Technology program GAAR 2023-27

Cyber Security

Table of Contents

1 Document Background

1.1 Purpose of this document

The purpose of this document is to outline a business case for a proposed program of work that will form part of AusNet's Technology GAAR submission.

1.2 References

Document	Version	Author
AusNet Services FY19-FY23 Technology Plan	V1.0	AusNet Digital
2021 Gas Business Plan	V1.0	Joanne Soysa
GAAR Technology Strategy 2024-2028	V1.0	Ausnet Digital

1.3 Document History

Date	Version	Comment	Author
15/2/2022	V0.2	Initial Document	Mathew Abraham
01/06/2022	V0.3	Amendments for review	Mathew Abraham
13/06/2022	V.04	Post review amendments	Mathew Abraham

1.4 Approvals

Position
Technology Leadership Team

2 Executive summary

2.1 Program summary

The table below provides a summary of the Cyber Security program. Additional information is provided following the table and throughout the brief.

Table 2.1: Summary table

Key objective(s) of the program	The ongoing objective of cyber security at AusNet are to: • [C-I-C]						
Key benefits	• [C-I-C]						
Cost allocation	Electricity Distribution	24%	Electricity Transmission	64%			
	Gas Distribution	12%					
Program type	**Recurrent**	☒					
	Non-Recurrent	☒					
Program timings	Program duration:	5 years					
Expenditure forecast	**($m)**	**FY24**	**FY25**	**FY26**	**FY27**	**FY28**	**Total**
	Capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$7.92
	Opex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$0.96
	Gas Distribution Cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$8.88**
	Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$74.39
Estimated life of system	Cyber security is not a static goal to be achieved, it is a continuously evolving, robust framework to mitigate the risk of attack and effectively respond to threats, that requires ongoing vigilance.						

Program Brief

Customer engagement	This program was proposed (and approved) as part of AusNet's Electricity Distribution Price Reset (EDPR) and Transmission Revenue Review (TRR) submissions. This brief pertains to the Gas Access Arrangement (GAAR) allocation of these cyber security costs. We have undertaken significant stakeholder engagement. As part of the EDPR process, we held deep dive workshops with stakeholders on ICT. In that engagement, we described the importance and need for ICT expenditure to meet our customers' evolving needs and to support compliance with regulatory and legal obligations. As part of the TRR, our cyber security proposal was presented to the Customer Advisory Panel (CAP). We acknowledge the feedback received from both sessions and have taken it into consideration when proposing the most appropriate option for this business case. This brief has also taken into consideration: • The challenge we received from stakeholders as part of the GAAR engagement process to minimise discretionary IT spend where possible – a challenge consistent with the broader feedback we received on our capital investments. • Recent customer engagement studies conducted by AusNet, including the Energy Sentiments Survey (2021) and the AusNet Listening Report "Engaging Victorians on the Future of the Gas Networks" (2021).

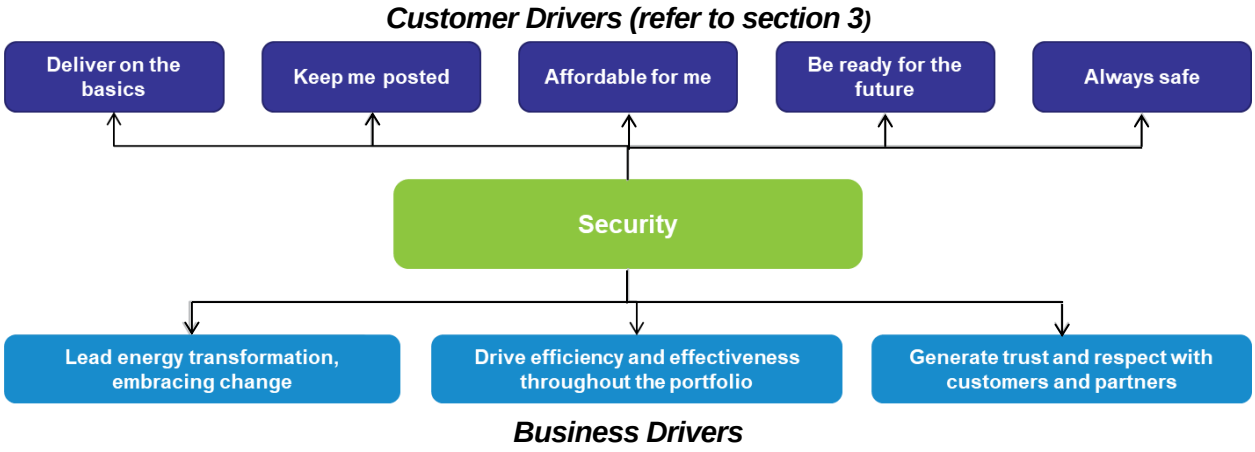
[C-I-C]

Program Brief

[C-I-C]

[C-I-C].

Program Brief



Alignment with the AER ICT expenditure assessment framework

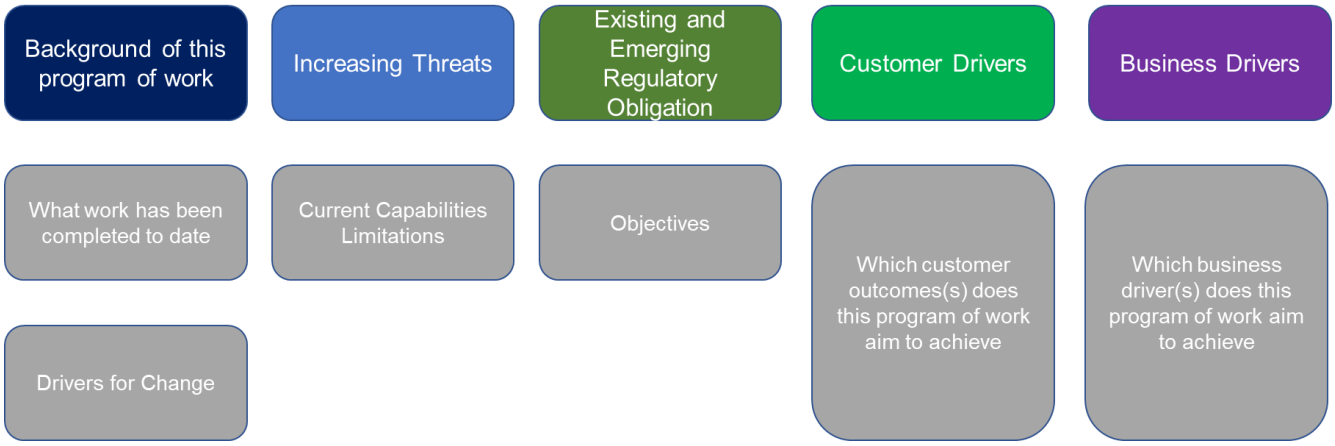
In accordance with the framework outlined in the AER – Guidance Note – Non-network ICT capex assessment approach for Gas distributors (28 November 2019), we have categorised 45% of this program as recurrent expenditure, on the basis that it relates to a compliance requirement, and that an ongoing refresh of AusNet's cyber security infrastructure is a cost that must be incurred periodically to comply with regulatory requirements.

Consistent with AusNet's internal practices, we have developed this detailed business case. We have also undertaken an NPV analysis for the non-recurrent proportion to weigh the costs and benefits of each option to help demonstrate the need for the investment and determine the appropriate option to take forward.

3 Context

This chapter provides an overview of the context in which this program of work is operating, and the figure below outlines four key areas to be discussed.

Figure 3-1 Key areas of the context to be discussed



3.1 Background

[C-I-C].

3.2 Increasing threats

[C-I-C]

3.3 Existing and emerging regulatory obligations

[C-I-C]

3.4 Objective(s)

[C-I-C]

3.5 Customer drivers

Through customer research carried out by AusNet, a succinct list of key customer values and priorities were identified. These customer drivers are:

- **delivering basic services** – deliver on the basics.
- **keeping customers informed** – keep me posted.
- **affordable services** – affordable for me.
- **adaptability** – be ready for the future.
- **safety** – always safe.

Additional information on each of these customer outcomes is provided in the overarching Technology GAAR submission FY2024-2028.

This program of work proposed by AusNet is considered to be directly linked to all of these five customer outcomes, and materially affect the reliability and security of the operation of the Distribution network.

Program Brief

We are **delivering on the basics** and **always safe** through upholding the security of critical systems which manage, monitor and control AusNet's network, and **keeping me posted** by ensuring that AusNet can continue to keep customers informed of outages or incidents. Also, this program is **affordable for me** and **ready for the future** as by taking proactive action to invest in cyber security, AusNet will inhibit future attacks and in turn limit the often-high costs associated with remediation.

We will further explore these customer drivers in the discussions of each of the options.

3.6 Business drivers

In the face of significant industry disruption resulting in a period of substantial uncertainty and increasing complexity across the industry, AusNet has selected four key business drivers which set the direction for the business.

These business drivers are:

- Maintain current service performance.
- Lead energy transformation, embracing change.
- Drive effectiveness throughout the portfolio.
- Generate trust and respect with customers and partners.

This program of work is essential to all four business drivers, through enhanced cyber protection capabilities that contribute to confidence in the business' ability to ensure security of supply. This enhanced security capability also enables the adoption of new and changing technologies. These issues are further explored in the discussions of each of the options we have considered.

In addition, the following security-related drivers have also been identified for the program:

[C-I-C]

3.7 Approach to developing expenditure forecast

For each program brief, a consistent approach is used to develop programs of work and the associated expenditure forecast for the regulatory period FY 2024-2028 regulatory period.

A full overview of the approach can be found in section 3.2 of the "*AusNet – Gas Distribution Revenue Review – Technology Strategy Document*".

To develop each program of work and associated expenditure, the following steps were taken:

- Needs analysis to identify areas of the network and business processes that require investment over the upcoming regulatory period.

Program Brief

- Bottom-up discussion with business and technology architects and delivery leads to develop options to address the investment need, including scope, key objectives, and drivers influencing the requirement for the programs.
- Consideration of different options to achieve the objectives of the program and analysis of their relative costs, benefits, and risks.
- Top-down view to ensure that the Technology Strategy investment portfolio represents prudent and efficient expenditure for the upcoming period, relative to AusNet's previous expenditure and also benchmarked against other comparable Distribution businesses.

4 Options

4.1 Overview

This section provides an overview of the three options we considered to address the requirement to meet MIL: 3. As mentioned in Section 3.3, these options represent a different approach and set of activities within each domain.

Table 4-1 Brief overview of the options

A brief overview of each of the options	
Option 1	[C-I-C]
Option 2 **(Recommended)**	[C-I-C]
Option 3	[C-I-C]

4.2 Option #1 [C-I-C]

This option involves [C-I-C].

Costs

[C-I-C]This is based on the gas allocation of total program costs to the gas distribution business.

Table 4-2 Costs of Option 1

($m)	FY24	FY25	FY26	FY27	FY28	Total
Gas Distribution capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$6.52
Gas Distribution opex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$0.96
Gas Distribution total cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$7.48**
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$41.56

Risks

The below table outlines the various risks associated with each domain, ranked according to our risk matrix. See Figure 6-1 for additional information on this rating system. Overall, this option is rated high risk.

Table 4-3 Risks for Option 1

	Domain	Risks	Consequence	Likelihood	Risk rating
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]

	Domain	Risks	Consequence	Likelihood	Risk rating
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]

Alignment to objectives

We do not consider that this option will achieve the intended objectives of this program of work, as shown in the table below.

Table 4-4 Objectives analysis of Option 1

Objective	Comments
[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]

[C-I-C]

Table 4-5 Business related drivers of Option 1

Business drivers	How this program achieves this
[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]

Alignment to Business related drivers of expenditure

As discussed in Section 3.6, there are four business drivers that AusNet has identified and is focusing on over the next regulatory period. The table below highlights how this option will input into the initiatives where relevant. Where we consider that a business driver is not directly relevant to the option, 'N/A' is applied.

Table 4-6 Business related drivers of Option 1

Business drivers	How this program achieves this
C-I-C	C-I-C
C-I-C	C-I-C
C-I-C	C-I-C
C-I-C	C-I-C

4.3 Option #2 [C-I-C])

- [C-I-C]

- [C-I-C]

Alignment to objectives

We consider that this option achieves all the intended objectives of this program of work, as shown in the table below.

Table 4-7 Objectives analysis of Option 2

Objective		Comments
[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]

Program Brief

Costs

The investment includes technology solutions and project implementation for both in-house and Managed Security Services to uplift the capabilities to MIL: 3 across all domains.

Table 4-8 Costs of Option 2

($m)	FY24	FY25	FY26	FY27	FY28	Total
Capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$7.92
Opex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$0.96
Gas Distribution cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$8.88**
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$74.39

Benefits

- [C-I-C].

Risks

There are risks associated with the implementation of this option, as highlighted in the table below. Based on the consequence and likelihood of each risk, we have rated each of the individual risks blue, green, yellow, orange or red (order of severity). See Figure 6-1 for additional information on this rating system.

While the consequence of the below risks are the same as Option 1, the likelihood of the risk eventuating decreases generally as MIL: 3 capabilities are introduced. We consider that, overall, this option is rated medium risk.

Table 4-9 Risks for Option 2

	Domain	Risks	Consequence	Likelihood	Risk rating
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]

Alignment to customer related drivers of expenditure

As discussed in Section 3.5, five key customer outcomes have been identified through discussions with customers. The table below highlights how this option will achieve these outcomes. Where we consider that a customer outcome is not directly achievable by the option or irrelevant, 'N/A' is applied.

Table 4-10 Customer related drivers of Option 2

Customer outcome		How this program achieves this
Deliver on the basics.	[C-I-C]	[C-I-C]
Keep me posted.	[C-I-C]	[C-I-C]
Affordable for me.	[C-I-C]	[C-I-C]
Be ready for the future.	[C-I-C]	[C-I-C]
Always safe.	[C-I-C]	[C-I-C]

Alignment to business related drivers of expenditure

As discussed in Section 3.6, there are four gas distribution business drivers that AusNet has identified and is focussing on over the next regulatory period. The table below highlights how this option will input into the initiatives where relevant. Where we consider that a business driver is not directly relevant to the option, 'N/A' is applied.

Table 4-11 Business related drivers of Option 2

Business drivers	How this program achieves this
Maintaining current performance in a disrupted environment.	[C-I-C]

Program Brief

Business drivers	How this program achieves this
Updating and implementing new technologies to enable AusNet to respond to industry wide changes.	[C-I-C]
Complying with new obligations.	[C-I-C]
Delivering improvements requested by our customers regarding sustainability and cost.	[C-I-C]

4.4 Option #3 [C-I-C]

[C-I-C]

Alignment to objectives

We consider that this option achieves all the intended objectives of this program of work, as shown in the table below, but is unlikely to do so in the required timeframes, and at greater cost and risk.

Table 4-12 Objectives analysis of Option 3

Objective		Comments
[C-I-C]	✔ ✔	[C-I-C]
[C-I-C]	✔	[C-I-C]
[C-I-C]	✔	[C-I-C]

Costs

Table 4-13 Costs of Option 3

($m)	FY23	FY24	FY25	FY26	FY27	Total
Capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$11.49
Opex (incl step change)	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$1.60
Gas Distribution cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$13.09
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$100.93

Benefits

Due to the complexity and speed of change of varied cyber threats to national critical infrastructure, the probability and impact of these threats can be hard to calculate. However, we have identified that the threat profile is increasing, and critical infrastructure is an important area to protect as referenced in the recent Critical Infrastructure Act 2018 in Australia. The main benefits of this option are summarised below:

- [C-I-C]

Risks

There are risks associated with the implementation of this option, as highlighted in the table below. Based on the consequence and likelihood of each risk, we have rated each of the individual risks blue, green, yellow, orange or red (in order of severity). See Figure 6-1 for additional information on this rating system.

Table 4-14 Risks of Option 3

	Domain	Risks	Consequence	Likelihood	Risk rating
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]

	Domain	Risks	Consequence	Likelihood	Risk rating
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]

We consider that overall, this option is rated medium risk.

Alignment to customer related drivers of expenditure

As discussed in Section 3.5, five key customer outcomes have been identified through discussions with customers. The table below highlights how this option will achieve these outcomes. Where we consider that a customer outcome is not directly achievable by the option or irrelevant, 'N/A' is applied.

Table 4-15 Customer related drivers of Option 3

Customer outcome		How this program achieves this
Deliver on the basics.	[C-I-C]	[C-I-C]
Keep me posted.	[C-I-C]	[C-I-C]
Affordable for me.	[C-I-C]	[C-I-C]
Be ready for the future.		[C-I-C]

Customer outcome		How this program achieves this
	[C-I-C]	
Always safe.	[C-I-C]	[C-I-C]

Alignment to business related drivers of expenditure

As discussed in Section 3.6, there are four gas distribution business drivers that AusNet has identified and is prioritising over the next regulatory period. The table below highlights how this option will input into the initiatives where relevant. Where we consider that a business driver is not directly relevant to the option, 'N/A' is applied.

Table 4-16 Business related drivers of Option 3

Business drivers	How this program achieves this
Maintaining current performance in a disrupted environment.	[C-I-C]
Updating and implementing new technologies to enable AusNet to respond to industry wide changes.	[C-I-C]
Complying with new obligations.	[C-I-C]
Delivering improvements requested by our customers regarding sustainability and cost.	[C-I-C]

5 Assessment and recommended option

5.1 Assessment of the options

To identify a recommended option for this program of work, we have selected a number of criteria to assess each of the options. These criteria ensure a comprehensive view of each option's ability to achieve AusNet's business and customer objectives as well as the AER's requirements that any expenditure is prudent and efficient.

The table below summarises our assessment of each of the options against the criteria. The box is highlighted in green where it is the highest scoring option.

Table 5-1 Summary table of the assessment of the options

	Option 1	Option 2	Option 3
Alignment to objectives	[C-I-C]	[C-I-C]	[C-I-C]
Costs	[C-I-C]	[C-I-C]	[C-I-C]
Overall risk rating	[C-I-C]	[C-I-C]	[C-I-C]
Alignment to customer related drivers of expenditure	[C-I-C]	[C-I-C]	[C-I-C]
Alignment to business related drivers of expenditure	[C-I-C]	[C-I-C]	[C-I-C]

Based on this assessment, Option 2 is the recommended option as it delivers the outcomes required, for the most prudent capital expenditure to meet the required outcomes.

5.2 NPV analysis

As defined in the AER Consultation Paper – ICT Assessment Approach, the AER is refining its approach to ICT assessment, requiring a NPV where ICT expenditure is driven by the need to meet a regulatory obligation.

Table 5-2, below shows the NPV results and Option 2 having the more favourable NPV.

Table 5-2 NPV analysis ($FY22m)

	Costs (NPV)	Benefit (NPV)	Net benefit (NPV)
Option 1	[C-I-C]	[C-I-C]	[C-I-C]
Option 2 *	[C-I-C]	[C-I-C]	[C-I-C]
Option 3	[C-I-C]	[C-I-C]	[C-I-C]

We have captured several primary benefits for this program:

[C-I-C]

5.3 Recommended option

[C-I-C]

[C-I-C]

Table 5-3 Confirmation of scope of recommended option

Domains		Risks	Key Initiatives
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C] •
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C] •
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C] •
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C] •
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C] •
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C] •
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]

Program Brief

Domains		Risks	Key Initiatives
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C] •
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C] •
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]

6 Attachment – Risks level matrix

The figure below shows the risk level matrix to which we have assessed each of the risks within the options. Risks of highest concern are rated red, whereas those of lowest concern are rated blue.

Figure 6-1

Likelihood	Consequence 1	2	3	4	5
Almost Certain	C	C	B	A	A
Likely	D	C	B	B	A
Possible	E	D	C	B	A
Unlikely	E	D	D	C	B
Rare	E	E	D	C	C

Consequence Rating	
5	Catastrophic
4	Major
3	Moderate
2	Minor
1	Insignificant

Overall Risk Rating	
A	Extreme
B	High
C	Medium
D	Low
E	Very Low

7 AES-CSF domains and practices

Domains		AES-CSF Practices
RM	Risk Management	• Establish Cybersecurity Risk Management Strategy. • Manage Cybersecurity Risk.
ACM	Asset, Change, and Configuration Management	• Manage Asset Inventory. • Manage Asset Configuration. • Manage Changes to Assets.
IAM	Identity and Access Management	• Establish and Maintain Identities. • Control Access.
TVM	Threat and Vulnerability Management	• Identify and Respond to Threats. • Reduce Cybersecurity Vulnerabilities.
SA	Situational Awareness	• Perform Logging. • Perform Monitoring. • Establish and Maintain a Common Operating Picture.
ISC	Information Sharing and Communications	• Share Cybersecurity Information.
IR	Event and Incident Response, Continuity of Operations	• Detect Cybersecurity Events. • Escalate Cybersecurity Events and Declare Incidents. • Respond to Incidents and Escalated Cybersecurity Events. • Plan for Continuity.
EDM	Supply Chain and External Dependencies Management	• Identify Dependencies. • Manage Dependency Risk.
WM	Workforce Management	• Assign Cybersecurity Responsibilities. • Control the Workforce Life Cycle. • Develop Cybersecurity Workforce. • Increase Cybersecurity Awareness.
CPM	Cybersecurity Program Management	• Establish Cybersecurity Program Strategy. • Sponsor Cybersecurity Program. • Establish and Maintain Cybersecurity Architecture. • Perform Secure Software Development.
APM	Australian Privacy Management	• Focuses on matters that intersect with or provide cyber security maturity. • Leverage the Australian Privacy Principles and the office of the Australian Information Commissioner. Privacy related elements of the international standard.