

Technology program

Cyber Security

PUBLIC

Program Brief

Table of Contents

1	Document Background	3
1.1	Purpose of this document	3
1.2	References	3
1.3	Document History	3
1.4	Approvals	4
2	Executive summary	5
2.1	Program summary	5
3	Context	9
3.1	Background	9
3.2	Current limitations	10
3.3	Objective(s)	10
3.4	Customer outcomes	11
3.5	Business drivers	12
4	Options	13
4.1	Overview	13
4.2	Option #1 [C-I-C]	13
4.3	Option #2 [C-I-C]	16
4.4	Option #3 [C-I-C]	21
5	Assessment and recommended option	25
5.1	Assessment of the options	25
5.2	Recommended option	26
6	Attachment – Risks level matrix	30
7	AES-CSF domains and practices	31

Program Brief

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 EDPR submission.

1.2 References

Document	Version	Author
AusNet Services FY19-FY23 Technology Plan	V1.00	AusNet Services
Australia's Cyber Security Strategy	2016	Commonwealth of Australia
Security of Critical Infrastructure Act 2018	2018	The Parliament of Australia
Notifiable Data Breaches Act 2017	2017	The Parliament of Australia
Privacy Act 1988	2014	The Parliament of Australia
AusNet Services FY19-FY23 Technology Plan	V1.00	AusNet Services
Cybersecurity Capability Maturity Model (C2M2)	V1.10	U.S. Department of Energy
IT Key Metrics Data 2018: Key IT Security Measures	V1.00	Gartner
Risk Assessment Criteria Summary		AusNet Services
Cyber resilience: Health check, report 429	2015	ASIC

1.3 Document History

Date	Version	Comment	Author
09/08/2018	V1.0	1 st draft	Yuanyuan Zhao
29/08/2018	V1.1	Input	Katherine Robins
29/08/2018	V1.2	2 nd draft	Yuanyuan Zhao
15/04/2019	V1.3	Updated brief including preferred option, costs and risks	Kevin Shaw, Doron Harel, Christina Keing, Yuanyuan Zhao
16/04/2019	V1.4	Minor edits	Janine Perri
18/04/2019	V1.5	Final review of risks and benefits	Kevin Shaw, Janine Perri

Program Brief

08/05/2019	V1.6	Correction to Option 2 costs confirmed by Deloitte (Opex costs captured in Costs tab are BAU opex costs not Propex)	Yuanyuan Zhao, Kevin Shaw, Janine Perri
13/05/2019	V1.7	AEMO footnotes added	Janine Perri
23/08/2019	V2	Update to costs	Emily Pong
31/10/2019	V3	Draft issued to Regulatory team	Samantha Scanlon
19/11/2019	V3.2	Incorporated feedback	Samantha Scanlon
14/01/2020	V3.5	Incorporated feedback	Samantha Scanlon

1.4 Approvals

Position	Date
Technology Leadership Team	

Program Brief

2 Executive summary

2.1 Program summary

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

Program Brief

3 Context

[C-I-C]

3.1 Background

[C-I-C]

Program Brief

3.2 Current limitations

[C-I-C]

3.3 Objective(s)

[C-I-C]

Program Brief

[C-I-C]

3.4 Customer outcomes

[C-I-C]

Program Brief

3.5 Business drivers

[C-I-C]

Program Brief

4 Options

4.1 Overview

[C-I-C]

4.2 Option #1 [C-I-C]

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

4.3 Option #2 [C-I-C]

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

Program Brief

4.4 Option #3 [C-I-C]

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

Program Brief

5 Assessment and recommended option

5.1 Assessment of the options

[C-I-C]

Program Brief

[C-I-C]

5.2 Recommended option

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

Program Brief

[C-I-C]

Program Brief

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
L i k e l i h o o d	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

Program Brief

7 AES-CSF domains and practices

Domains		AESCSF Practices
RM	Risk Management	<ul style="list-style-type: none"> Establish Cybersecurity Risk Management Strategy Manage Cybersecurity Risk
ACM	Asset, Change, and Configuration Management	<ul style="list-style-type: none"> Manage Asset Inventory Manage Asset Configuration Manage Changes to Assets
IAM	Identity and Access Management	<ul style="list-style-type: none"> Establish and Maintain Identities Control Access
TVM	Threat and Vulnerability Management	<ul style="list-style-type: none"> Identify and Respond to Threats Reduce Cybersecurity Vulnerabilities
SA	Situational Awareness	<ul style="list-style-type: none"> Perform Logging Perform Monitoring Establish and Maintain a Common Operating Picture
ISC	Information Sharing and Communications	<ul style="list-style-type: none"> Share Cybersecurity Information
IR	Event and Incident Response, Continuity of Operations	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> Identify Dependencies Manage Dependency Risk
WM	Workforce Management	<ul style="list-style-type: none"> Assign Cybersecurity Responsibilities Control the Workforce Life Cycle Develop Cybersecurity Workforce Increase Cybersecurity Awareness
CPM	Cybersecurity Program Management	<ul style="list-style-type: none"> Establish Cybersecurity Program Strategy Sponsor Cybersecurity Program Establish and Maintain Cybersecurity Architecture Perform Secure Software Development
APM	Australian Privacy Management	<ul style="list-style-type: none"> 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.