Technology Document ICT Program Brief Cyber Security

2023-27 Transmission Revenue Reset

PUBLIC

Submitted: 29 October 2020

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 Services' Technology TRR submission.

1.2 References

Document	Version	Author
Digital Utility Strategy	V1.3	S Scanlon
FY21 Electricity Transmission Business Plan	V0.3	A Hill
TRR Technology Strategy	V0.21	S Scanlon

1.3 Document History

Date	Version	Comment	Author
21/10/2020	V1.0	Published	S Scanlon

1.4 Approvals

Position	Date
Technology Leadership Team	

2 Executive summary

2.1 Program summary

The table below provides a summary of the program discussed in this brief. Additional information is provided following the table and throughout the brief.

Table 2-1 Summary table

Key objective(s) of the program	The ongoing objectives of cyber security at AusNet Services are to: • [C-I-C] • [C-I-C] • [C-I-C] • [C-I-C] • [C-I-C].						
Key benefits	• [C-I-C] • [C-I-C] • [C-I-C] • [C-I-C] • [C-I-C]						
Cost allocation	Electricity Distribution	25%	Electricity Transmission	63%			
	Gas Distribution	12%					
Program type	**Recurrent**	☒					
	Non-Recurrent	☒					
	Client Devices	☐					
Program timings	Program duration:	5 years					
Expenditure forecast	**($m)**	**FY23**	**FY24**	**FY25**	**FY26**	**FY27**	**Total**
	Capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$15.47
	Opex (incl step change)	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$31.05
	Electricity Transmission Cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$46.52**
	Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$74.39
Estimated life of system	[C-I-C]						

Customer Engagement	[C-I-C]

[C-I-C]

[C-I-C]

[C-I-C]

[C-I-C]

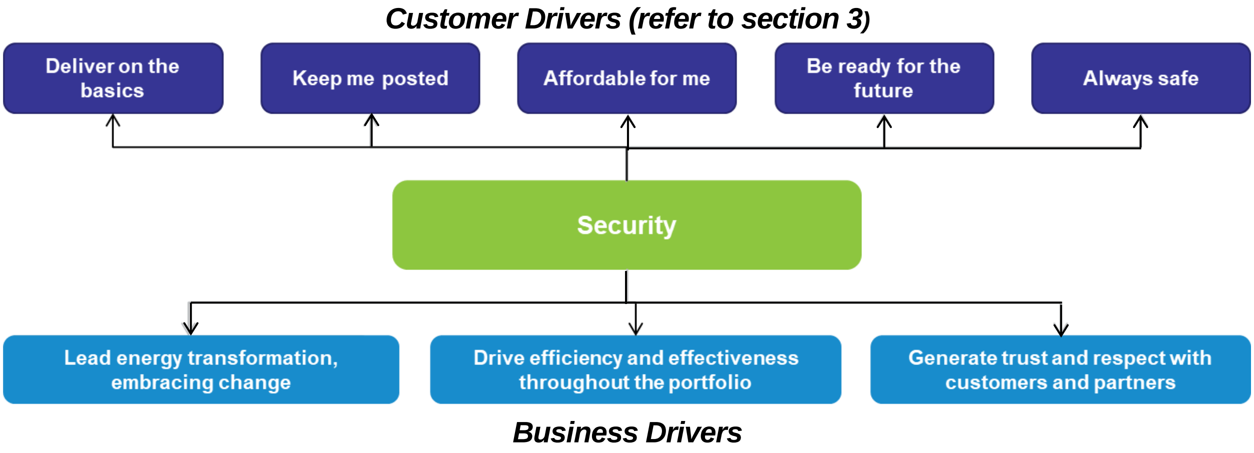
The recommended budget will enable AusNet Services to:

- [C-I-C]

- [C-I-C]
- [C-I-C]
- [C-I-C]

[C-I-C]

[C-I-C]


Customer Drivers (refer to section 3)
Deliver on the basics
Keep me posted
Affordable for me
Be ready for the future
Always safe
Security
Lead energy transformation, embracing change
Drive efficiency and effectiveness throughout the portfolio
Generate trust and respect with customers and partners
Business Drivers

Alignment with the AER ICT expenditure assessment framework

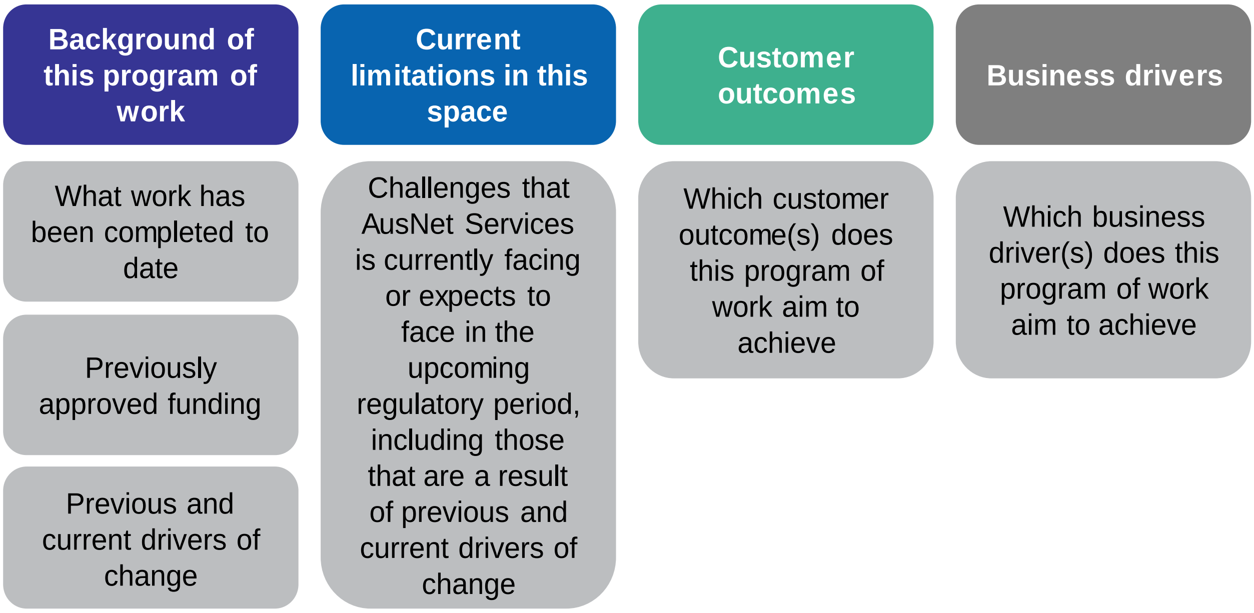
In accordance with the framework outlined in the AER – Guidance Note – Non-network ICT capex assessment approach for electricity distributors (28 November 2019), we have categorised 45% of this program as recurrent expenditure, on the basis that it relates to a compliance requirement, and that an ongoing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

Consistent with AusNet Services' 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 address the need for investment in order to determine the chosen option.

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



Background of this program of work

What work has been completed to date

Previously approved funding

Previous and current drivers of change

Current limitations in this space

Challenges that AusNet Services is currently facing or expects to face in the upcoming regulatory period, including those that are a result of previous and current drivers of change

Customer outcomes

Which customer outcome(s) does this program of work aim to achieve

Business drivers

Which business driver(s) does this program of work aim to achieve

3.1 Background

[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]

3.2 Increasing threats

[C-I-C]

3.3 Existing and emerging regulatory obligations

[C-I-C]

[C-I-C]

3.4 Objective(s)

By establishing [C-I-C] capabilities, we will:

- [C-I-C]
- [C-I-C]
- [C-I-C]
- [C-I-C]
- [C-I-C]

3.5 Customer drivers

Through customer research carried out by AusNet Services, 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 TRR submission FY2023-2027.

This program of work proposed by AusNet Services 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 transmission network.

[C-I-C].

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 Services has selected four key business drivers which set the direction for the business.

These business drivers are:

- **Maintaining current service performance** in a disrupted environment where risks are changing due to the increasingly complex nature of the grid.
- Updating and implementing **new technologies** to enable AusNet Services to respond to changes within the growing renewable generation market;
- Complying with **new obligations**; and
- Delivering improvements requested by our customers regarding **sustainability and cost**.

This program of work is considered to be 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. We will further explore this in the discussions of each of the options.

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

- [C-I-C]
- [C-I-C]
- [C-I-C]
- [C-I-C]
- [C-I-C]
- [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 FY2023-2027.

A full overview of the approach can be found in section 3.2 of the "*AusNet Services – Transmission 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,
- 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, and
- Top down view to ensure that the Technology Strategy investment portfolio represents prudent and efficient expenditure for the upcoming period, relative to AusNet Services' previous expenditure and also benchmarked against other comparable Transmission businesses.

4 Options

4.1 Overview

This section provides an overview of the three options 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]

[C-I-C]

Costs

[C-I-C]

Table 4-2 Costs of option 1

($m)	FY23	FY24	FY25	FY26	FY27	Total
Electricity transmission capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$9.32
Electricity transmission opex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$1.37
Electricity transmission total cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$10.69**
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$35.63

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
R1	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B
R2	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B
R3	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B
R4	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B
R5	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B
R6	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B
R7	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B

	Domain	Risks	Consequence	Likelihood	Risk rating
R8	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B
R9	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B
R10	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B
R11	[C-I-C]	[C-I-C]	[C-I-C]	Likely	B

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
Protect the organisational assets, including information, applications, systems, networks and end user devices from internal and external threats.	✗	[C-I-C].
Uplift capability maturity level to respond to increasing complexity and sophistication of the cyber security attacks	✗	[C-I-C]
Demonstrate the adherence to current and emerging regulatory standards and guidelines	✗	[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 4-5 Customer related drivers of option 1

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

Alignment to Business related drivers of expenditure

As discussed in Section 3.6, there are four Transmission business drivers that AusNet Services 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
Maintaining current service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid	[C-I-C]
Updating and implementing new technologies to enable AusNet Services to respond to changes within the growing renewable generation market	[C-I-C]
Complying with new obligations	[C-I-C]
Delivering improvements requested by our customers regarding sustainability and cost	[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
Protect organizational assets, including information, applications, systems, networks and end-user devices from internal and external threats	✓	[C-I-C]
Uplift capability maturity level to respond to increasing complexity and sophistication of the cyber security attacks	✓	[C-I-C]
Demonstrate the adherence to current and emerging regulatory standards and guidelines	✓	[C-I-C]

Costs

[C-I-C]

Table 4-8 Costs of option 2

($m)	FY23	FY24	FY25	FY26	FY27	Total
Capex	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$15.47
Opex (incl step change)	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$31.05
Electricity transmission cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$46.52**
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$74.39

[C-I-C]

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 very 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 in Australia. Main benefits of this option are summarised below:

[C-I-C]

Risks

There are risks associated with the implementation of this particular 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.

[C-I-C]

Table 4-9 Risks for option 2

	Domain	Risks	Consequence	Likelihood	Risk rating
R1	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	C
R2	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	C
R3	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	D
R4	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	C
R5	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	C
R6	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	D
R7	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	C
R8	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	C
R9	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	D
R10	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	C
R11	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	D

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]
Keep me posted	✓	[C-I-C]
Affordable for me	✓	[C-I-C]
Be ready for the future	✓	[C-I-C]
Always safe	✓	[C-I-C]

Alignment to business related drivers of expenditure

As discussed in Section 3.6, there are four Transmission business drivers that AusNet Services 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 service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid	[C-I-C]
Updating and implementing new technologies to enable AusNet Services to respond to changes within the growing renewable generation market	[C-I-C]

Business drivers	How this program achieves this
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
Protect the organisational assets, including information, applications, systems, networks and end user devices from internal and external threats.	✓	[C-I-C]
Uplift capability maturity level to respond to increasing complexity and sophistication of the cyber security attacks and	✓	[C-I-C]
Demonstrate the adherence to current and emerging regulatory standards and guidelines	✓	[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]	$31.13
Opex (incl step change)	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$34.48
Electricity transmission cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	**$65.61**
Total program cost	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]	$100.93

[C-I-C]

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 very 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 in Australia. Main benefits of this option are summarised below:

- [C-I-C]
- [C-I-C]
- [C-I-C]
- [C-I-C]

Risks

There are risks associated with the implementation of this particular 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.

Table 4-14 Risks of option 3

	Domain	Risks	Consequence	Likelihood	Risk rating
R1	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	🟨 C
R2	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	🟩 C
R3	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	🟩 D
R4	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	🟨 C
R5	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	🟩 C

	Domain	Risks	Consequence	Likelihood	Risk rating
R6	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	D
R7	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	C
R8	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	C
R9	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	D
R10	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	C
R11	[C-I-C]	[C-I-C]	[C-I-C]	Unlikely	D

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]
Keep me posted	✓	[C-I-C]

Customer outcome		How this program achieves this
Affordable for me	N/A	[C-I-C]
Be ready for the future	✓	[C-I-C]
Always safe	✓	[C-I-C]

Alignment to business related drivers of expenditure

As discussed in Section 3.6, there are four Transmission business drivers that AusNet Services 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 service performance in a disrupted environment where risks are changing due to the increasingly complex nature of the grid;	[C-I-C]
Updating and implementing new technologies to enable AusNet Services to respond to changes within the growing renewable generation market;	[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. We consider that these criteria represent a comprehensive view of each option, in achieving AusNet Services' business and customer objectives as well as requirements of the AER in ensuring that any expenditure is both 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	Does not achieve program objectives This option would result in non-compliance	Achieves all program objectives	Achieves all program objectives
Costs	$10.69	$46.52	$65.61
Overall risk rating	High	Medium	Medium
Alignment to customer related drivers of expenditure	No alignment (0/5)	High alignment (5/5)	High alignment (4/5)
Alignment to business related drivers of expenditure	No alignment (1/4)	High alignment (4/4)	High alignment (4/4)

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 ($FY21m)

	Costs (NPV)	Benefit (NPV)	Net benefit (NPV)
Option 1	$9.39	$22.22	$12.83
Option 2 *	$40.88	$72.76	$31.88
Option 3	$57.65	$72.76	$15.11

[C-I-C]

5.3 Sensitivity Analysis of Benefits

When developing the NPV, we have considered variable assumptions to ensure that we have contemplated alternative scenarios relative to the benefits defined. This allowed us to establish a level of confidence in quantifying the benefits described.

Three levels of sensitivity were considered, they are:

- A *conservative* level, where some of the variables in the benefit calculations were halved from the values used in the NPV stated in this brief.
- A *moderate* level, which became the basis for the calculated NPV in this program brief
- A *bullish* level, where some of the variables in the benefit calculations were doubled from the values used in the NPV stated in this brief.

For example, the NPV sensitivity range for Option 2 is listed below.

Conservative level NPV	-$3.23
Moderate level NPV	$31.88 (recommended)
Bullish level NPV	$102.41

5.4 Recommended option

[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]

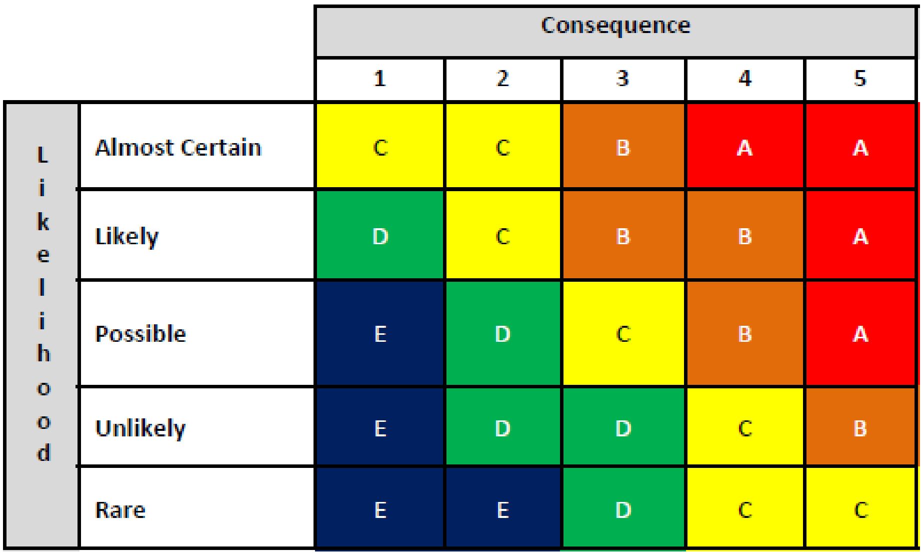
Domains		Risks	Key Initiatives
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]
[C-I-C]	[C-I-C]	[C-I-C]	[C-I-C]

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]

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



		Consequence				
		1	2	3	4	5
Likelihood	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.