.00
Meets customer expectations	◕	◑	○

[21] Option 1 assumes additional resources will be a balance of infrastructure, information, services and labour contracts

[22] Option 2 assumes minimal capex due to predominantly internal resourcing efforts and labour and service engagements, & less extensive capability coverage

[23] Option 3 assumes a moderate amount of infrastructure and solutions still required to manage/provide visibility into external service and infra offerings, with premium market rates with 'retainer' and consumption style costs due to high demand nationally

[24] A BCR has not been derived because this is a compliance-driven project, not a benefits-driven project

Aligns with Asset Objectives	●	◑	◑
Technical Viability	●	○	○
Deliverability	●	○	○
Preferred	✓	✗	✗
Ranking	1	2	3

●	Fully addresses the issue	◕	Adequately addresses the issue	◑	Partially addresses the issue	○	Does not address the issue

3.1.1 Option 1 – Blended resourcing model to achieve SP-2 compliance

Power and Water's resourcing challenges

Power and Water faces a number of challenging factors which influence the viable approaches to such a large demand on resources and technology represented by the Cyber Security Project. Power and Water's operating environment covers a large and remote geographic footprint, involving multi-utility services, provided to a small but diverse customer base with broad needs. Power and Water's IT and OT infrastructure (hardware, systems, applications) is undergoing a slow but steady transition to COTS, fit-for-purpose, class-leading assets to enable power and water to both be more efficient and to effectively manage the changing energy landscape (i.e. cyber-attacks, distributed energy resources, EVs, and deterioration of affordability, to name a few). [redacted]

[redacted]

Blended resourcing strategy

Considering all the factors above, considerable contractor resource will be required to assist Power and Water deliver the project. Power and Water will provide internal resources to provide program, delivery and operational governance. Power and Water staff will manage the project design and development. The implementation of the multiple initiatives will be undertaken largely by external service providers.

The contractual arrangements will be selected and negotiated through a competitive tender process to provide services and solutions. The strategy for controlling cost and work flow will be seeking partners that can scale their involvement to match the varying demands (volume and skill) over the project lifecycle. Power and Water will also pursue practical contractual options to leverage existing service providers, such as the Northern Territory Government's (NTG) DCDD[25] and DCS,[26] in supplying cyber capability uplifts where

[25] Department of Corporate and Digital Development, which provides enterprise information and technology services and shared corporate services to support NTG agencies

[26] NTG Data Centre Services

possible, as this will be a significantly faster, more cost- and resource-effective approach than attempting to procure, establish and operate new solutions.

Some of the internal resources for the Project will need to be seconded full-time and backfilled by recruitment of contractors.

Blended resourcing will still require a limited and prudent selection of technologies to improve Power and Water's capabilities to prevent, detect, respond to, and recover from cyber threats and incidents. Technologies which provide automation to support coordinated governance, management and operations across Power and Water's entire enterprise, including 3rd party service providers, are a key component to ensuring efficient and practicable security controls which are supportable with a blended resourcing model of internal, government and external resources.

Project initiatives

Power and Water has a history of successful delivery of small to medium (<$2m) technology investments by effective use of outsourced implementation, operations and advisory services combined with internally resourced project management and governance. With the appropriate project structure and delivery partners, the project can be delivered as a number of smaller initiatives over time. Combined with a strong ICT senior management team, the blended resourcing approach gives the most practical and manageable approach.

The table below summarises the proposed approach to achieving SP-1 and then SP-2 but after focussing for the first 6 months on the AESCSF Priority Practices.[27] The Project will therefore be delivered via 18 initiatives, but as shown in Appendix B, there are 62 work packages within the 18 initiatives. The AESCSF SP-1 level is designed to be achieved within two years (i.e. +18 months from completion of the Priority Practices). Achieving SP-2 is planned to be achieved within the ensuing 42 months to reach a compliant position within 5 years of commencement.

Table 7 - List of proposed initiatives and at which milestone (AESCSF Priority Processes, SP1 Baseline and SP2/3 Priority Set) will be achieved)

Initiative Name	Need	Primary Security Alignment Goal	[redacted]	[redacted]	[redacted]
CSU-01 Cyber Training Uplift	Uplift of enterprise wide and specific functional group training in cyber security (incl PCI-DSS / OT ICS engineering)	Create culture of security	[redacted]	[redacted]	[redacted]
CSU-02 Improve security governance	Establishment of an information security program encompassing the two control domains of Information Security and Organisational Structure	Improve security governance	[redacted]	[redacted]	[redacted]
CSU-03 Identity and Access Management	Capability to enable the ability to manage all authentication and authorisation systems and services centrally under a single platform	Create culture of security	[redacted]	[redacted]	[redacted]

[27] The ACSC has defined a total of 26 Priority Practices within the AESCSF. These are the areas of capability and maturity that the ACSC recommends organisations prioritise first as part of any uplift program. This is due to their high impact on cyber security risk reduction and being the 'must-have' foundational capabilities blocks upon which other AESCSF capabilities are built upon

CSU-06 Information Security Roadmap	This initiative encompasses all aspects of information security governance and controls across the enterprise data, application and technology landscapes. This initiative also encompasses all aspects of information security classification.	Manage compliance obligations	▮	▮	▮
CSU-08 Security Compliance and Governance regulations	Addition or augmentation of existing cyber security controls to address the combined governance compliance from the AESCSF regulation and the EY and Deloitte audit reports	Manage compliance obligations	▮	▮	▮
CSU-11 Endpoint Security Platform	Capability to protect all Power and Water endpoint device and appliance systems from all potential threat actors and ensuring appropriate vulnerability management	Manage Compliance Obligations	▮	▮	▮
CSU-17 Security Metrics	Metrics are defined to measure the effectiveness of the security program	Manage Compliance Obligations	▮	▮	▮
CSU-18 Business Impact Assessment Reviews	All planned business impact assessment activities and reporting must be reviewed by principal cyber security for every Power and Water business unit. All findings identifying potential system security and service availability gaps must be mitigated	Manage Compliance Obligations	▮	▮	▮
CSU-09 Data Sharing & Privacy	Capability to ensure appropriate information sharing cyber security controls are available and applied/enforced across all on-premise, hybrid and cloud hosted enterprise solutions	Protect data	▮	▮	▮
CSU-10 Incident Response Capability	Establishment of a Cyber Security Incident Response capability encompassing both cyber personnel resources and technical capability uplifts	Protect Data	▮	▮	▮
CSU-04 Network Access Control Implementation	Capability to invoke and governance access control from any network attached device across any ICT/OT enterprise domains	Secure the Infrastructure	▮	▮	▮
CSU-05 ICT Domain Network Segmentation	Establish appropriate controls to ensure that every Power and Water enterprise service and workload is effectively segmented across the Power and Water network	Secure the Infrastructure	▮	▮	▮
CSU-07 Asset Management	Managing and securing all assets in line with AESCSF and the critical infrastructure bill	Secure the Infrastructure	▮	▮	▮
CSU-12 OT Security Architecture Re-design/Uplift	Review & gap analysis of the entire Power and Water OT network & utility service infrastructure by an independent 3rd party. Design & Uplift	Secure the Infrastructure	▮	▮	▮
CSU-13 Application Security Management	Ensure the security of all code development and code life cycle management is highly secure and meets all industry compliance standards	Secure the Infrastructure	▮	▮	▮
CSU-16 Protection of Backups and Archives	All backups (ICT/OT/On Premise/Cloud) are secured by appropriate levels of storage encryption to protect against ransomware and other threats	Secure the Infrastructure	▮	▮	▮
CSU-14 Centralised Logging & Threat Detection Management	Establishment of a capability to retrieve, correlate, analyse, assess and act upon events that have occurred throughout the Power and Water on premise, hybrid and cloud-based networks & network attached systems	Detect & Respond to Threats	▮	▮	▮

CSU-15 Forensic investigation tooling to support incident response	Forensic investigations are performed as part of security incident management. Forensic evidence and e-discovery data is collected and preserved as required	Detect & Respond to Threats	[redacted]	[redacted]	[redacted]

4	Fully addresses issue	3	Adequately addresses issue	2	Partially addresses issue	1	Minimally addresses issue

This is the recommended option.

3.1.2 Option 2 – Internal resource model to achieve SP-2

This option is based on only using internal resources to undertake the Project. This option does not include seconding staff to the project and back filling them with external resources, as this is a fundamental aspect of Option 1. Therefore for Option 2, staff would need to work part time on the project whilst undertaking their substantive roles. The advantage of Option 2 over Option 1 is that it would likely require less expenditure in the next RCP. However, the disadvantage is that the very limited availability of people with the required skills and experience will either compromise delivery of the project or compromise delivery of day-to-day operations; the most likely outcome is that both will be adversely affected. This is because the experienced staff are already at full capacity (in addition to their operational or day-to-day roles, they also contribute to active strategic initiatives). Therefore their capacity for doing even more by working on the project is limited-to-zero. An alternative considered to reduce the reliance on experienced staff was to train suitable staff in cyber and information security so that they could contribute to the project, either by:

- Training on the job – this would increase the number of staff who could work on the Project, but it would create other issues:
  - instead of doing just their normal roles, the staff would also be required to work on the project with limited skills and experience, at least initially; this would compromise their operational work and would slow progress on the Project due to low productivity whilst learning the Project work
  - their total workload would be unsustainable, which would likely lead to turnover, further compromising day-to-day operations, other initiatives they are working on, and the project
- Training prior to commencement of the project – this would provide a larger pool of more qualified staff to work part-time on the project; the advantage of this approach is that when the training is complete, project productivity would be higher than for the on-the-job training option; however this approach also causes issues:
  - the project will be delayed whilst people are in training
  - the staff have limited-to-zero capacity to undertake training without compromising day-to-day operations and any other initiatives they are working on
  - their total workload would be unsustainable, which would likely lead to turnover, further compromising day-to-day operations and the Project.

Given the gap in skills, experience and capacity, the ability to adopt new technologies in this option are considered to be very limited, as the overhead associated with the definition of requirements, coordination of vendors and internal staff, market scans, product selection, contract negotiation, implementation, and transition to support would present unacceptable levels of operational and delivery risk. This would be compounded by resourcing constraints already in place due to other significant and high priority investments which require the same very limited, highly skilled technical resources Power and Water has available.

The end result of this option from a project perspective is significant delay and probably sub-optimal outcomes. The outcome from a wider ICT perspective is unacceptable risk to day-to-day operations and other initiatives plus higher than usual turnover.

This approach and likely outcome would be unlikely to meet the reasonable expectations of Power and Water's customers, who would expect selection of an option that better balances cost, risk and benefits.

This option is not recommended.

3.1.3 Option 3 – Outsourced resource model to achieve SP-2

This option is based on a fully outsourced model for (i) achieving SP-2, including planning, designing, and implementing the systems and processes, and (ii) sustaining SP-2, which includes the monitoring, control, response to attacks/breaches, undertaking regular cyber security exercises and vulnerability assessments to build cyber preparedness.

The advantage of this option is that it would greatly reduce the burden on internal resources. A fully externally serviced model is attractive from an operational management point of view, however such services and resources are likely to approach almost double the cost of an internal or blended approach, whilst lacking the responsiveness, visibility and control Power and Water would require preventing, responding to, and recovering from cyber and information security incidents.

As the accountable owners of assets classified against the AESCSF, Power and Water holds the obligation to plan, effect, demonstrate and report on the appropriate levels of security. Whilst significant portions of the activities and investments can be based on outsourced labour and services, the need for visibility and control requires an in-sourced set of processes and supporting systems to be effective, particularly when an incident response is underway.

Power and Water's resourcing and expertise constraints would also become the bottleneck for a large number of managed-service and ongoing contractual engagements. It would be both imprudent and inefficient to have large, externally run capabilities which are unable to effectively integrate within the organisational limitations.

Technology investments in this option are limited, as the focus of the option is to avoid additional overhead on internal resources. Given Power and Water's low level of cyber security-related technological sophistication, the uplift in operational expenses to implement and operate new technology platforms is not part of this option. Instead, the intent is to consume "as a service" offerings where ever practicable. This option is rendered less attractive given the implications of "as a service" options, as managing external cyber-related services with 3rd parties requiring access to Power and Water (and potentially NT Government connected) systems and information would be complex in operation, manually intensive for Power and Water staff, potentially inadequately controllable in an incident during out of standard hours or via remote locations, as well as having substantial implications from a supply chain, service and security management perspective.

This approach and likely outcome would be unlikely to meet the reasonable expectations of Power and Water's customers, who would expect selection of an option that better balances cost, risk and benefits.

This option is not recommended.

3.2 Non-credible options

Two non-credible options were considered but not progressed:

3.2.1 Maintaining the current cyber security maturity level throughout the next RCP

With this option, no investment would be made other than required to maintain the cyber security maturity at [redacted][28] The advantage of this option is the reduced capex, opex, and resource requirements. The disadvantages are:

- [redacted]
- The threat landscape is continuing to worsen and Power and Water's infrastructure would be increasingly vulnerable to cyber-attack and supply disruption.

These risks are intolerable and accordingly this option is not considered to be credible.

3.2.2 Maturing to AESCSF SP-3 by the end of the next RCP

Whilst achieving a cyber security maturity level of SP-3 (requiring completion of 282 practices and anti-patterns, an increase of 82 on the number required for SP-2) would strengthen Power and Water's cyber-attack resilience, there are several reasons this option was not considered further:

- [redacted]
- [redacted]
- The additional cost of achieving SP-3 would be significant – although the work has not been costed in detail, it is likely a further 30-50% totex would be required on top of the $24.5 million estimate for achieving SP-2 (i.e. another [redacted])
- If it is later determined that SP-3 is an appropriate maturity level for Power and Water, the vast majority of the work would need to be sequenced to occur after SP-2 is achieved
- It is likely that a few high priority SP-3 practices will be implemented during the course of the next RCP, but this will occur based on a risk-cost analysis.

[28] Marginal improvements and initiatives will be required in order to maintain current capabilities

4. Recommendation

For Power and Water to uplift its cyber security posture and meet its mandatory compliance obligations under the amended SOCI Act and noting the AER Ring Fencing compliance regulation, Option 1 is recommended.

The prudent and efficient method of investing in the large program of work is to adopt a blended resourcing model. The project structure will be targeted and phased to ensure the following milestones are achieved: AESCSF Priority Practices (26) within 6 months of project commencement, SP-1 by the end of the current RCP, and SP-2 by December 2027 (i.e. 42 months after achieving SP-1).

Option 1 is based on a combination of internal and external resources, with built-in flexibility to adjust the contracted services. It enables the investments to be adjusted to meet growing and evolving needs without committing to or relying on extensive technology, automation, and permanent internal resourcing up-front.

Not progressing Option 1 will mean Power and Water fails to meet its mandatory compliance obligations and the practical and prudent operational cyber security requirements. This in turn will mean Power and Water would be unable to provide safe, stable and reliable electricity to the Northern Territory population, with implications for reputational damage to the corporation and its Board and executives. In the worst case, financial and criminal penalties may be applied to Power and Water and individuals.

4.1 Strategic Alignment

This proposal aligns with Power and Water's Cyber Security Management Standard and meets the mandatory obligations under the Security of Critical Infrastructure Act, AER Ring Fencing compliance regulations and contributes to the D2021/260606 "Power and Water Strategic Direction" as indicated in the table below.

Strategic direction focus area		Strategic direction priority
1	Always Safe	Improve Public Health and Safety
2	Sustainable solutions for the future	Sustainable Energy and Water Services

4.2 Dependent projects

Whilst the implementation of these initiatives will influence solutions for other initiatives, there are no known projects or other network issues that are scope-dependent on the uplift in these capabilities. The accountability and costs for some services and capabilities may fall to NTG departments, creating interdependencies that are as yet unable to be qualified or quantified. This will be addressed as each initiative progresses internally to full business case.

4.3 Deliverability

Power and Water has a strong and successful history of small to medium technology project delivery and is building capability in larger, complex ICT projects with the Meter to Cash project. With this in mind, the structure of the cyber and information security program to meet operational security requirements and SOCI Act and SP-2 compliance is structured to keep each initiative sized, sequenced and structured to play to Power and Water's strengths and expanding expertise.

The foundational elements (15 practices across AESCSF SP-1) are relatively discrete, not heavily integrated, and will fall within the envelope of scale and sizing for IT and OT to implement the changes without anticipated difficulty.

The balance of SP-1 (73 practices) are fully or largely implemented within IT, but for the most part not implemented in OT (or are 'reliant' on IT). The initiatives required to achieve SP-1 are predominantly deliverable, requiring process updates, or are service-based, and so also fall within Power and Water's historically successful delivery scale.

The key challenges impacting deliverability of the additional 112 practices required to achieve SP-2, are:

- the scale of procurement
- the high number of solutions required
- the complexity of integrations and operations required
- the overhead in running and operating new capabilities as others are added.

Mitigations/manageability considerations to help optimise deliverability include:

- A phased and capability-aligned approach to minimise impacts on teams and key SMEs
- Instrumentation and Automation will be applied to minimise manual labour/handling/entry of data
- A right-sourced approach to operational services (e.g. monitoring, alerting) will be adopted
- Utilising existing service providers and leveraging their obligations as a provider to a government owned corporation with SoNS.

4.4 Customer considerations

The primary project driver is to provide reliable, network stability and consistent services to the Northern Territory consumers by enhancing our cyber security capability and posture, while meeting our mandatory obligations under the SOCI Act. Fundamentally, the impact and benefit to customer revolves around suitable protections of their information, and continuity of access to power and water products and services.

Furthermore, customers expect Power and Water to prudently balance delivery risk, cost, and benefit. The analysis undertaken indicates that Option 1 is the best way to deliver the required cyber maturity outcomes which are expected of a prudent operator in a cost-efficient way, by blending external and internal expertise with a knowledge transfer from the former to the latter over the 7 year duration of the project.

4.5 Expenditure profile

Total expenditure is 28.31 million (real 2021/22).

The tables below show a summary of the expenditure requirements for the current regulatory period and next regulatory period.

Table 8 Estimated annual capital and operational expenditure – current regulatory period ($'000, real 2021/22)

Item	FY20	FY21	FY22	FY23	FY24	Total
Capex				1.65	2.00	3.65
Opex				1.16	1.40	2.56
Total	**n/a**	**n/a**	**n/a**	**2.81**	**3.40**	**6.21**

Table 9 Forecast annual capital and operational expenditure – next regulatory period ($'000, real 2021/22)

Item	FY25	FY26	FY27	FY28	FY29	Total
Capex	2.50	3.00	3.00	2.50	2.00	**13.00**
Opex	1.75	2.10	2.10	1.75	1.40	**9.10**
Total	**4.25**	**5.10**	**5.10**	**4.25**	**3.40**	**22.10**

The tables below show a summary of the expenditure requirements for the current regulatory period and next regulatory period, allocated to Standard Control Services as per the CAM.

Table 10 Estimated annual capital and operational expenditure – current regulatory period – allocated to SCS ($'000, real 2021/22)

Item	FY20	FY21	FY22	FY23	FY24	Total
Capex				1.29	1.56	2.85
Opex				0.58	0.69	1.27
Total	**n/a**	**n/a**	**n/a**	**1.87**	**2.25**	**4.12**

Table 11 Forecast annual capital and operational expenditure – next regulatory period – allocated to SCS ($'000, real 2021/22)

Item	FY25	FY26	FY27	FY28	FY29	Total
Capex	1.95	2.35	2.35	1.95	1.56	10.16
Opex	0.87	1.04	1.04	0.87	0.69	4.51
Total	**2.82**	**3.39**	**3.39**	**2.82**	**2.25**	**14.67**

The tables below show a summary of the expenditure requirements for the current regulatory period and next regulatory period, allocated to recurrent and non-recurrent categories.

Table 12 Estimated annual capital expenditure – current regulatory period – recurrent and non-recurrent

Item	FY20	FY21	FY22	FY23	FY24
Recurrent				0%	0%
Non-recurrent				100%	100%

Table 13 Forecast annual capital expenditure – next regulatory period – recurrent and non-recurrent

Item	FY25	FY26	FY27	FY28	FY29
Recurrent	0%	0%	0%	100%	100%
Non-recurrent	100%	100%	100%	0%	0%

4.6 High-level scope

The project will involve the same high level scope items for each initiative:

- Initiation and business engagement,
- Functional & Technical requirements / Product architecture
- Market Scan, options definition and analysis
- Contract management
- Project management
- Initiative design
- Initiative implementation, including where new technology is involved:
  - Establishing new application environments (dev, test, production), application migration, testing (system, integration and user acceptance), end-user communication, coordination, Change Management, updated support documentation and end-user training

The project currently comprises 18 initiatives to embed the 200 practices necessary to achieve SP-2 across the 11 AESCSF domains. The table below shows the 17 Power and Water cyber security initiatives mapped to the AESCSF. The seventeen initiatives comprise 63 work packages to deliver the 200 practices required, which are outlined in Appendix A.

Table 14: Cyber security project initiatives mapped to the 11 AESCSF domains

AESCSF Full Domain	Primary Initiative	Secondary Initiative
AESCSF-WM Domain: Workforce Management	CSU-01 Cyber Training Uplift	CSU-02 Improve security governance
		CSU-03 Identity and Access Management
		CSU-06 Information Security Roadmap
		CSU-08 Security Compliance and Governance regulations
		CSU-17 Security Metrics
		CSU-18 Business Impact Assessment Reviews
AESCSF-RM Domain: Risk management	CSU-02 Improve security governance	CSU-06 Information Security Roadmap
		CSU-08 Security Compliance and Governance regulations

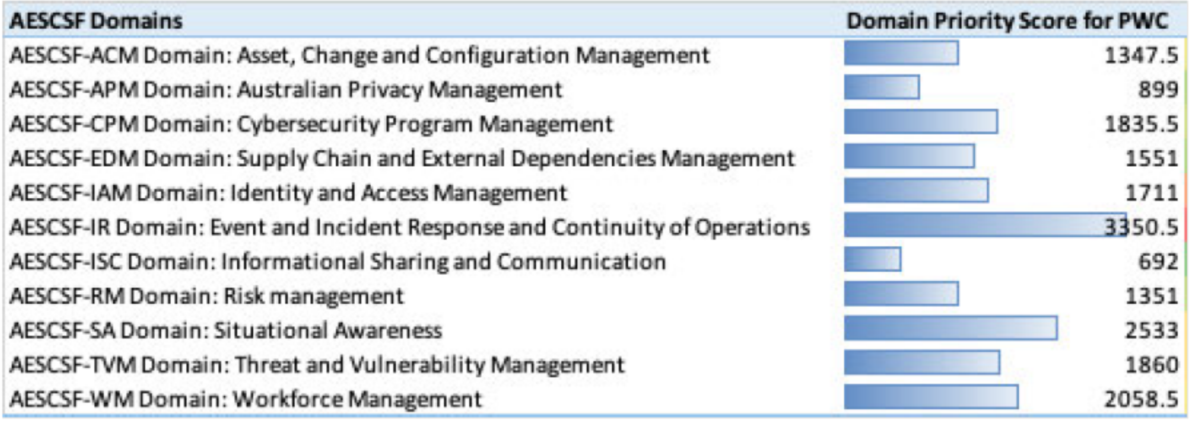
		CSU-12 OT Security Architecture Re-design/Uplift CSU-17 Security Metrics
AESCSF-IAM Domain: Identity and Access Management	CSU-03 Identity and Access Management	CSU-04 Network Access Control Implementation
AESCSF-CPM Domain: Cybersecurity Program Management	CSU-05 ICT Domain Network Segmentation	CSU-08 Security Compliance and Governance regulations
AESCSF-ACM Domain: Asset, Change and Configuration Management	CSU-07 Asset Management	CSU-12 OT Security Architecture Re-design/Uplift
AESCSF-APM Domain: Australian Privacy Management	CSU-09 Data Sharing & Privacy	CSU-08 Security Compliance and Governance regulations
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	CSU-10 Incident Response Capability	CSU-02 Improve security governance CSU-08 Security Compliance and Governance regulations CSU-10 Incident Response Capability CSU-15 Forensic investigation tooling to support incident response CSU-18 Business Impact Assessment Reviews
AESCSF-SA Domain: Situational Awareness	CSU-11 Endpoint Security Platform	CSU-12 OT Security Architecture Re-design/Uplift CSU-15 Forensic investigation tooling to support incident response CSU-16 Protection of Backups and Archives CSU-17 Security Metrics
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	CSU-13 Application Security Management	CSU-18 Business Impact Assessment Reviews
AESCSF-TVM Domain: Threat and Vulnerability Management	CSU-14 Centralised Logging & Threat Management	CSU-12 OT Security Architecture Re-design/Uplift CSU-16 Protection of Backups and Archives
AESCSF-ISC Domain: Informational Sharing and Communication	CSU-17 Security Metrics	CSU-02 Improve security governance

Appendix A. Key assumptions

The initiatives provide coverage for Cyber and Information Security hazards for IT and OT, but do not cover other domains, such as supply chain, or physical and natural hazards. Some elements of SP-3 may also be covered within the timeframe, depending on emergent threats, on a risk-prioritised basis; these elements are not called out or costed as part of this business case.

The overall program of works has been scored against required AESCSF practices, their maturity level, Power and Water's current capabilities and target maturity, the size of the gaps for both IT and OT, the complexity of the practices required, and the overall risk posed to Power and Water by current gaps and maturity levels.

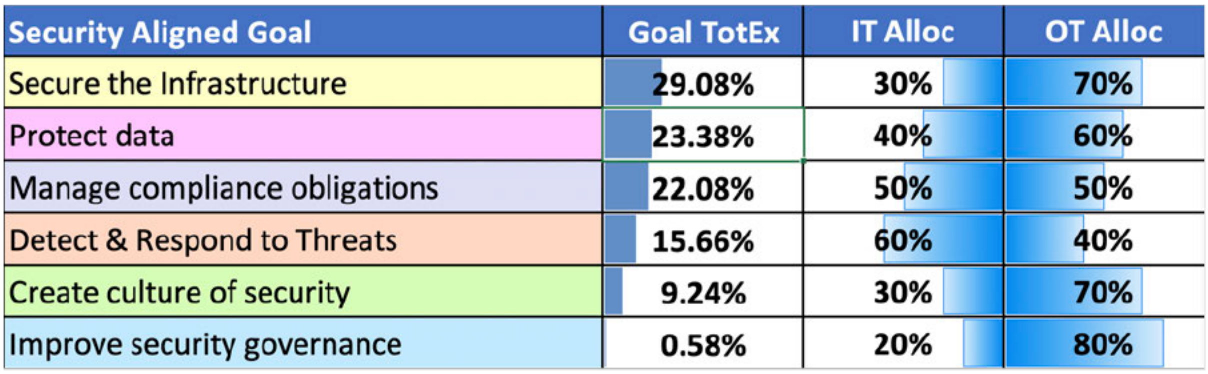
Figure 3 – Power and Water's Domain priority scores (higher the score the higher the effort/investment required)



AESCSF Domains	Domain Priority Score for PWC
AESCSF-ACM Domain: Asset, Change and Configuration Management	1347.5
AESCSF-APM Domain: Australian Privacy Management	899
AESCSF-CPM Domain: Cybersecurity Program Management	1835.5
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	1551
AESCSF-IAM Domain: Identity and Access Management	1711
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	3350.5
AESCSF-ISC Domain: Informational Sharing and Communication	692
AESCSF-RM Domain: Risk management	1351
AESCSF-SA Domain: Situational Awareness	2533
AESCSF-TVM Domain: Threat and Vulnerability Management	1860
AESCSF-WM Domain: Workforce Management	2058.5

The overall set of proposed initiatives to address AESCSF compliance cover the 6 key goals are presented in the figure below. The initiatives are all summarised to the primary goal and are aggregated to show the relative sizing and allocations for estimated IT and OT spend.

Figure 4 – Sizing/Spend proportion per Security Goal/Theme to meet Power and Water's cyber and information security needs. Note the colours of the security goals continue through subsequent tables.



Security Aligned Goal	Goal TotEx	IT Alloc	OT Alloc
Secure the Infrastructure	29.08%	30%	70%
Protect data	23.38%	40%	60%
Manage compliance obligations	22.08%	50%	50%
Detect & Respond to Threats	15.66%	60%	40%
Create culture of security	9.24%	30%	70%
Improve security governance	0.58%	20%	80%

Whilst SP-2 is scheduled be achieved within 42 months of the commencement of the next RCP, there is an ongoing requirement for capex and opex because due to the relatively small scale of Power and Water, it won't be able to implement everything as automated/semi-automated or contract-managed options immediately – some manual processes will be in place that still require investment to be rendered more sustainable/resilient. Also ongoing opex will be required to support the increased staff numbers discussed in the main body of this business case. Power and Water will be able to demonstrate performance of the required practices adequately,

but more expenditure in the latter years of the next RCP will be required to make cyber security practices manageable in the longer term with less reliance on people.

Appendix B. Cost estimation

The cost estimate has been developed based on a bottom-up assessment as shown in the following tables.

B.1 AESCSF Foundations and SP-1 Compliance – Current Regulatory Period

Power and Water needs to first deliver an overall program plan and a set of investments to meet two key milestones within the current regulatory period. Within the first 6 months the foundations and framework must be delivered, then within the following 12 months, a further set of initiatives need to be delivered to meet AESCSF SP-1 **for both IT and OT**. The total investment per initiative is shown below, representing SP-1 by 30th June 2024, under the assumption of January 1st 2023 start.

Table 15 – Level of investment per initiative to deliver Foundations and SP1 Compliance within 18 months Jan 1st, 2023

Initiative Name	Primary Security Alignment Goal	[redacted]	[redacted]
CSU-01 Cyber Training Uplift	Create culture of security	[redacted]	[redacted]
CSU-03 Identity and Access Management	Create culture of security	$ [redacted]	[redacted]
CSU-14 Centralised Logging & Threat Management	Detect & Respond to Threats	[redacted]	[redacted]
CSU-15 Forensic investigation tooling to support incident response	Detect & Respond to Threats	[redacted]	[redacted]
CSU-02 Improve security governance	Improve security governance	[redacted]	[redacted]
CSU-06 Information Security Roadmap	Manage compliance obligations	[redacted]	[redacted]
CSU-08 Security Compliance and Governance regulations	Manage compliance obligations	[redacted]	[redacted]
CSU-17 Security Metrics	Manage Compliance Obligations	[redacted]	[redacted]
CSU-18 Business Impact Assessment Reviews	Manage Compliance Obligations	[redacted]	[redacted]
CSU-11 Endpoint Security Platform	Manage Compliance Obligations	[redacted]	[redacted]
CSU-09 Data Sharing & Privacy	Protect data	[redacted]	[redacted]
CSU-10 Incident Response Capability	Protect Data	[redacted]	[redacted]
CSU-04 Network Access Control Implementation	Secure the Infrastructure	[redacted]	[redacted]
CSU-05 ICT Domain Network Segmentation	Secure the Infrastructure	[redacted]	[redacted]
CSU-07 Asset Management	Secure the Infrastructure	$ [redacted]	[redacted]
CSU-12 OT Security Architecture Re-design/Uplift	Secure the Infrastructure	[redacted]	[redacted]
CSU-13 Application Security Management	Secure the Infrastructure	[redacted]	[redacted]
CSU-16 Protection of Backups and Archives	Secure the Infrastructure	[redacted]	[redacted]
		[redacted]	[redacted]
			[redacted]

B.2 AESCSF SP-2 – Regulatory Period 24-29

To achieve SP-2 for both IT and OT requires additional investment in projects within the initiatives shown below. SP-2 involves significantly more investment to achieve than SP-1, and a greater proportion of capital expenditure due to the scale, diversity and locality of Power and Water's assets and services to be protected.

Table 16 – Level of investment per initiative to deliver SP2 Compliance within 60 months of Jan 1st 2023 ($,000, real 2022)

Initiative Name	Primary Security Alignment Goal	[redacted]	[redacted]
CSU-01 Cyber Training Uplift	Create culture of security	[redacted]	[redacted]
CSU-03 Identity and Access Management	Create culture of security	[redacted]	[redacted]
CSU-14 Centralised Logging & Threat Management	Detect & Respond to Threats	[redacted]	[redacted]
CSU-15 Forensic investigation tooling to support incident response	Detect & Respond to Threats	[redacted]	[redacted]
CSU-02 Improve security governance	Improve security governance	[redacted]	[redacted]
CSU-06 Information Security Roadmap	Manage compliance obligations	[redacted]	[redacted]
CSU-08 Security Compliance and Governance regulations	Manage compliance obligations	[redacted]	[redacted]
CSU-17 Security Metrics	Manage Compliance Obligations	[redacted]	[redacted]
CSU-18 Business Impact Assessment Reviews	Manage Compliance Obligations	[redacted]	[redacted]
CSU-11 Endpoint Security Platform	Manage Compliance Obligations	[redacted]	[redacted]
CSU-09 Data Sharing & Privacy	Protect data	[redacted]	[redacted]
CSU-10 Incident Response Capability	Protect Data	[redacted]	[redacted]
CSU-04 Network Access Control Implementation	Secure the Infrastructure	[redacted]	[redacted]
CSU-05 ICT Domain Network Segmentation	Secure the Infrastructure	[redacted]	[redacted]
CSU-07 Asset Management	Secure the Infrastructure	[redacted]	[redacted]
CSU-12 OT Security Architecture Re-design/Uplift	Secure the Infrastructure	[redacted]	[redacted]
CSU-13 Application Security Management	Secure the Infrastructure	[redacted]	[redacted]
CSU-16 Protection of Backups and Archives	Secure the Infrastructure	[redacted]	[redacted]
		[redacted]	[redacted]
			[redacted]

Appendix C. Initiatives and Work Packages to achieve AESCSF SP-1 and SP-2

Note that SP-3 items are not shown in these materials.

C.1 AESCSF Rankings by AESCSF priority, risk, current process gap, and maturity gap

Items in this section which have the same scores have the same calculated score of relative priority, risk and effort; by implication, Power and Water are interpreting these as relative groups for sequencing/prioritisation purposes.

Higher scores for total size indicate higher challenges to implement, and higher scores for priority group indicates higher priorities and earlier sequencing.

Reading the scoring columns together:

- Items with high priority and a high complexity: the most impactful items to address but require a substantial uplift in scope and/or maturity of process.
- Items with a high priority and a low complexity: impactful items where the processes, solutions or maturity gaps are smaller and more achievable for less effort.
- Items with a low priority and a high complexity: reconsider approaches to minimise/spread the complexity
- Items with a low priority and a low complexity: defer or sequence at convenience when resourcing allows.

Table 17 - AESCSF Practices sorted by SP level, then AESCSF priority and Risk level, then grouped by size of challenge/gap with Power and Water's current practices – with Related Initiative/s which cover the uplift required

AESCSF Full Domain	AESCSF Full Practice	SP	MIL	[redacted]	[redacted]	Primary Initiative
AESCSF-WM Domain: Workforce Management	AESCSF-WM-2A Personnel vetting (e.g., background checks, drug tests) is performed, at least in an ad hoc manner, at hire for positions that have access to the assets required for delivery of the function	SP-1	MIL-1	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-1A There is an inventory of OT and IT assets that are important to the delivery of the function; management of the inventory may be ad hoc	SP-1	MIL-1	[redacted]	[redacted]	CSU-07 Asset Management
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-1B There is an inventory of information assets that are important to the delivery of the function (e.g., SCADA set points, customer information, financial data); management of the inventory may be ad hoc	SP-1	MIL-1	[redacted]	[redacted]	CSU-07 Asset Management
AESCSF-APM Domain: Australian	AESCSF-APM-1B The organisation has defined what it considers personal	SP-1	MIL-1	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy

Privacy Management	information in the context of its business activities, even in an ad-hoc manner.					
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-2A Resources (people, tools, and funding) are provided, at least in an ad hoc manner, to support the Cyber Security program	SP-1	MIL-1	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-2B Senior management provides sponsorship for the Cyber Security program, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-1A Important IT and OT supplier dependencies are identified (i.e., external parties on which the delivery of the function depend, including operating partners), at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2A Significant Cyber Security risks due to suppliers and other dependencies are identified and addressed, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-3C Reporting of escalated Cyber Security events and incidents is performed (e.g., internal reporting, ACSC), at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-4A The activities necessary to sustain minimum operations of the function are identified, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-4B The sequence of activities necessary to return the function to normal operation is identified, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-RM Domain: Risk management	AESCSF-RM-2A Cyber Security risks are identified, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-02 Improve security governance
AESCSF-RM Domain: Risk management	AESCSF-RM-2B Identified Cyber Security risks are mitigated, accepted, tolerated, or transferred, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-02 Improve security governance
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-1C Threats that are considered important to the function are addressed (e.g., implement mitigating controls, monitor threat status), at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-WM Domain: Workforce Management	AESCSF-WM-2B Personnel termination procedures address Cyber Security, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-1B Logging requirements have been defined for all assets important to the function (e.g., scope of activity and	SP-1	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint

	coverage of assets, Cyber Security requirements [confidentiality, integrity, availability])			🟥	🟧	Security Platform
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-AP1 Where technical or business reasons restrict the ability to remediate an identified vulnerability, no mitigating or compensating controls are investigated and applied	SP-1	MIL-1	🟥■	🟧■	CSU-14 Centralised Logging & Threat Management
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-3B Changes to inventoried assets are logged, at least in an ad hoc manner	SP-1	MIL-1	🟧■	🟧■	CSU-07 Asset Management
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2B Cyber Security requirements are considered, at least in an ad hoc manner, when establishing relationships with suppliers and other third parties	SP-1	MIL-1	🟧■	🟧■	CSU-13 Application Security Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-4C Continuity plans are developed, at least in an ad hoc manner, to sustain and restore operation of the function	SP-1	MIL-1	🟧■	🟧■	CSU-10 Incident Response Capability
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-2B Operational environments are monitored, at least in an ad hoc manner, for anomalous behaviour that may indicate a Cyber Security event	SP-1	MIL-1	🟧■	🟧■	CSU-11 Endpoint Security Platform
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-2A Cyber Security monitoring activities are performed (e.g., periodic reviews of log data), at least in an ad hoc manner	SP-1	MIL-1	🟧■	🟧■	CSU-11 Endpoint Security Platform
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-2F Root privileges, administrative access, emergency access, and shared accounts receive additional scrutiny and monitoring	SP-1	MIL-2	🟧■	🟧■	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-1F Identities are deprovisioned within organisationally defined time thresholds when no longer required	SP-1	MIL-2	🟨■	🟧■	CSU-03 Identity and Access Management
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-2A Configuration baselines are established, at least in an ad hoc manner, for inventoried assets where it is desirable to ensure that multiple assets are configured similarly	SP-1	MIL-1	🟩■	🟧■	CSU-07 Asset Management
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-2B Configuration baselines are used, at least in an ad hoc manner, to configure assets at deployment	SP-1	MIL-1	🟩■	🟧■	CSU-07 Asset Management
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-3A Changes to inventoried assets are evaluated, at least in an ad hoc manner, before being implemented	SP-1	MIL-1	🟩■	🟧■	CSU-07 Asset Management

AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-1A Privacy requirements applicable to the organisation have been identified, even in an ad-hoc manner.	SP-1	MIL-1	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy
AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-1C There is a point of contact (person or role) to whom privacy issues could be reported, even in an ad-hoc manner.	SP-1	MIL-1	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-1A The organisation has a Cyber Security program strategy, which may be developed and managed in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-3A A strategy to architecturally isolate the organisation's IT systems from OT systems is implemented, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-1B Important customer dependencies are identified (i.e., external parties that are dependent on the delivery of the function including operating partners), at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-1A Identities are provisioned, at least in an ad hoc manner, for personnel and other entities (e.g., services, devices) who require access to assets (note that this does not preclude shared identities)	SP-1	MIL-1	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-1B Credentials are issued, at least in an ad hoc manner, for personnel and other entities that require access to assets (e.g., passwords, smart cards, certificates, keys)	SP-1	MIL-1	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-1C Identities are deprovisioned, at least in an ad hoc manner, when no longer required	SP-1	MIL-1	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-2A Access requirements, including those for remote access, are determined	SP-1	MIL-1	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-2B Access is granted to identities, at least in an ad hoc manner, based on requirements	SP-1	MIL-1	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-2C Access is revoked, at least in an ad hoc manner, when no longer required	SP-1	MIL-1	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-1A There is a point of contact (person or role) to whom Cyber Security events could be reported	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability

AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-1B Detected Cyber Security events are reported, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-1C Cyber Security events are logged and tracked, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-2A Criteria for Cyber Security event escalation are established, including Cyber Security incident declaration criteria, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-2B Cyber Security events are analysed, at least in an ad hoc manner, to support escalation and the declaration of Cyber Security incidents	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-2C Escalated Cyber Security events and incidents are logged and tracked, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-3A Cyber Security event and incident response personnel are identified and roles are assigned, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-3B Responses to escalated Cyber Security events and incidents are implemented, at least in an ad hoc manner, to limit impact to the function and restore normal operations	SP-1	MIL-1	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-ISC Domain: Informational Sharing and Communication	AESCSF-ISC-1A Information is collected from and provided to selected individuals and/or organisations, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-17 Security Metrics
AESCSF-ISC Domain: Informational Sharing and Communication	AESCSF-ISC-1B Responsibility for Cyber Security reporting obligations are assigned to personnel (e.g., internal reporting to management, external reporting to government (e.g. ACSC) or law enforcement (e.g. AFP), at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-17 Security Metrics
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-1A Logging is occurring, at least in an ad hoc manner, for assets important to the function, where possible	SP-1	MIL-1	[redacted]	[redacted]	[redacted]-11 Endpoint Security Platform
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-1A Information sources to support threat management activities are identified, at least in an ad hoc manner.	SP-1	MIL-1	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management

AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-1B Cyber Security threat information is gathered and interpreted for the function, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-2A Information sources to support Cyber Security vulnerability discovery are identified (e.g. industry associations, vendors, federal briefings, internal assessments), at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-2B Cyber Security vulnerability information is gathered and interpreted for the function, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-2C Cyber Security vulnerabilities that are considered important to the function are addressed (e.g., implement mitigating controls, apply Cyber Security patches), at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-2G Cyber Security vulnerabilities are addressed according to the assigned priority	SP-1	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-WM Domain: Workforce Management	AESCSF-WM-1A Cyber Security responsibilities for the function are identified, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-WM Domain: Workforce Management	AESCSF-WM-1B Cyber Security responsibilities are assigned to specific people, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-WM Domain: Workforce Management	AESCSF-WM-3A Cyber Security training is made available, at least in an ad hoc manner, to personnel with assigned Cyber Security responsibilities	SP-1	MIL-1	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-WM Domain: Workforce Management	AESCSF-WM-4A Cyber Security awareness activities occur, at least in an ad hoc manner	SP-1	MIL-1	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP1 Identities (users) are created, and access to assets is provisioned, before confirming if the identity (user) has a genuine need for access	SP-1	MIL-1	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP10 The continued need for an identity (user) to have access to an asset is not validated when identity (user) repositories are reviewed	SP-1	MIL-1	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP11 Identities (users) are not prohibited (by organisational policy) from connecting to critical assets using unknown or unauthorised assets	SP-1	MIL-1	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-ISC Domain: Informational Sharing and Communication	AESCSF-ISC-1C Information-sharing stakeholders are identified based on their relevance to the continued operation of the function (e.g., connected utilities, vendors,	SP-1	MIL-2	[redacted]	[redacted]	CSU-17 Security Metrics

	sector organisations, regulators, internal entities)					
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP2 Logging data is only monitored when a cyber security incident occurs	SP-1	MIL-1	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-1G Requirements for credentials are informed by the organisation's risk criteria (e.g., multifactor credentials for higher risk access) (RM-1c)	SP-1	MIL-3	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-4J Continuity plans are periodically reviewed and updated	SP-1	MIL-3	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP9 Unknown or unauthorised identities (users) and assets can connect to known assets	SP-1	MIL-3	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-AP3 Incident responders do not know which authorities (including law enforcement) should be contacted or how to contact them	SP-1	MIL-3	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-3E Cyber Security event and incident response plans are exercised at an organisation- defined frequency	SP-1	MIL-2	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-2D Alarms and alerts are configured to aid in the identification of Cyber Security events (IR-1b)	SP-1	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-1D Criteria are established for Cyber Security event detection (e.g., what constitutes an event, where to look for events)	SP-1	MIL-2	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-1E There is a repository where Cyber Security events are logged based on the established criteria	SP-1	MIL-2	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-RM Domain: Risk management	AESCSF-RM-1A There is a documented Cyber Security risk management strategy	SP-1	MIL-2	[redacted]	[redacted]	CSU-02 Improve security governance
AESCSF-RM Domain: Risk management	AESCSF-RM-2C Cyber Security risk assessments are performed to identify risks in accordance with the risk management strategy	SP-1	MIL-2	[redacted]	[redacted]	CSU-02 Improve security governance
AESCSF-ACM Domain: Asset, Change and	AESCSF-ACM-3C Changes to assets are tested prior to being deployed, whenever possible	SP-1	MIL-2	[redacted]	[redacted]	CSU-07 Asset Management

Configuration Management						
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-AP2 Remote or third-party access to assets circumvents network security controls	SP-1	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP4 Non-public, Internet-facing assets can be accessed using single-factor authentication	SP-1	MIL-2	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-WM Domain: Workforce Management	AESCSF-WM-3D Cyber Security training is provided as a prerequisite to granting access to assets that support the delivery of the function (e.g., new personnel training, personnel transfer training)	SP-1	MIL-2	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-3A Methods of communicating the current state of Cyber Security for the function are established and maintained	SP-1	MIL-2	[redacted]	[redacted]	[redacted]-11 Endpoint Security Platform
AESCSF-RM Domain: Risk management	AESCSF-RM-2D Identified Cyber Security risks are documented	SP-1	MIL-2	[redacted]	[redacted]	CSU-02 Improve security governance
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-2H Operational impact to the function is evaluated prior to deploying Cyber Security patches	SP-1	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-1D Business activities which involve the collection, processing, storage or transmission of personal information have been identified	SP-1	MIL-2	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy
AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-AP1 The function is unaware whether personal information is collected	SP-1	MIL-2	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-AP1 Operational assets can route traffic directly to the Internet	SP-1	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP5 Privileged access to one or more assets is provisioned by default	SP-1	MIL-2	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-AP1 Critical functions have not been identified	SP-1	MIL-2	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-AP2 Services and assets that support the delivery of critical functions have not been identified (IR-AP1)	SP-1	MIL-2	[redacted]	[redacted]	CSU-10 Incident Response Capability

AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP7 Identities (users) have edit (write) access to centralised logging data without a confirmed need	SP-1	MIL-2	🟩 [redacted]	🟧 [redacted]	CSU-11 Endpoint Security Platform
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP8 Third party vendors or services have privileged access that is not logged	SP-1	MIL-2	🟩 [redacted]	🟧 [redacted]	CSU-11 Endpoint Security Platform
AESCSF-WM Domain: Workforce Management	AESCSF-WM-1D Cyber Security responsibilities are documented (e.g., in position descriptions)	SP-1	MIL-2	🟩 [redacted]	🟧 [redacted]	CSU-01 Cyber Training Uplift
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP1 Operational assets are monitored only for performance and not for cyber security events	SP-2	MIL-2	🟥 [redacted]	🟨 [redacted]	CSU-11 Endpoint Security Platform
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-2E Criteria for Cyber Security event escalation, including Cyber Security incident declaration criteria, are updated at an organisation-defined frequency	SP-2	MIL-2	🟥 [redacted]	🟨 [redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-3F Cyber Security event and incident response plans address OT and IT assets important to the delivery of the function	SP-2	MIL-2	🟥 [redacted]	🟨 [redacted]	CSU-10 Incident Response Capability
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-3G Training is conducted for Cyber Security event and incident response teams	SP-2	MIL-2	🟥 [redacted]	🟨 [redacted]	CSU-10 Incident Response Capability
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-3C Information from across the organisation is available to enhance the common operating picture	SP-2	MIL-2	🟥 [redacted]	🟨 [redacted]	CSU-11 Endpoint Security Platform
AESCSF-WM Domain: Workforce Management	AESCSF-WM-2C Personnel vetting is performed at an organisation-defined frequency for positions that have access to the assets required for delivery of the function	SP-2	MIL-2	🟥 [redacted]	🟨 [redacted]	CSU-01 Cyber Training Uplift
AESCSF-RM Domain: Risk management	AESCSF-RM-AP2 Identified cyber security risks remain untreated for long periods of time	SP-2	MIL-2	🟥 [redacted]	🟨 [redacted]	CSU-02 Improve security governance
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP10 Logging data from impacted assets cannot be inspected when investigating a cyber security event	SP-2	MIL-2	🟥 [redacted]	🟨 [redacted]	CSU-11 Endpoint Security Platform
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP11 Indicators of Compromise cannot be added to security monitoring solutions that monitor critical assets	SP-2	MIL-2	🟥 [redacted]	🟨 [redacted]	CSU-11 Endpoint Security Platform
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-1C Log data are being aggregated within the function	SP-2	MIL-2	🟥 [redacted]	🟨 [redacted]	CSU-11 Endpoint Security Platform

AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-1C Supplier dependencies are identified according to established criteria	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2F Agreements with suppliers and other external entities include Cyber Security requirements	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2G Evaluation and selection of suppliers and other external entities includes consideration of their ability to meet Cyber Security requirements	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2H Agreements with suppliers require notification of Cyber Security incidents related to the delivery of the product or service	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2I Suppliers and other external entities are periodically reviewed for their ability to continually meet the Cyber Security requirements	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-2D Criteria for Cyber Security event escalation, including Cyber Security incident criteria, are established based on the potential impact to the function	SP-2	MIL-2	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-RM Domain: Risk management	AESCSF-RM-2G Cyber Security risk analysis is informed by network (IT and/or OT) architecture	SP-2	MIL-2	[redacted]	[redacted]	CSU-02 Improve security governance
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-2C Monitoring and analysis requirements have been defined for the function and address timely review of event data	SP-2	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-2E Indicators of anomalous activity have been defined and are monitored across the operational environment	SP-2	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-2F Monitoring activities are aligned with the function's threat profile (TVM-1d)	SP-2	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-1D A threat profile for the function is established that includes characterisation of likely intent, capability, and target of threats to the function	SP-2	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-AP3 Critical assets cannot be isolated from non-critical assets in response to a cyber security threat or incident	SP-2	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation

AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-1D Customer dependencies are identified according to established criteria	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-1E Single-source and other essential dependencies are identified	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-1F Dependencies are prioritised	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-3B Monitoring data are aggregated to provide an understanding of the operational state of the function (i.e., a common operating picture; a COP may or may not include visualisation or be presented graphically)	SP-2	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-1D Inventoried assets are prioritised based on their importance to the delivery of the function	SP-2	MIL-2	[redacted]	[redacted]	CSU-07 Asset Management
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-1D The Cyber Security program strategy defines the organisation's approach to provide program oversight and governance for Cyber Security activities	SP-2	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-1E The Cyber Security program strategy defines the structure and organisation of the Cyber Security program	SP-2	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-1F The Cyber Security program strategy is approved by senior management	SP-2	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-2D Adequate funding and other resources (i.e., people and tools) are provided to establish and operate a Cyber Security program aligned with the program strategy	SP-2	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-3D Cyber Security event and incident response is performed according to defined procedures that address all phases of the incident life cycle (e.g., triage, handling, communication, coordination, and closure)	SP-2	MIL-2	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-RM Domain: Risk management	AESCSF-RM-1B The Cyber Security risk management strategy provides an approach for risk prioritisation, including consideration of impact	SP-2	MIL-2	[redacted]	[redacted]	CSU-02 Improve security governance

AESCSF-WM Domain: Workforce Management	AESCSF-WM-2D Personnel transfer procedures address Cyber Security	SP-2	MIL-2	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2D Contracts and agreements with third parties incorporate sharing of Cyber Security threat information	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-2F There is a repository where escalated Cyber Security events and Cyber Security incidents are logged and tracked to closure	SP-2	MIL-2	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-RM Domain: Risk management	AESCSF-RM-2E Identified Cyber Security risks are analysed to prioritise response activities in accordance with the Cyber Security risk management strategy	SP-2	MIL-2	[redacted]	[redacted]	CSU-02 Improve security governance
AESCSF-RM Domain: Risk management	AESCSF-RM-2F Identified Cyber Security risks are monitored in accordance with the Cyber Security risk management strategy	SP-2	MIL-2	[redacted]	[redacted]	CSU-02 Improve security governance
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-1F Identified threats are analysed and prioritised	SP-2	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-1G Threats are addressed according to the assigned priority	SP-2	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-AP3 Controls are not updated in response to new and emerging high priority cyber threats	SP-2	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-1D Identity repositories are periodically reviewed and updated to ensure validity (i.e., to ensure that the identities still need access)	SP-2	MIL-2	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-2D Access requirements incorporate least privilege and separation of duties principles	SP-2	MIL-2	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP6 Logging data from critical assets is only stored on the asset and not centralised	SP-2	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-3D Change management practices address the full life cycle of assets (i.e., acquisition, deployment, operation, retirement)	SP-2	MIL-2	[redacted]	[redacted]	CSU-07 Asset Management

AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-AP1 Changes to Internet-facing assets are not assessed or tested to identify potential cyber security vulnerabilities arising from the change itself, prior to implementation	SP-2	MIL-2	[redacted]	[redacted]	CSU-07 Asset Management
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-AP2 The management of asset inventories is not linked to data governance or business impact assessment activities	SP-2	MIL-2	[redacted]	[redacted]	CSU-07 Asset Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-1E Credentials are periodically reviewed to ensure that they are associated with the correct person or entity	SP-2	MIL-2	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP2 A complete and current register of identities (users) with privileged access is not maintained	SP-2	MIL-2	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP3 Identity (user) deprovisioning is not informed and supported by organisational risk criteria (RM-1C)	SP-2	MIL-2	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP6 Identities (users) have been provisioned with access to assets which breaches a segregation of duties requirement	SP-2	MIL-2	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-4F Continuity plans are evaluated and exercised	SP-2	MIL-2	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-RM Domain: Risk management	AESCSF-RM-AP3 Assets are risk-assessed in isolation. Interdependencies with other assets are not considered	SP-2	MIL-2	[redacted]	[redacted]	CSU-02 Improve security governance
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP3 Normal asset operation is not sufficiently baselined to support the identification of abnormal asset operation	SP-2	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP9 Indicators of Compromise (IOCs) are only monitored and considered during or after a cyber security incident	SP-2	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-AP2 Internet-facing assets are not periodically assessed for cyber security vulnerabilities	SP-2	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-3B A Cyber Security architecture is in place to enable segmentation, isolation, and other requirements that support the Cyber Security strategy	SP-2	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity	AESCSF-CPM-3C Architectural segmentation and isolation is maintained according to a documented plan	SP-2	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain

Program Management						Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-4A Software to be deployed on assets that are important to the delivery of the function is developed using secure software development practices	SP-2	MIL-2	■	■	CSU-05 ICT Domain Network Segmentation
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-4D Business impact analyses inform the development of continuity plans	SP-2	MIL-2	■	■	CSU-10 Incident Response Capability
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-2C The design of configuration baselines includes Cyber Security objectives	SP-2	MIL-2	■	■	CSU-07 Asset Management
AESCSF-RM Domain: Risk management	AESCSF-RM-AP1 Identified risks are not periodically reviewed	SP-2	MIL-2	■	■	CSU-02 Improve security governance
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-1C Inventory attributes include information to support the Cyber Security strategy (e.g., location, asset owner, applicable Security requirements, service dependencies, service level agreements, and conformance of assets to relevant industry standards)	SP-2	MIL-2	■	■	CSU-07 Asset Management
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-1B The Cyber Security program strategy defines objectives for the organisation's Cyber Security activities	SP-2	MIL-2	■	■	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-1C The Cyber Security program strategy and priorities are documented and aligned with the organisation's strategic objectives and risk to critical infrastructure	SP-2	MIL-2	■	■	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-2C The Cyber Security program is established according to the Cyber Security program strategy	SP-2	MIL-2	■	■	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-2E Senior management sponsorship for the Cyber Security program is visible and active (e.g., the importance and value of Cyber Security activities is regularly communicated by senior management)	SP-2	MIL-2	■	■	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-2F If the organisation develops or procures software, secure software development practices are sponsored as an element of the Cyber Security program	SP-2	MIL-2	■	■	CSU-05 ICT Domain Network Segmentation

AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-2G The development and maintenance of Cyber Security policies is sponsored	SP-2	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-CPM Domain: Cybersecurity Program Management	AESCSF-CPM-2H Responsibility for the Cyber Security program is assigned to a role with requisite authority	SP-2	MIL-2	[redacted]	[redacted]	CSU-05 ICT Domain Network Segmentation
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2C Identified Cyber Security dependency risks are entered into the risk register (RM-2j)	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2E Cyber Security requirements are established for suppliers according to a defined practice, including requirements for secure software development practices where appropriate	SP-2	MIL-2	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-WM Domain: Workforce Management	AESCSF-WM-3B Cyber Security knowledge, skill, and ability gaps are identified	SP-2	MIL-2	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-WM Domain: Workforce Management	AESCSF-WM-3C Identified gaps are addressed through recruiting and/or training	SP-2	MIL-2	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-2E Access requests are reviewed and approved by the asset owner	SP-2	MIL-2	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-4E Recovery time objectives (RTO) and recovery point objectives (RPO) for the function are incorporated into continuity plans	SP-2	MIL-2	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-2D Cyber Security vulnerability information sources that address all assets important to the function are monitored	SP-2	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-2E Cyber Security vulnerability assessments are performed (e.g., architectural reviews, penetration testing, Cyber Security exercises, vulnerability identification tools)	SP-2	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-2F Identified Cyber Security vulnerabilities are analysed and prioritised	SP-2	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-1E The organisation's personal information holdings are documented	SP-2	MIL-2	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy

AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-1F A privacy policy has been documented and communicated within the organisation and the general public	SP-2	MIL-2	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy
AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-1G The organisation's requirements for handling of personal information have been defined within the privacy policy	SP-2	MIL-2	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy
AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-1H Specific roles and accountabilities have been assigned for privacy management within the organisation	SP-2	MIL-2	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy
AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-1I A privacy management plan has been implemented to govern the organisation's ongoing compliance with applicable privacy requirements	SP-2	MIL-2	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy
AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-1J Privacy related risks have been identified, assessed and documented in a risk register	SP-2	MIL-2	[redacted]	[redacted]	CSU-09 Data Sharing & Privacy
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP7 Identities (users) cannot be individually identified and attributed to a person	SP-2	MIL-2	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-ISC Domain: Informational Sharing and Communication	AESCSF-ISC-1D Information is collected from and provided to identified information-sharing stakeholders	SP-2	MIL-2	[redacted]	[redacted]	CSU-17 Security Metrics
AESCSF-ISC Domain: Informational Sharing and Communication	AESCSF-ISC-1E Technical sources are identified that can be consulted on Cyber Security issues	SP-2	MIL-2	[redacted]	[redacted]	CSU-17 Security Metrics
AESCSF-ISC Domain: Informational Sharing and Communication	AESCSF-ISC-1F Provisions are established and maintained to enable secure sharing of sensitive or classified information	SP-2	MIL-2	[redacted]	[redacted]	CSU-17 Security Metrics
AESCSF-ISC Domain: Informational Sharing and Communication	AESCSF-ISC-1G Information-sharing practices address both standard operations and emergency operations	SP-2	MIL-2	[redacted]	[redacted]	CSU-17 Security Metrics
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP4 Alerts and alarms are not configured to include security events	SP-2	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-AP5 Logging data is not time synchronised	SP-2	MIL-2	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-TVM Domain: Threat and Vulnerability Management	AESCSF-TVM-1E Threat information sources that address all components of the threat profile are prioritised and monitored	SP-2	MIL-2	[redacted]	[redacted]	CSU-14 Centralised Logging & Threat Management
AESCSF-WM Domain: Workforce Management	AESCSF-WM-1C Cyber Security responsibilities are assigned to specific roles, including external service providers	SP-2	MIL-2	[redacted]	[redacted]	CSU-01 Cyber Training Uplift

AESCSF-WM Domain: Workforce Management	AESCSF-WM-4B Objectives for Cyber Security awareness activities are established and maintained	SP-2	MIL-2	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-WM Domain: Workforce Management	AESCSF-WM-4C Cyber Security awareness content is based on the organisation's threat profile (TVM-1d)	SP-2	MIL-2	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-3D Monitoring data are aggregated to provide near-real-time understanding of the Cyber Security state for the function to enhance the common operating picture	SP-2	MIL-3	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-3O Restored assets are configured appropriately and inventory information is updated following execution of response plans	SP-2	MIL-3	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-SA Domain: Situational Awareness	AESCSF-SA-2G Monitoring requirements are based on the risk to the function	SP-2	MIL-3	[redacted]	[redacted]	CSU-11 Endpoint Security Platform
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-3K Cyber Security event and incident response plans are reviewed and updated at an organisation-defined frequency	SP-2	MIL-3	[redacted]	[redacted]	CSU-10 Incident Response Capability
AESCSF-WM Domain: Workforce Management	AESCSF-WM-2H A formal accountability process that includes disciplinary actions is implemented for personnel who fail to comply with established Security policies and procedures	SP-2	MIL-3	[redacted]	[redacted]	CSU-01 Cyber Training Uplift
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2L Agreements with suppliers require notification of vulnerability-inducing product defects throughout the intended life cycle of delivered products	SP-2	MIL-3	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-2I Anomalous access attempts are monitored as indicators of Cyber Security events	SP-2	MIL-3	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-EDM Domain: Supply Chain and External Dependencies Management	AESCSF-EDM-2M Acceptance testing of procured assets includes testing for Cyber Security requirements	SP-2	MIL-3	[redacted]	[redacted]	CSU-13 Application Security Management
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-3E Changes to assets are tested for Cyber Security impact prior to being deployed	SP-2	MIL-3	[redacted]	[redacted]	CSU-07 Asset Management
AESCSF-IAM Domain: Identity and Access Management	AESCSF-IAM-AP8 Unusual or suspicious access to assets is not monitored by security monitoring solutions	SP-2	MIL-3	[redacted]	[redacted]	CSU-03 Identity and Access Management
AESCSF-IAM Domain: Identity	AESCSF-IAM-2G Access privileges are reviewed and updated to ensure validity, at an organisationally defined frequency	SP-2	MIL-3	[redacted]	[redacted]	CSU-03 Identity and

and Access Management						Access Management
AESCSF-APM Domain: Australian Privacy Management	AESCSF-APM-1L The organisation provides privacy training to staff responsible for handling personal information	SP-2	MIL-3	■	■	CSU-09 Data Sharing & Privacy
AESCSF-ACM Domain: Asset, Change and Configuration Management	AESCSF-ACM-1F The asset inventory is current (as defined by the organisation)	SP-2	MIL-3	■	■	CSU-07 Asset Management
AESCSF-IR Domain: Event and Incident Response and Continuity of Operations	AESCSF-IR-3J Cyber Security event and incident response personnel participate in joint Cyber Security exercises with other organisations (e.g., table top, simulated incidents)	SP-2	MIL-3	■	■	CSU-10 Incident Response Capability
AESCSF-WM Domain: Workforce Management	AESCSF-WM-1E Cyber Security responsibilities and job requirements are reviewed and updated as appropriate	SP-2	MIL-3	■	■	CSU-01 Cyber Training Uplift
AESCSF-WM Domain: Workforce Management	AESCSF-WM-AP1 Cyber security capabilities are dependent on one or two key personnel and no succession plan is in place to ensure retention of critical knowledge	SP-2	MIL-3	■	■	CSU-01 Cyber Training Uplift

C.2 Work Packages within the Initiatives

Each initiative may contain multiple work packages to deliver the required capabilities – the table below lists work packages where specific improvement is required for IT, OT, Common IT/OT, or Corporate allocations – i.e. structured to enable simple cost allocation where required across regulated and non-regulated elements for the same overall initiative.

Table 18 - Work packages where specific improvement is required for IT, OT, Common IT/OT, or Corporate allocation

Work Package Full Name	Work Package Allocation Type	Work Package Name	Parent Initiative Name	Primary Security Alignment Goal	Primary Security Domain
CSU-01.01 Enterprise Cyber Training Programme Materials (Corporate)	Corporate	01 Enterprise Cyber Training Programme Materials	CSU-01 Cyber Training Uplift	Create culture of security	Information Security Program
CSU-01.02 Externally run cyber exercises (Corporate)	Corporate	02 Externally run cyber exercises	CSU-01 Cyber Training Uplift	Create culture of security	Information Security Program
CSU-01.03 Externally built Facilities, Materials and Infrastructure for ongoing exercises (Corporate)	Corporate	03 Externally built Facilities, Materials and Infrastructure for ongoing exercises	CSU-01 Cyber Training Uplift	Create culture of security	Information Security Program

CSU-02.01 Build Risk Management Plan (Common IT/OT)	Common IT/OT	01 Build Risk Management Plan	CSU-02 Improve security governance	Improve security governance	Organizational Structure
CSU-02.02 Build the supporting Frameworks (Common IT/OT)	Common IT/OT	02 Build the supporting Frameworks	CSU-02 Improve security governance	Improve security governance	Organizational Structure
CSU-02.03 Populate and maintain the Frameworks (Common IT/OT)	Common IT/OT	03 Populate and maintain the Frameworks	CSU-02 Improve security governance	Improve security governance	Organizational Structure
CSU-02.04 Run the governance processes (Common IT/OT)	Common IT/OT	04 Run the governance processes	CSU-02 Improve security governance	Improve security governance	Organizational Structure
CSU-03.01 Implement and Operate IDAM Solution (Common IT/OT)	Common IT/OT	01 Implement and Operate IDAM Solution	CSU-03 Identity and Access Management	Create culture of security	Security Culture and Awareness
CSU-03.02 Implement and Operate PAM Solution (Common IT/OT)	Common IT/OT	02 Implement and Operate PAM Solution	CSU-03 Identity and Access Management	Create culture of security	Security Culture and Awareness
CSU-03.04 Establish and Operate services for network services monitoring, notifications, configuration and rollback (Common IT/OT)	Common IT/OT	04 Establish and Operate services for network services monitoring, notifications, configuration and rollback	CSU-03 Identity and Access Management	Create culture of security	Security Culture and Awareness
CSU-04.01 Define framework and services for network access control (OT)	OT	01 Define framework and services for network access control	CSU-04 Network Access Control Implementation	Secure the Infrastructure	Security Risk Management
CSU-04.02 Establish and operate management services for network access control (OT)	OT	02 Establish and operate management services for network access control	CSU-04 Network Access Control Implementation	Secure the Infrastructure	Security Risk Management
CSU-04.03 Manage and perform connections and disconnections (Common IT/OT)	Common IT/OT	03 Manage and perform connections and disconnections	CSU-04 Network Access Control Implementation	Secure the Infrastructure	Security Risk Management
CSU-04.04 Maintain and refresh infrastructure (IT)	IT	04 Maintain and refresh infrastructure	CSU-04 Network Access Control Implementation	Secure the Infrastructure	Security Risk Management
CSU-05.01 Plan and design consolidated network (Common IT/OT)	Common IT/OT	01 Plan and design	CSU-05 ICT Domain Network Segmentation	Secure the Infrastructure	Security Policies

		consolidated network			
CSU-05.02 Build new network infrastructure (Common IT/OT)	Common IT/OT	02 Build new network infrastructure	CSU-05 ICT Domain Network Segmentation	Secure the Infrastructure	Security Policies
CSU-05.03 Build and configure network/s (Common IT/OT)	Common IT/OT	03 Build and configure network/s	CSU-05 ICT Domain Network Segmentation	Secure the Infrastructure	Security Policies
CSU-05.05 Maintain and refresh infrastructure (Common IT/OT)	Common IT/OT	05 Maintain and refresh infrastructure	CSU-05 ICT Domain Network Segmentation	Secure the Infrastructure	Security Policies
CSU-06.Planning and Coordination of OT Deliverables within Cyber domain (OT)	OT	Planning and Coordination of OT Deliverables within Cyber domain	CSU-06 Information Security Roadmap	Manage compliance obligations	Security Compliance Management
CSU-06.Planning and Coordination of IT Deliverables within Cyber domain (IT)	IT	Planning and Coordination of IT Deliverables within Cyber domain	CSU-06 Information Security Roadmap	Manage compliance obligations	Security Compliance Management
CSU-07.Accountability Model (Common IT/OT)	Common IT/OT	Accountability Model	CSU-07 Asset Management	Secure the Infrastructure	Security Audit
CSU-07.Asset Lifecycle Management Plan (OT)	OT	Asset Lifecycle Management Plan	CSU-07 Asset Management	Secure the Infrastructure	Security Audit
CSU-07.Asset Inventory Collection (OT)	OT	Asset Inventory Collection	CSU-07 Asset Management	Secure the Infrastructure	Security Audit
CSU-07.Asset Lifecycle Management Plan (IT)	IT	Asset Lifecycle Management Plan	CSU-07 Asset Management	Secure the Infrastructure	Security Audit
CSU-07.Asset Inventory Collection (IT)	IT	Asset Inventory Collection	CSU-07 Asset Management	Secure the Infrastructure	Security Audit
CSU-07.Asset Management (OT)	OT	Asset Management	CSU-07 Asset Management	Secure the Infrastructure	Security Audit
CSU-07.Asset Management (IT)	IT	Asset Management	CSU-07 Asset Management	Secure the Infrastructure	Security Audit
CSU-08.External Cyber Advisory (IT)	IT	External Cyber Advisory	CSU-08 Security Compliance and Governance regulations	Manage compliance obligations	Identity and Access Management
CSU-08.External Cyber Advisory (OT)	OT	External Cyber Advisory	CSU-08 Security Compliance and	Manage compliance obligations	Identity and Access

			Governance regulations		Management
CSU-08.Internal and External Cyber audit and compliance (IT)	IT	Internal and External Cyber audit and compliance	CSU-08 Security Compliance and Governance regulations	Manage compliance obligations	Identity and Access Management
CSU-08.Internal and External Cyber audit and compliance (OT)	OT	Internal and External Cyber audit and compliance	CSU-08 Security Compliance and Governance regulations	Manage compliance obligations	Identity and Access Management
CSU-08.Maintain knowledge, relevance, coverage and compliance of Cyber RMP (Common IT/OT)	Common IT/OT	Maintain knowledge, relevance, coverage and compliance of Cyber RMP	CSU-08 Security Compliance and Governance regulations	Manage compliance obligations	Identity and Access Management
CSU-09.Data classification and obfuscation requirements and classification (Corporate)	Corporate	Data classification and obfuscation requirements and classification	CSU-09 Data Sharing & Privacy	Protect data	Hardware Asset Management
CSU-09.External Data Sharing Solution (Corporate)	Corporate	External Data Sharing Solution	CSU-09 Data Sharing & Privacy	Protect data	Hardware Asset Management
CSU-09.Data Audit Solution - Data Activity (Corporate)	Corporate	Data Audit Solution - Data Activity	CSU-09 Data Sharing & Privacy	Protect data	Hardware Asset Management
CSU-09.Data Audit Solution - Data Loss Prevention (Corporate)	Corporate	Data Audit Solution - Data Loss Prevention	CSU-09 Data Sharing & Privacy	Protect data	Hardware Asset Management
CSU-09.Data Audit Solution - Compliance, Remediation and Controls (Corporate)	Corporate	Data Audit Solution - Compliance, Remediation and Controls	CSU-09 Data Sharing & Privacy	Protect data	Hardware Asset Management
CSU-09.Data Audit Solution - DevOps Management (Corporate)	Corporate	Data Audit Solution - DevOps Management	CSU-09 Data Sharing & Privacy	Protect data	Hardware Asset Management
CSU-09.Data Audit Solution - Data Privacy Classifications and Management (Corporate)	Corporate	Data Audit Solution - Data Privacy Classifications and Management	CSU-09 Data Sharing & Privacy	Protect data	Hardware Asset Management

CSU-10.External Threat monitoring, response and recovery solution (Corporate)	Corporate	External Threat monitoring, response and recovery solution	CSU-10 Incident Response Capability	Protect Data	Data Security & Privacy
CSU-10.3rd Party service provide management and administration (Corporate)	Corporate	3rd Party service provide management and administration	CSU-10 Incident Response Capability	Protect Data	Data Security & Privacy
CSU-10.Infrastructure and plant monitoring solutions (Corporate)	Corporate	Infrastructure and plant monitoring solutions	CSU-10 Incident Response Capability	Protect Data	Data Security & Privacy
CSU-10.Security Management Platform (Corporate)	Corporate	Security Management Platform	CSU-10 Incident Response Capability	Protect Data	Data Security & Privacy
CSU-10.Build and Operate Incident Response capabilities (Corporate)	Corporate	Build and Operate Incident Response capabilities	CSU-10 Incident Response Capability	Protect Data	Data Security & Privacy
CSU-10.Acquire and operate compliance and forensics processes and services (Corporate)	Corporate	Acquire and operate compliance and forensics processes and services	CSU-10 Incident Response Capability	Protect Data	Data Security & Privacy
CSU-11.Endpoint Solution (Corporate)	Corporate	Endpoint Solution	CSU-11 Endpoint Security Platform	Compliance obligations	Network Security
CSU-11.Endpoint Configuration Management (Corporate)	Corporate	Endpoint Configuration Management	CSU-11 Endpoint Security Platform	Compliance obligations	Network Security
CSU-12.Network Infrastructure Design Audit (Common IT/OT)	Common IT/OT	Network Infrastructure Design Audit	CSU-12 OT Security Architecture Re-design/Uplift	Secure the Infrastructure	Endpoint Security
CSU-12.Network Infrastructure accountability model and implementation (Common IT/OT)	Common IT/OT	Network Infrastructure accountability model and implementation	CSU-12 OT Security Architecture Re-design/Uplift	Secure the Infrastructure	Endpoint Security
CSU-13.Application Inventory and SOEs (Corporate)	Corporate	Application Inventory and SOEs	CSU-13 Application Security Management	Secure the Infrastructure	Application Security

CSU-13.Infrastructure, device and application configuration management implementation and operation (Corporate)	Corporate	Infrastructure, device and application configuration management implementation and operation	CSU-13 Application Security Management	Secure the Infrastructure	Application Security
CSU-13.Application development processes and solution (Corporate)	Corporate	Application development processes and solution	CSU-13 Application Security Management	Secure the Infrastructure	Application Security
CSU-14.Implement logging and threat management solution, processes and services (Corporate)	Corporate	Implement logging and threat management solution, processes and services	CSU-14 Centralised Logging & Threat Management	Detect & Respond to Threats	Physical Security
CSU-14.Operate logging and threat management (Corporate)	Corporate	Operate logging and threat management	CSU-14 Centralised Logging & Threat Management	Detect & Respond to Threats	Physical Security
CSU-15.Implement forensic tooling (Corporate)	Corporate	Implement forensic tooling	CSU-15 Forensic investigation tooling to support incident response	Detect & Respond to Threats	Security Incident Management
CSU-15.Operate forensic response capabilities (Corporate)	Corporate	Operate forensic response capabilities	CSU-15 Forensic investigation tooling to support incident response	Detect & Respond to Threats	Security Incident Management
CSU-16.Design storage architecture (Corporate)	Corporate	Design storage architecture	CSU-16 Protection of Backups and Archives	Secure the Infrastructure	Human Resource Security
CSU-16.Implement backup restoration solution (Corporate)	Corporate	Implement backup restoration solution	CSU-16 Protection of Backups and Archives	Secure the Infrastructure	Human Resource Security
CSU-16.Implement storage and backup testing programs (Corporate)	Corporate	Implement storage and backup testing programs	CSU-16 Protection of Backups and Archives	Secure the Infrastructure	Human Resource Security
CSU-17.Define and operate Industry standard metrics program (Corporate)	Corporate	Define and operate Industry standard metrics program	CSU-17 Security Metrics	Manage Compliance Obligations	Security Metrics
CSU-18.Define and build business impact assessment	Corporate	Define and build business impact	CSU-18 Business Impact	Manage Compliance Obligations	InfoSec in Business

framework and program (Corporate)		assessment framework and program	Assessment Reviews		Continuity Planning
CSU-18.Operate and manage the business impact assessment capabilities (Corporate)	Corporate	Operate and manage the business impact assessment capabilities	CSU-18 Business Impact Assessment Reviews	Manage Compliance Obligations	InfoSec in Business Continuity Planning

[redacted] [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Power and Water Corporation

55 Mitchell Street, Darwin NT 0800

Phone 1800 245 092

powerwater.com.au