EMC[a]

energy market consulting associates

Ausgrid 2024 to 2029 Regulatory Proposal

REVIEW OF PROPOSED EXPENDITURE ON ICT CYBER SECURITY

Report prepared for:

AUSTRALIAN ENERGY REGULATOR

August 2023

Preface

This report has been prepared to assist the Australian Energy Regulator (AER) with its determination of the appropriate revenues to be allowed for the prescribed distribution services of Ausgrid from 1st July 2024 to 30th June 2029. The AER's determination is conducted in accordance with its responsibilities under the National Electricity Rules (NER).

This report covers a particular and limited scope as defined by the AER and should not be read as a comprehensive assessment of proposed expenditure that has been conducted making use of all available assessment methods nor all available inputs to the regulatory determination process. This report relies on information provided to EMCa by Ausgrid. EMCa disclaims liability for any errors or omissions, for the validity of information provided to EMCa by other parties, for the use of any information in this report by any party other than the AER and for the use of this report for any purpose other than the intended purpose. In particular, this report is not intended to be used to support business cases or business investment decisions nor is this report intended to be read as an interpretation of the application of the NER or other legal instruments.

EMCa's opinions in this report include considerations of materiality to the requirements of the AER and opinions stated or inferred in this report should be read in relation to this over-arching purpose.

Except where specifically noted, this report was prepared based on information provided to us prior to 1st August 2023 and any information provided subsequent to this time may not have been taken into account. Some numbers in this report may differ from those shown in Ausgrid's regulatory submission or other documents due to rounding.

Enquiries about this report should be directed to:

Paul Sell
Managing Director
psell@emca.com.au

Prepared by
Mark de Laeter and Paul Sell with input from Cesare Tizi and Eddie Syadan

Date saved
26/09/2023 3:15 PM

Version
Final v4

Energy Market Consulting associates
ABN 75 102 418 020

Sydney Office
L25, 100 Mount Street, North Sydney NSW 2060
PO Box 592, North Sydney NSW 2059
+(61) 2 8923 2599
contact@emca.com.au
www.emca.com.au

Perth Office
Level 1, 2 Mill Street, Perth WA 6000
contact@emca.com.au
www.emca.com.au

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

ABBREVIATIONS

Term	Definition
ACM	Asset, Change, and Configuration Management AESCSF Domain
ACSC	Australian Cyber Security Centre
AEMO	Australian Energy Market Operator
AESCSF	Australian Energy Sector Cyber Security Framework
AER	Australian Energy Regulator
AGD	Ausgrid
APM	Australian Privacy Management AESCSF Domain
CAM	Cost Allocation Method
Capex	Cyber Security-related Capital Expenditure
CIRMP	Critical Infrastructure Risk Management Plan
CISC	Cyber and Infrastructure Security Centre
CPM	Cybersecurity Program Management AESCSF Domain
Current RCP	FY20-FY24
DNSP	Distribution Network Service Provider
EBSS	Efficiency Benefits Sharing Scheme
E-CAT	Electricity – Criticality Assessment Tool
ECSO	Enhanced Cyber Security Obligations
EDM	Supply Chain and External Dependencies Management AESCSF Domain
EEMM	Essential Eight Maturity Model
FY	Financial Year
IAM	Identity and Access Management AESCSF Domain
ICT	Information and Communications Technology
IR	Event and Incident Response, Continuity of Operations AESCSF Domain
ISC	Information Sharing and Communications AESCSF Domain
IT	Information technology
MIL	Maturity Indicator Level
NER	National Electricity Rules
Next RCP	FY25-FY29
NPC	Net Present Cost
NPV	Net Present Value
NSP	Network Service Provider
NSW	New South Wales

Term	Definition
RCP	Regulatory Control Period
RM	Risk Management AESCSF domain
RMP	Risk Management Plan
RP	Revenue Proposal
Opex	Operational expenditure
OT	Operational Technology
SA	Situational Awareness AESCSF Domain
SCS	Standard Control Services
SLACI Act	Security Legislation Amendment (Critical Infrastructure) Act
SOCI Act	Security of Critical Infrastructure Act
SoNS	Systems of National Significance
SP	Security Profile
TNSP	Transmission Network Service Provider
TVM	Threat and Vulnerability Management AESCSF Domain
WM	Workforce Management AESCSF Domain

1 INTRODUCTION

The AER has asked us to review and provide advice on Ausgrid's proposed allowance for cyber security-related expenditure in the next Regulatory Control Period. Our review is based on information that Ausgrid provided and on aspects of the National Electricity Rules relevant to assessment of expenditure allowances.

1.1 Objective of this report

1. In January 2023, Ausgrid submitted its Revenue Proposal (RP) for the next Regulatory Control Period 2024-29 (next RCP) to the Australian Energy Regulator (AER).
2. The purpose of this report is to provide the AER with a technical review of Ausgrid's proposed cyber security-related capital expenditure (capex) and step-change operating expenditure (opex) included in Ausgrid's RP for the next RCP.
3. The assessment contained in this report is intended to assist the AER in its own analysis of the proposed capex and opex allowance as an input to its Draft Determination on Ausgrid's revenue requirements for the next RCP.

1.2 Our scope

4. The scope of this review covers Ausgrid's proposed allowance for:
   - Non-recurrent ICT cyber security capex; and
   - An opex step change for ICT cyber security.
5. In preparing our findings, we are required to have regard to the AER's role under s.6 of the NER and the AER's forecast assessment guidelines.

1.3 Our review approach

6. In undertaking our review, we:
   - Completed a desktop review of the information provided to us by the AER followed by preparing requests for information to Ausgrid to help ensure that we correctly understood the methodology and assumptions that Ausgrid had applied in estimating its expenditure requirements;
   - Completed an assessment of relevant aspects of the expenditure forecast, including by taking into account the responses from Ausgrid to information requests; and
   - Documented our findings in this report.
7. We also provided feedback to AER staff on our preliminary findings in a teleconference, while drafting this report.
8. Our review considers the requirements of the National Electricity Rules (NER), specifically the capex and opex criteria and objectives, and the AER's expenditure assessment guideline.
9. Where we find that Ausgrid's forecast expenditure is not reasonable in terms of the relevant requirements of the NER, we have identified the extent to which the issues we have found have resulted in a higher level of expenditure than what would be required of a prudent and efficient service provider.
10. The limited nature of our review does not extend to advising on all options and alternatives that may be reasonably considered by Ausgrid, nor on all parts of its capex forecast or its

proposed opex step change. To the extent that there may be implications for aspects of Ausgrid's RP that are beyond our scope, we have included additional observations in some areas that we trust may assist the AER with its own assessment.

1.3.1 Conformance with NER requirements

11. In undertaking our review, we have been cognisant of the relevant aspects of the NER under which the AER is required to make its determination.

Capex Objectives and Criteria

12. The most relevant aspects of the NER in this regard are the 'capital expenditure criteria' and the 'capital expenditure objectives.' Specifically, the AER must accept the Network Service Provider's (NSP) capex proposal if it is satisfied that the capex proposal reasonably reflects the capital expenditure criteria, and these in turn reference the capital expenditure objectives.

13. We have taken particular note of the following aspects of the capex and opex criteria and objectives:

- Drawing on the wording of the first and second capex and opex criteria, our findings refer to efficient and prudent expenditure. We interpret this as encompassing the extent to which the need for a project or program has been prudently established and the extent to which the proposed solution can be considered to be an appropriately justified and efficient means for meeting that need;
- The capex and opex criteria require that the forecast '*reasonably reflects*' the expenditure criteria and in the third criterion, we note the wording of a '*realistic expectation*' (emphasis added). In our review we have sought to allow for a margin as to what is considered reasonable and realistic, and we have formulated negative findings where we consider that a particular aspect is outside of those bounds;
- We note the wording '*meet or manage*' in the first capex and opex objective (emphasis added), encompassing the expected demand for standard control services over the next RCP;
- We tend towards a strict interpretation of compliance (under the second capex and opex objective), with the onus on the Distribution Network Service Provider (DNSP) in this case to evidence specific compliance requirements rather than to infer them; and
- We note the word '*maintain*' in capex and opex objectives 3 and 4. Depending on the context, we have sought evidence that the NSP has demonstrated that it has properly assessed the proposed expenditure as being required to reasonably maintain, as opposed to enhancing or diminishing, the aspects referred to in those objectives.

14. The NER's capex criteria and capex objectives are reproduced in Figure 1.1 and Figure 1.2.

Figure 1.1: NER capital expenditure criteria

NER capital expenditure criteria

The AER must:

(1) subject to subparagraph (c)(2), accept the forecast of required capital expenditure of a Distribution Network Service Provider that is included in a building block proposal if the AER is satisfied that the total of the forecast capital

> *expenditure for the regulatory control period reasonably reflects each of the following (**the capital expenditure criteria**):*
>
> *(i) the efficient costs of achieving the capital expenditure objectives;*
>
> *(ii) the costs that a prudent operator would require to achieve the capital expenditure objectives; and*
>
> *(iii) a realistic expectation of the demand forecast and cost inputs required to achieve the capital expenditure objectives.*

Source: NER 6.5.7(c) Forecast capital expenditure, v200

Figure 1.2: NER capital expenditure objectives

> *NER capital expenditure objectives*
>
> (a) *A building block proposal must include the total forecast capital expenditure for the relevant regulatory control period which the Distribution Network Service Provider considers is required in order to achieve each of the following (**the capital expenditure objectives**):*
>
> *(1) meet or manage the expected demand for standard control services over that period;*
> *(2) comply with all applicable regulatory obligations or requirements associated with the provision of standard control services;*
> *(3) to the extent that there is no applicable regulatory obligation or requirement in relation to:*
> *(i) the quality, reliability or security of supply of standard control services; or*
> *(ii) the reliability or security of the distribution system through the supply of standard control services,*
>
> *to the relevant extent:*
>
> *(iii) maintain the quality, reliability and security of supply of standard control services; and*
> *(iv) maintain the reliability and security of the distribution system through the supply of standard control services; and*
> *(4) maintain the safety of the distribution system through the supply of standard control services.*

Source: NER 6.5.7(a) Forecast capital expenditure, v200

15. The NER's opex criteria and opex criteria are reproduced in Figure 1.3 and Figure 1.4.

Figure 1.3: NER operational expenditure criteria

NER operating expenditure criteria

(c) *The AER must accept the forecast of required operating expenditure of a Distribution Network Service Provider that is included in a building block proposal if the AER is satisfied that the total of the forecast operating expenditure for the regulatory control period reasonably reflects each of the following (the operating expenditure criteria):*

(1) the efficient costs of achieving the operating expenditure objectives; and

(2) the costs that a prudent operator would require to achieve the operating expenditure objectives; and

(3) a realistic expectation of the demand forecast and cost inputs required to achieve the operating expenditure objectives

Source: NER 6.5.6 (c) Forecast operating expenditure

Figure 1.4: NER operating expenditure objectives

NER operating expenditure objectives

(a) *A building block proposal must include the total forecast operating expenditure for the relevant regulatory control period which the Distribution Network Service Provider considers is required in order to achieve each of the following (**the operating expenditure objectives**):*

(1) meet or manage the expected demand for standard control services over that period;

(2) comply with all applicable regulatory obligations or requirements associated with the provision of standard control services;

(3) to the extent that there is no applicable regulatory obligation or requirement in relation to:

(i) the quality, reliability or security of supply of standard control services; or

(ii) the reliability or security of the distribution system through the supply of standard control services,

to the relevant extent:

(iii) maintain the quality, reliability and security of supply of standard control services; and

(iv) maintain the reliability and security of the distribution system through the supply of standard control services; and

(4) maintain the safety of the distribution system through the supply of standard control services.

Source: NER 6.5.6 (a) Forecast operating expenditure

How we have interpreted the capex and opex criteria and objectives in our assessment

16. We have taken particular note of the following aspects of the capex and opex criteria and objectives:

- Drawing on the wording of the first and second criteria, our findings refer to efficient and prudent expenditure. We interpret this as encompassing the extent to which the need for a project or program or opex item has been prudently established and the extent to which the proposed solution can be considered to be an appropriately justified and efficient means for meeting that need;
- The criteria require that the forecast 'reasonably reflects' the expenditure criteria and in the third criterion, we note the wording of a 'realistic expectation' (emphasis added). In our review we have sought to allow for a margin as to what is considered reasonable and realistic, and we have formulated negative findings where we consider that a particular aspect is outside of those bounds;
- We note the wording 'meet or manage' in the first objective (emphasis added), encompassing the need for the NSP to show that it has properly considered demand management and non-network options;
- We tend towards a strict interpretation of compliance (under the second objective), with the onus on the NSP to evidence specific compliance requirements rather than to infer them; and
- We note the word 'maintain' in objectives 3 and 4 and, accordingly, we have sought evidence that the NSP has demonstrated that it has properly assessed the proposed expenditure as being required to reasonably maintain, as opposed to enhancing or diminishing, the aspects referred to in those objectives.

17. The DNSPs subject to our review have applied a Base Step Trend approach in forecasting their aggregate opex requirements. Since our review scope encompasses only proposed expenditure for certain purposes, we have sought to identify where the DNSP has proposed an opex step change that is relevant to a component that we have been asked to review. Where the DNSP has not proposed a relevant opex step change, then we assume that any opex referred to in documentation that the DNSP has provided is effectively absorbed and need not be considered in our assessment.

1.3.2 Technical review

18. Our assessments comprise a technical review. While we are aware of stakeholder inputs on aspects of what Ausgrid has proposed, our technical assessment framework is based on engineering considerations and economics.

19. We have sought to assess Ausgrid's expenditure proposal based on Ausgrid's analysis and Ausgrid's own assessment of technical requirements and economics and the analysis that it has provided to support its proposal. Our findings are therefore based on this supporting information and, to the extent that Ausgrid may subsequently provide additional information or a varied proposal, our assessment may differ from the findings presented in the current report.

20. We have been provided with a range of reports, internal documents, responses to information requests and modelling in support of what Ausgrid has proposed and our assessment takes account of this range of information provided. To the extent that we found discrepancies in this information, our default position is to revert to Ausgrid regulatory submission documents as provided on its submission date, as the 'source of record' in respect of what we have assessed.

1.4 About this report

1.4.1 Report structure

21. The following sections of our report are structured as follows:

- In section 2, we present relevant context to our assessment including contextual information on cyber security threat to Australian electricity networks, regulation relevant

to critical infrastructure, the relevant assessment framework and relevant regulatory guidelines;

- In section 3, we present what Ausgrid has proposed for cyber security, as the basis for our assessment; and
- In section 4, we describe our assessment of Ausgrid's proposed cyber security allowance, our findings on the prudency and efficiency of that allowance and the implications of those findings for the expenditure allowance that Ausgrid has proposed.

1.4.2 Information sources

22. We have examined relevant documents that Ausgrid has published and/or provided to AER in support of the areas of focus and projects that the AER has designated for review. This included further information at a virtual meeting and further documents in response to our information requests. These documents are referenced directly where they are relevant to our findings.

23. Except where specifically noted, this report was prepared based on information provided to us prior to 1st August 2023 and any information provided subsequent to this time may not have been taken into account.

1.4.3 Presentation of expenditure amounts

24. Expenditure is presented in this report in $2024 real terms, to be consistent with Ausgrid's RP, unless stated otherwise. In some cases, we have converted to this basis from information provided by the business in other terms.

25. While we have sought to reconcile expenditure amounts presented in this report to source information, in some cases there may be discrepancies in source information provided to us and minor differences due to rounding. Any such discrepancies do not affect our findings.

2 RELEVANT CONTEXT TO OUR ASSESSMENT

We have conducted our review in the context of increasing cyber security threats and a typically increasing threat surface, taking account of relevant regulatory compliance obligations and industry frameworks for assessing cyber risk criticality and risk mitigation maturity.

2.1 Cyber security threat in Australia

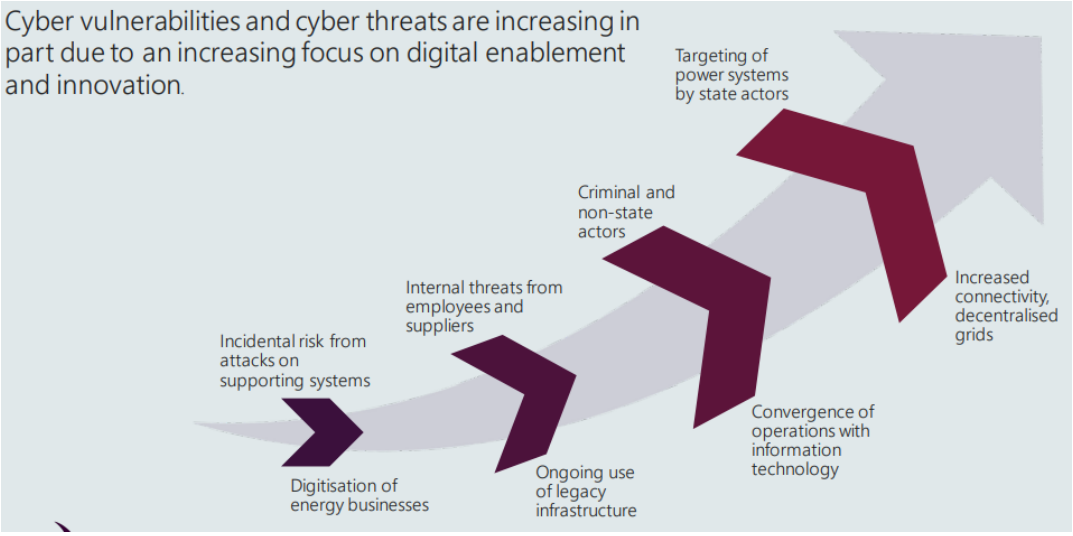
26. The Australian Cyber Security Centre (ACSC) monitors Australia's cyber threat landscape and among other things publishes an annual Cyber Threat Report. In its latest report (2021-22) it states that: *The ACSC received over 76,000 cybercrime reports, an increase of nearly 13 per cent from the previous financial year.* In the same report it identifies the following cyber security trends:

- Cyberspace has become a battleground;
- Australia's prosperity is attractive to cybercriminals;
- Ransomware remains the most destructive cybercrime;
- 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. Potential disruptions to Australian essential services in 2021–22 were averted by effective cyber defences, including network segregation and effective, collaborative incident response; and
- The rapid exploitation of critical public vulnerabilities became the norm - the majority of significant incidents ACSC responded to in 2021–22 were due to inadequate patching.

27. The Electricity, Gas, Water and Waste services sectors accounted for 3% of cyber security incidents in 2021-22. Among other things the ACSC promotes the Essential Eight cyber security measures.

28. At its 2022 AESCSF education workshop with the Department of Industry, Science, Energy and Resources, Australian Energy Market Operator (AEMO) discussed cyber threat actors, motivations, and case studies and included the following figure in its presentation.

Figure 2.1: The cyber security problem



Source: AEMO, 2022 Australian Energy Sector Cyber Security Framework Education Workshop, slide 5

29. This figure highlights the twin issues of increasing cyber-attack threat landscape and the increasing vulnerability of electricity utility assets due to the increasing 'attack surface' presented due to increased digitalisation and interconnectivity.

2.2 Critical infrastructure - changes to regulation

2.2.1 Amendments to the SOCI Act

30. The Security of Critical Infrastructure Act 2018 (SOCI Act) places obligations on specific entities in the electricity and other industries.

31. The Security Legislation Amendment (Critical Infrastructure) Act 2021 (SLACI Act) and the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 (SLACIP Act) have recently amended the SOCI Act to strengthen the security and resilience of critical infrastructure by expanding the sectors and asset classes the SOCI Act applies to, and to introduce new obligations.

32. The amendments were made because '*Australia is facing increasing cyber security threats to essential services, businesses and all levels of government.* [1] Electricity assets may be classed as critical infrastructure within the framework under the Act. The new 'Positive Security Obligations' that apply to certain sets of critical infrastructure assets are:

- Register of Critical Infrastructure Assets: which requires reporting entities, who are either direct interest holders or the responsible entity of critical infrastructure assets, to provide to Government ownership, operational, interest and control information; and
- Mandatory Cyber Incident Reporting: Responsible entities for critical infrastructure assets will be required to report critical and other cyber security incidents to the Australian Cyber Security Centre's online cyber incident reporting portal.

33. On 2 April 2022, amendments to the SOCI Act introduced the following:

- A new obligation for responsible entities to create and maintain a Critical Infrastructure Risk Management Program (CIRMP) with the obligation commencing on 17 February 2023;[2] and

[1] Department of Home Affairs, Cyber and Infrastructure Security Centre website

[2] CISC Factsheet – Risk Management Program

- a new framework for enhanced cyber security obligations (ECSO) required for operators of systems of national significance (SoNS), Australia's most important critical infrastructure assets. [3]

34. The CIRMP is a written program which requires a responsible entity for a critical infrastructure asset to (i) to identify each hazard where there is a material risk that the occurrence of the hazard could have a relevant impact on the asset, and so far as it is reasonably practicable to do so, (ii) minimise or eliminate any material risk of such a hazard occurring, and (iii) mitigate the relevant impact of such a hazard on the asset.[4]

35. The ECSO will vary between each SoNS, depending on the specific role and function of that asset, with the obligations including (i) developing cyber security incident response plans to prepare for a cyber security incident, (ii) undertaking cyber security exercises to build cyber preparedness, (iii) undertaking vulnerability assessments to identify vulnerabilities for remediation, and/or (iv) providing system information to develop and maintain a near real-time threat picture.[5]

2.2.2 CIRMP - AESCSF Security Profile 1 and Essential Eight Maturity Model

36. Under the Security of Critical Infrastructure (Critical Infrastructure Risk Management Program) Rules 2023, a responsible entity must establish and maintain a process or system in the CIRMP to (a) comply with a framework contained in one of five documents referred to in the CIRMP, and (b) meet the corresponding condition for that document.[6] The CIRMP must be in place within 18 months of the commencement of the instrument or within 18 months of the asset being designated a critical (electricity) infrastructure asset.[7]

37. The 2020-21 Australian Energy Sector Cyber Security Framework (AESCSF) Framework Core published by AEMO is one of the five documents referred to in the CIRMP instrument and the condition that is required to be met is SP-1. Therefore SP-1 is the legislative obligation that NSPs must comply with if the NSP is defined as a responsible entity and selects the AESCSF as the cyber security framework.

38. Equally, the *Essential Eight Maturity Model* (EEMM) published by the Australian Signals Directorate is another referenced framework and the condition if it is adopted by an NSP is meeting Maturity Indicator Level one (MIL-1). Therefore MIL-1 is the legislative obligation to which NSPs must comply with if the NSP is defined as a responsible entity and selects the EEMM as its cyber security framework.

2.2.3 Privacy Act amendments 2022[8]

39. The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 ('Bill') amends the Privacy Act 1988 to expand the Australian Information Commissioner's enforcement and information sharing powers, and to increase penalties for serious or repeated interferences with privacy.

40. The Bill increases the maximum penalty under section 13G of the Privacy Act for a body corporate to an amount not exceeding the greater of $50 million, three times the value of the benefit obtained or, if the court cannot determine the value of the benefit, 30% of their adjusted turnover in the relevant period. The maximum penalty of $50 million is an increase from the pre-existing maximum of $2.22m.

---

3 CISC Factsheet – Systems of National Significance and Enhanced Cyber Security Obligations

4 Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023 – explanatory statement

5 Department of Home Affairs, Cyber and Infrastructure Security Centre website

6 Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023; subsection 8 (4)

7 Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2023; subsection 4(2) and subsection 8(3)

8 https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r6940

41. Within the Explanatory Memorandum to the Bill, it is stated that '*[b]y strengthening penalties, Australia will be signalling its expectations that businesses undertake robust privacy and security practices.*'[9]

2.2.4 Distributor's Licence under the Electricity Supply Act 1995 (NSW) – Licence Conditions Variations[10]

42. Critical Infrastructure Licence Conditions 9 (Substantial presence in Australia), 10 (Data Security), and 11 (Compliance) of the Licence are of relevance to DNSPs in NSW. Within these Conditions there are multiple requirements. Among other things, Condition 11 requires the Licence Holder to report to the Tribunal by 30 September each year detailing how it has complied with conditions 9 and 10 over the preceding financial year.

2.3 The Australian Energy Sector Cyber Security Framework (AESCSF)

2.3.1 AESCSF Version 1 (V1)

43. In response to the Finkel National Electricity Market Review recommendation 2.10, in 2018 AEMO collaborated with industry and government to develop the AESCSF. Among other markets, it covers Australia's electricity sector and is voluntary but has been adopted by NSPs.[11] The AESCSF is divided into 11 domains, ten C2M2[12] domains, and the Australian Privacy Management Domain. There were minor revisions to the AESCSF in 2019, 2021, and 2022, with no significant changes in version 2022 compared to version 2021.[13] AESCSF Version 1 (V1) encompasses the 2018 and subsequent iterations up to and including the 2022 revision.

44. The AESCSF V1 program includes the Electricity Criticality Assessment Tool (E-CAT), which is designed to assess the relative criticality of NSPs and other participants in the electricity sector.

45. The E-CAT allows assessment of the relative criticality of entities participating in the electricity and other energy sectors. The diagram below represents the criticality banding for the electricity sub-sector only, with TNSPs rated as High criticality and with DNSP criticality rating ranging between the High and Medium bands.

9 Privacy Legislation Amendment (ENFORCEMENT and Other Measures) Bill 2022 EXPLANATORY MEMORANDUM, in reference to Section 13G – civil penalties (para 12)

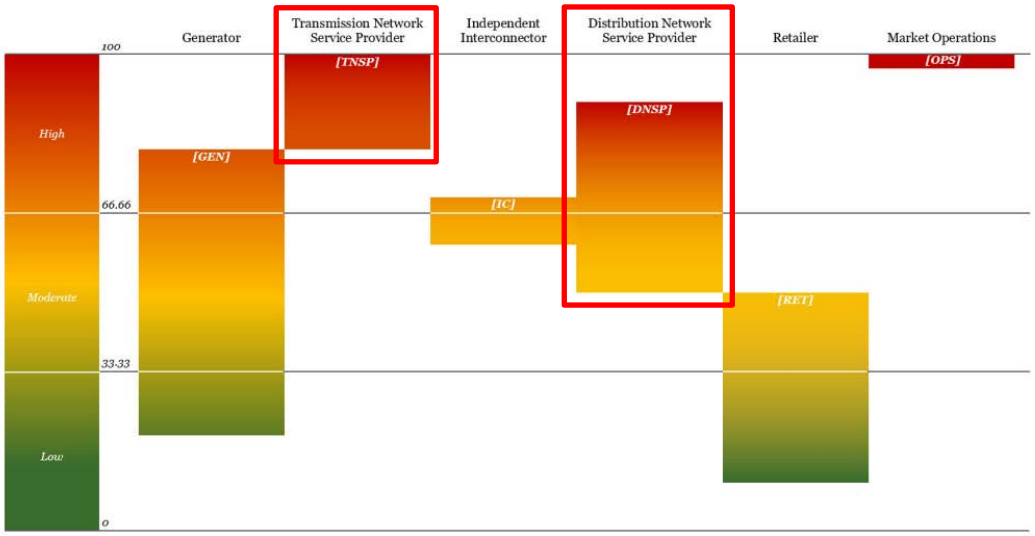
10 The Minister for Resources and Energy issues the DNSP licences. IPART administers compliance with the licence conditions on behalf of the Minister. Licence conditions for Ausgrid are available from IPART's website

11 AEMO, AESCSF Framework and Resources, AEMO website

12 United States Department of Energy Cyber Security Capability Maturity Model

13 AEMO AESCSF Framework Overview – 2022 Program, page 1

Figure 2.2: AESCSF E-CAT criticality bands for electricity sector – TNSPs and DNSPs highlighted



Source: AEMO, AESCSF Electricity Criticality Assessment Tool (E-CAT), per AESCSF V1

46. The table in the figure below '*indicates which SP an organisation in the electricity sub-sector should achieve based on their criticality (as determined by the E-CAT).*'[14] This may be construed as an obligation, however AEMO also states that *'[t]he CAT should be treated as general guidance only. Results obtained from the CAT do not indicate that an entity has obligations under or is compliant with applicable Commonwealth (Cth) legislation.'*[15]

Figure 2.3: Relationship between SPs, participant criticality , practices/anti-patterns and MILs – per AESCSF V1

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: AEMO, AESCSF Electricity Criticality Assessment Tool (E-CAT), per AESCSF V1

47. To help organisations define roadmaps to improved cyber security maturity, the ACSC included guidance on 'Priority Practices' within each Security Profile (SP). The Priority Practices are recommended for completion first as part of any uplift program. There are 20 priority practices across the 11 domains within SP-1, 5 across 5 domains in SP-2 and one in the ACM[16] domain in SP-3.[17]

2.3.2 AESCSF Version 2 (V2)

48. In December 2022, Energy Ministers endorsed AESCSF V2, providing guidance about the continued role of the program to support energy sector cyber uplift and increasing cyber

14 AEMO AESCSF Framework Overview – 2022 Program, page 9

15 AEMO AESCSF Framework Overview – 2022 Program, page 3

16 Asset, Change and Configuration Management

17 AEMO AESCSF Framework Overview – 2022 Program, pages 9, 20

security requirements for the energy sector in line with escalating and evolving cyber threats.

> *'AEMO has worked in partnership with DCCEEW and the Department of Home Affairs Critical Infrastructure Centre (CISC) on the 2023 Program to support energy organisations' continued cyber maturity journey and to support energy organisation's Risk Management Plan (RMP) regulatory obligations under the SoCI Act.'*[18]

49. The 2023 program intends to support AESCSF V2 assessment, AESCSF V1 (noting RMP minimum obligations), and a transition plan to 'sunset' AESCSF V1.

50. The release of AESCSF V2 was scheduled for May-June 2023, but at the date of writing this report, no further information about the V2 is available on the AEMO website.

2.4 AER Guidelines for non-network ICT assessment

2.4.1 Assessment of non-network ICT capex

51. The scope of our assessment includes cyber security capex and opex and is categorised as non-network ICT.

52. The AER's 2019 non-network ICT capex assessment approach guideline ('ICT assessment guideline') is relevant to Ausgrid's proposed cyber security capex. The proposed expenditure is also 'non-recurrent'.

53. The AER requires DNSPs to allocate their non-recurrent ICT expenditures into the three subcategories for which it applies different assessment approaches, as described below.[19]

Maintaining existing services, functionalities, capability and/or market benefits

54. The AER states that: '*Given that these expenditures are related to maintaining existing service, we note that it will not always be the case that the investment will have a positive NPV. As such, it is reasonable to choose the least negative NPV option from a range of feasible options including the counterfactual.*[7] *For such investments, we consider that they should be justified on the basis of the business case, where the business case considers possible multiple timing and scope options of the investments (to demonstrate prudency) and options for alternative systems and service providers (to demonstrate efficiency). The assessment methodology would also give regard to the past expenditure in this subcategory.'*

Complying with new / altered regulatory obligations / requirements

55. The AER states that: *'It is likely that for such investments, the costs will exceed the measurable benefits and as such, the least cost option will likely be reasonably acceptable in regard to the NER expenditure criteria. Therefore the assessment of these expenditures is similar to subcategory one. Should there be options to achieve compliance through the use of external service provides [sic], the costs and merits of these should be compared.'*

New or expanded ICT capability, functions and services

56. The AER states that: '*We consider that these expenditures require justification through demonstrating benefits exceed costs (positive NPV). We will make our assessment therefore through assessing the cost-benefit analysis. Where benefits exceed costs consideration should also be given to self-funding of the investment.*

57. *For each subcategory of non-recurrent expenditure, we note that there may be cases where the highest NPV option is not chosen. In these cases, where either the chosen option*

18 AEMO website, AESCSF Program

19 In cases where programs/projects cover multiple categories of expenditure, the distributor is expected to apportion costs from individual components across multiple categories to reflect the nature of the work undertaken

achieves benefits that are qualitative or intangible, we would expect evidence to support the qualitative assumptions. We consider the evidence provided must be commensurate with the cost difference between the chosen and highest NPV option.

58. *We also note that where non-recurrent projects either lead to or become recurrent expenditures in the future, this needs to be identified in the supporting business case and accounted for in any financial analysis undertaken to support the investment.*'

2.4.2 Assessment of opex step changes

59. Section 2.2 of the AER's Expenditure Forecast Assessment Guideline for Electricity Distribution outlines its general approach for assessing opex step changes and which we have followed. In summary:[20]

- The AER separately assesses the prudency and efficiency of forecast cost increases or decreases from new regulatory obligations and capex/opex trade-offs;
- For capex/opex trade-off step changes, the emphasis is on establishing whether it is prudent and efficient to substitute opex for capex; and
- For step changes arising from new regulatory obligations, the emphasis is on:
  - whether there is a binding change in regulatory obligations that affects the efficient forecast opex and when the change occurred
  - what options were considered and whether the selected option is an efficient option.

2.5 Implications for our assessment

Increasing threat landscape and attack surface mean cyber risk is increasing

60. The advice from government agencies is that both the cyber-attack landscape is worsening and the cyber-attack surface presented by NSPs is increasing, leading to an increasingly higher risk of cyber-attack and potential breach.

61. In our assessment we have sought to understand how Ausgrid has incorporated the increasing threat landscape and attack surface issues into its risk analysis and, ultimately into its option selection and proposed expenditure profile.

Cyber security compliance obligations for NSPs are derived from four aspects of the (amended) SOCI Act and from consideration of certain amendments to the Privacy Act

62. The minimum obligations for NSPs under the SOCI Act have been enhanced over the period FY22 and FY23 to include the following:

- Register of Critical Infrastructure Assets;
- Mandatory Cyber Incident Reporting; and
- CIRMP, which requires completion of all the practices (and absence of anti-patterns) required to achieve SP-1 (per AESCSF V1) by mid-2024, noting that SP-1 is the least onerous of the security profiles under the AESCSF.

63. If NSPs are classified as a SoNS, then ECSOs apply and which are applied on a case-by-case basis to the NSPs.

64. Further the civil penalties for a breach(es) of the Privacy Act have been increased in 2022 from $2.2m to $50.0m (maximum) with the expectation from the Federal government via the amendment that organisations such as Ausgrid will act accordingly to '*undertake robust privacy and security practices*' which we interpret to include cyber security-related practices.

65. We have assessed how Ausgrid has responded to its common and specific cyber security compliance obligations, cognisant of:

[20] AER, Expenditure Forecast Assessment Guideline for Electricity Distribution, p11

- the worsening threat landscape and attack surface issues; and
- its expected cyber security compliance position at the end of the current RCP.

66. We have also considered whether Ausgrid has identified any other relevant obligations.

Licence Conditions Variations to a Distributor's Licence under the Electricity Supply Act 1995 (NSW) do not represent new obligations

67. The Instrument of Variation to the Distributor's Licence has been available since 2019. We consider that Ausgrid should by now have responded to the conditions. We therefore consider that the opex implications of the Licence variations will be a part of the efficient base year and there are unlikely to be new non-recurrent capex or recurrent opex/opex step change arising from the variations.

AESCSF V1 was available for the preparation of Ausgrid's RP but the intent of V2 has already been promulgated

68. AESCSF V1 was the current version when Ausgrid prepared its RP and therefore the extent to which it has referenced this Program and, possibly, the Priority Practices, in developing its cyber security forecast expenditure for the next RCP is relevant.

69. However, it is also relevant to consider the extent to which Ausgrid has incorporated other frameworks, if any, into its proposed expenditure.

70. Whilst AESCSF V2 has not been publicly released at the time of writing this report, we assume that because V2 was '…*developed in consultation with industry, governments and specialist agencies*…'[21] that Ausgrid was broadly aware of the likely increase in the hurdles (number of practices) to achieve each of the three MILs and three SPs compared to V1. Again, it is relevant to take into consideration Ausgrid's incorporation of future regulatory obligations where there is a reasonable evidenced understanding of what they will be, noting that it has the opportunity for applying to the AER for a pass through if new obligations occur after approval of its RP and which could not reasonably have been anticipated.

71. It is reasonable also to consider Ausgrid's E-CAT score (if available) and its target SP level at the end of the current RCP and at the end of the next RCP, the initiatives it proposes to achieve them and by when, and the estimated costs of each.

[21] AEMO website, AESCSF Program

3 REVIEW OF PROPOSED ICT CYBER SECURITY EXPENDITURE

Ausgrid has proposed a cyber security-related capex allowance of $44.0m, $47.0m SaaS opex, and an opex step change of $20.6m. It has targeted fully implementing practices to achieve AESCSF Security Priority-3 maturity within the next RCP to reduce its residual cyber risk to 'Medium'.

We consider that Ausgrid should instead adopt a risk-prioritised approach to building its cyber security maturity, implementing SP-3 practices that offer the best value for money. We consider that an acceptable risk level can be achieved with considerably less totex than proposed by Ausgrid.

3.1 Overview of proposed expenditure

3.1.1 What Ausgrid has proposed in its RP

72. Ausgrid has advised that, for SCS, it expects to incur $44m capex and $47.0m SaaS opex on cyber security in the next regulatory period, a total of $91m. In addition, Ausgrid has proposed an opex step change of $20.6m.

73. We have assessed Ausgrid's proposed capex and opex step change, which together with the SaaS opex are shown in Table 3.1.

Table 3.1: Ausgrid proposed SCS ICT cyber security related expenditure - $million, real FY2024

Description	2025	2026	2027	2028	2029	Total
Non-recurrent ICT- cyber security related capex	9.0	9.0	9.0	8.0	9.0	**44.0**
Non-recurrent SaaS opex	10.0	9.0	9.0	10.0	9.0	**47.0**
Opex step change – ICT cyber security	2.4	4.0	4.4	4.7	5.1	**20.6**
Total SCS cyber security expenditure	**21.4**	**22.0**	**22.4**	**22.7**	**23.1**	**111.7**

Source: Ausgrid RP document, Figure 5.9.2 and Opex model (Attachment 6.1.b)
Note: numbers may not add exactly due to rounding errors

3.2 Summary of the basis for Ausgrid's proposed cyber security expenditure

3.2.1 Documents supporting proposed cyber security program

74. Ausgrid initially provided two core documents to support its cyber security strategy, initiatives and investment:

- Attachment 5.9 – Technology Plan for 2024-29 – 31 Jan 2023
- Attachment 5.9.c – Cyber security program – 31 Jan 2023d

75. The Technology Plan covers a range of matters whereas the Cyber security program document is singular in its focus and is our primary reference document. We also made

several formal information requests (IR) to Ausgrid. We draw on Ausgrid's responses in our assessment.

3.2.2 Ausgrid's problem definition and risk assessment

76. In its Cyber security program document the increase in cyber security risk is recognised, with the sources as discussed in section 2 (i.e. increased sophistication and frequency of attacks and Ausgrid's increase attack surface due to increased connectivity and automation).

> *'In the worst possible scenario, a complete shutdown of our network (which includes the Sydney CBD) would have catastrophic implications for the community … For our customers, a cyber breach of this magnitude impacting our network, even for a few hours, would severely disrupt lives and livelihoods.'*[22]

77. Ausgrid also provides an analysis of the changes to its compliance obligations, including to the SOCI Act, via SLACIP Act, the SLACI Act, and the Privacy Act. Ausgrid also outlines its NSW-specific License conditions which are relevant to its cyber security program.[23]

78. Ausgrid rates its inherent (current) cyber security risk as very High, rising to 'Extreme' by the end of the current RCP (i.e. FY24).[24] Without any intervention to mitigate risk in the next RCP, Ausgrid has assessed that its cyber security risk will be at the 'upper end' of Extreme by FY29, presumably because it has rated each of seven sources of cyber security risk to be Extreme by FY29. In each case, the likelihood of the risk manifesting is assessed to be 'Almost certain' and the consequence is assessed by Ausgrid to be 'Significant' (which is the most severe consequence rating).

3.2.3 Ausgrid's cyber security strategy and objectives

79. Ausgrid summarises eight drivers shaping its cyber security planning given that '…it services the Sydney CBD and other critical infrastructure businesses which account for 30% of Australia's gross domestic product.'[25]

80. Ausgrid's cyber security strategy is to align to the AESCSF and the objective is 'to meet our statutory and regulatory obligations and to remain within risk appetite for the risk of a significant protective security incident.'[26] It has designed its investment to achieve SP-3 in FY27.[27]

81. Ausgrid's investment objectives are listed as '*prudently and efficiently:*

- Mitigating assessed, known, emerging and future cyber security risks;
- Countering the increasing cyber threat, we face from multiple threat actors;
- Maintaining control design and effectiveness of implemented cyber security controls;
- Implementing new cyber security controls to mitigate known, unknown risks in the corporate and OT environments; and
- Providing our customers, the assurance that we can identify, detect, protect, and respond to increasing cyber security threats.'[28]

22 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 5

23 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, pages 11, 12

24 Ausgrid - EMCa Technical Review - 17 Apr 2023, slide 22

25 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 9

26 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 15

27 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 16

28 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, pages 16-17

3.2.4 Ausgrid's cyber security current state

82. Ausgrid advises that it is fully compliant with all of its regulatory cyber security obligations.[29] It further reports that in September 2022 it had achieved:[30]

- [redacted] SP-1 practices;
- [redacted] of SP-2 practices; and
- [redacted] SP-3 practices, although in the same source document [redacted] of SP-3 practices are reported as being achieved overall.

3.2.5 Options considered by Ausgrid for managing cyber security obligations and risks

83. Ausgrid considers three options in its Cyber security program document:[31]

- Option 1 ($34.1m totex) – Current minimum compliance: maintains SP-1, with no significant investments in cyber security practices and systems in the next RCP;
- Option 2 ($84.8m totex) – Base Case – Enhance cyber security maturity level: achieve and perform security practices at AESCSF SP-2; and
- Option 3 ($111.7m totex) – Target state – Highest cyber security maturity level: Active management of cyber risk expands on SP-2 and enables achievement of SP-3.

84. Ausgrid's preferred option is Option 3 with $44.4m SCS[32] capex, $46.7m SCS opex and an opex step change of $20.6m ('ongoing new opex').

29 IR011 Ausgrid - 1f. Cyber Security Strategy 2023 v2 - 20230414 – Confidential, slide 7

30 IR011 Ausgrid - 1c. Ausgrid's most recent AESCSF assessment - 20230414 - Confidential

31 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, Table 4

32 Cost allocation method (CAM) allocated standard control services (SCS) component.

4 OUR ASSESSMENT

We consider that Ausgrid's cyber security risk assessment leads to an unnecessarily onerous target of achieving fully implemented SP-3 practices by the end of the next RCP and consequently an unreasonably high cost. We consider that a prudently-applied risk prioritisation-based approach would lead to SP-3 practices being largely implemented at lower cost.

While each NSP has its own circumstances to consider, we have reached this conclusion based on the electricity industry cyber security experience available to us within our team and also through comparing approaches that are being applied by a range of NSPs that we have reviewed.

4.1 Observations on Ausgrid's current state and cyber security priorities for the current RCP

Ausgrid is currently [redacted] and we would expect a prudent network service provider to continue to improve its cyber security maturity throughout the current RCP

85. As reported in September 2022, Ausgrid had achieved [redacted] of SP-1 practices[33] and was fully compliant with its relevant NSW Licence, SOCI Act, SLACI Act, SLACIP Act and Privacy Act obligations.[34] We understand from its Proposal that the cost of remaining compliant with these obligations (and sustaining SP-1) is an average annual cost of $6.8m (totex) based on Ausgrid's proposed Option 1.

86. As of September 2022 (and possibly prior to that) Ausgrid was also assessed as having achieved [redacted] of the 112 SP-2 practices and [redacted] of the 82 SP-3 practices.[35]

Ausgrid's cyber security budget in the current RCP is $41.7m which supports cyber security maturity improvements

87. We would expect that Ausgrid would continue to invest in progressing its cyber security maturity through to the end of the current RCP. This appears to be the case, with Ausgrid stating in its 2023 Cyber Security Strategy that its highest priority projects for the ensuing 12 months are for:[36]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

88. These projects combine to mostly achieve SP-2 practices in five of the eleven AESCSF domains by the end of the FY24. It is evident from Ausgrid's 'long term plan'[37] shown in Figure 4.1 that some other SP-2 practices will be implemented by the end of FY24 but that it does not plan to achieve SP-2 until FY25. These cyber security enhancements and

33 When we refer to AESCSF practices being largely or fully implemented, we recognise that anti-patterns must also be assessed as being absent but we do not continually refer to them for the sake of brevity

34 Ausgrid - EMCa Technical Review - 17 Apr 2023, slide 17

35 [redacted]

36 IR011 Ausgrid - 1f. Cyber Security Strategy 2023 v2 - 20230414 – Confidential, slide 4

37 IR011 Ausgrid - 1f. Cyber Security Strategy 2023 v2 - 20230414 – Confidential, slide 13

[redacted] is underpinned by a budget of $41.7m in the current RCP[38] (compared to the proposed $91.1m[39] for the next RCP as shown in Figure 4.2).

89. Ausgrid has not identified a Base Year cyber security opex component.[40]

Figure 4.1: Ausgrid's long term cyber security plan

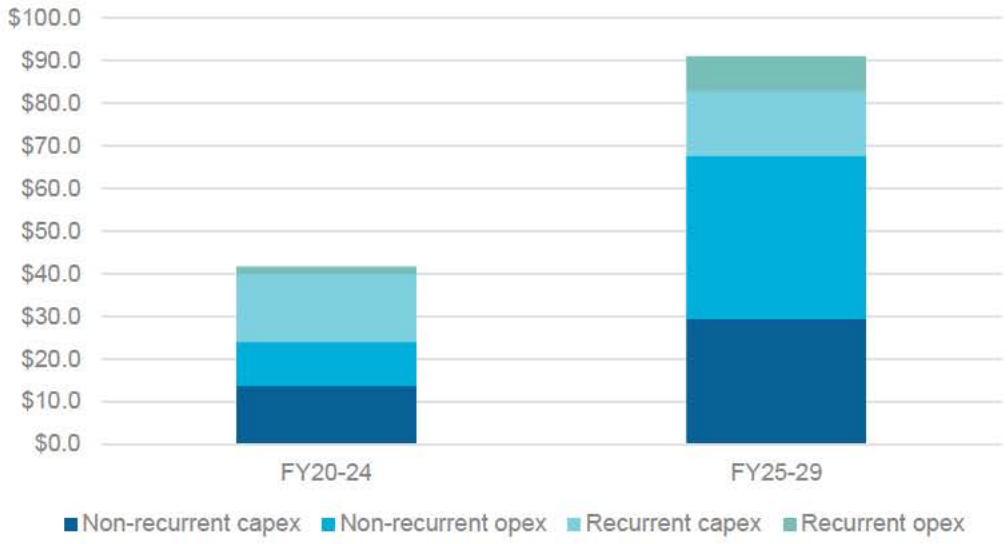
[redacted]

[38] IR011 Ausgrid - 1.b. Cyber Expenditure - 20230414 – Public, not including 'business as usual' non-recurrent opex

[39] Not including opex step change (aka 'opex uplift from base year' / 'ongoing new opex') of $20.6m

[40] Ausgrid - Att. 6.1.b - Step changes model - 31 Jan 2023 – Public

Figure 4.2: Ausgrid's actual and proposed cyber security expenditure (opex is only for SaaS configuration costs) $m, real FY2024



Source: IR011 Ausgrid – 1.b. Cyber Expenditure – 20230414 – Public; FY25-29 excludes $20.6m of 'ongoing new opex'

4.2 Ausgrid's risk analysis

Ausgrid has appropriately identified the increasing cyber security risks in the electricity sector which will lead to an increased risk profile for its operations over the next RCP

90. We are satisfied that there is a case for action by Ausgrid in the next RCP to address what it has appropriately identified as an increasing cyber security risk profile from the combined effects of:

- Increasing cyber security threat landscape; and
- Increasing Ausgrid attack surface.

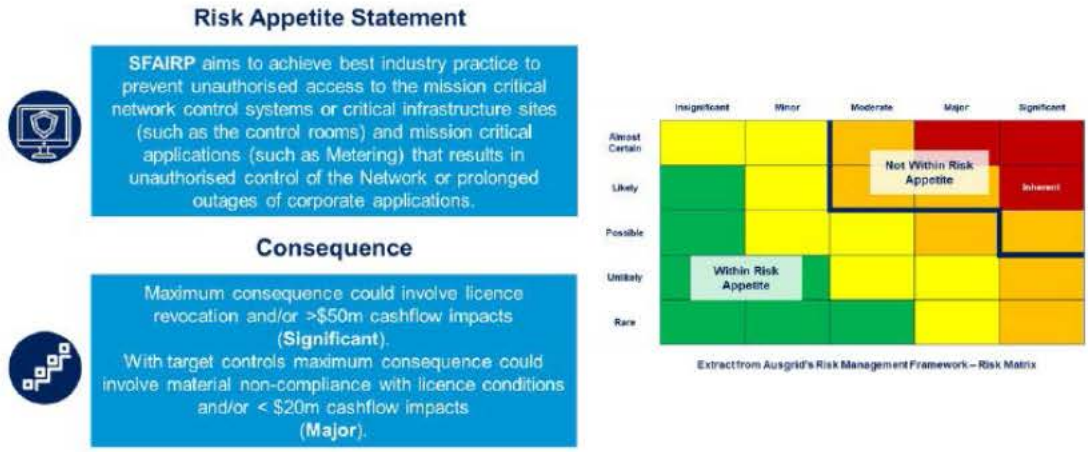
91. Our focus in the remainder of this section is Ausgrid's application of its corporate risk matrix to establish the residual risk level (i.e. without further intervention and at the end of FY29).

Ausgrid's risk appetite for cyber security is based on the SFAIRP principle

92. Ausgrid aims to '*achieve best industry practice to prevent a significant protective security incident so far as is reasonably practical*' as shown in the figure below with its interpretation of the limits to its risk appetite in the context of its Risk Matrix.

93. In accordance with the AER's guidelines, if Ausgrid proposes to invest in improving its risk profile it needs to demonstrate that there is a net economic benefit in doing so. We discuss this further in assessing Ausgrid's preferred Option 3 in section 4.5.4.

Figure 4.3: Ausgrid's risk statement, risk appetite, and risk matrix



Source: Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, Figure 5

Ausgrid has undertaken qualitative and quantitative risk assessment

94. Ausgrid presents a qualitative and a quantitative (probabilistic risk-cost) analysis of the cyber security risk by the end of the next RCP under Options 1, 2 and 3. We consider each of these insights into Ausgrid's risk assessment, starting with Option 1 in this section and Options 2 and 3 in sections 4.5.3 and 4.5.4, respectively.

Ausgrid's has assessed its residual (FY29) cyber risk rating as Extreme

95. Ausgrid has assessed the inherent (or current) cyber risk and the residual (FY29) cyber risk across seven risk sources. The Inherent risk rating is assessed by Ausgrid to be High, bordering on Extreme (refer to Figure 4.5). In Table 4.1, Ausgrid summarises the residual risk assessment for the three options it has evaluated.

Table 4.1: Ausgrid's assessment of key risks and residual position by FY29

	Option 1		Option 2		Option 3	
Risk description	Likelihood x Consequence	Risk rating	Likelihood x Consequence	Risk rating	Likelihood x Consequence	Risk rating
R1 – Ransomware attacks	Almost certain x Significant	Extreme	Likely x Major	High	Possible x Major	High
R2 – Compromise via unpatched applications	Almost certain x Significant	Extreme	Likely x Major	High	Possible x Moderate	Medium
R3- Data loss	Almost certain x Significant	Extreme	Likely x Major	High	Possible x Moderate	Medium
R4 – Insider attack	Almost certain x Significant	Extreme	Likely x Major	High	Possible x Moderate	Medium
R5 – External attack	Almost certain x Significant	Extreme	Likely x Major	High	Possible x Major	High
R6 – Supply chain /vendor compromise	Almost certain x Significant	Extreme	Likely x Major	High	Possible x Major	High
R7 – Non-compliance to regulatory requirements	Almost certain x Significant	Extreme	Likely x Major	High	Unlikely x Moderate	Medium

Source: Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, Tables 18-20, Figure 11

96. Figure 4.4 shows Ausgrid's definition of Likelihood of the cyber security risks R1-R7 manifesting.

Figure 4.4: Ausgrid's definitions of Likelihood

Likelihood	*Frequency*	*Probability*
Almost certain	1 in 0.2 year event	500%
Likely	1 in 1 year event	100%
Possible	1 in 10 year event	10%
Unlikely	1 in 25 year event	4%
Rare	1 in 125 year event	0.8%

Source: Ausgrid - EMCa Technical Review - 17 Apr 2023, slide 22

97. Whilst there are definitions of 'significant' consequence across six dimensions in Ausgrid's explanation of its Risk Management process,[41] the bases for the consequence assessments in Table 4.1 are not presented in the source tables nor in the contiguous descriptions. Significant events represent consequences with the highest impact that Ausgrid can identify and we consider them further below, but first we focus on Ausgrid's assigned Likelihood ratings.

For option 1, we consider that an overall Likelihood rating of 'Likely' is more appropriate

98. Option 1 is designed to maintain SP-1, with no significant investments in new or enhanced cyber security practices and systems in the next RCP. As indicated from the proposed totex of $34.1m, it is far from a zero-cost option. The mitigating controls under Option 1 include all the cyber security measures in place by the end of the current RCP, which, as discussed above:

- Are sufficient to satisfy the minimum requirements of the SLACI Act;
- Are sufficient to satisfy the other relevant cyber security-related obligations under the SLACI Act and the SLACIP Act;
- Are sufficient to address the 20 cyber security-related NSW Distribution Licence obligations;
- Will include completion of the five high priority projects; and
- Will include a significant number of SP-2 practices and some SP-3 practices, presumably selected for their positive impact and deliverability.

99. Furthermore, Option 1 includes provision for upgrades of certain cyber security related systems and software during the course of the RCP (as discussed further below), which will improve their efficacy.

100. Also, upgrades/refreshes of other IT and OT systems/applications will occur over the course of the next RCP under the ICT program which, among other things, will provide patches and other improvements in cyber security.[42]

101. With these controls, and cognisant of the assumed consequences and the lack of compelling evidence from Ausgrid, we consider that it is not reasonable to conclude that it is likely that there will be (on average) five successful attacks (i.e. 'almost certain') through the causes denoted in Table 4.1 during the next RCP under this option.

102. Based on the occurrence of cyber breaches in the energy sector in Australia and in the rest of the world, we do however consider a rating of 'Possible' or 'Likely' is more appropriate for

41 IR011 Ausgrid - 1h. Framework - Risk Management - 20230414 – Confidential, page 26

42 For example, transitioning so IaaS or SaaS is likely to offer more robust cyber security

risks R1-R6 by 2029.[43] In our view, risk R7 (regulatory non-compliance) is a Low risk because of the controls in place and the introduction of any new obligation would both allow time for compliance and the opportunity for Ausgrid to secure a pass-through of costs from the AER.

103. On this basis, most of the risks denoted in Table 4.1 by the end of the next RCP under the Option 1 scenario would be 'High' or, at worst, 'Extreme'.

104. We next compare this qualitative analysis with Ausgrid's quantitative analysis.

Ausgrid's quantification of the Likelihood of events occurring appear to be overstated

105. Ausgrid presents eight consequence examples, listed in Table 4.2, which we assume include the highest event / consequences that it could identify. In addition to the estimated consequence value, Ausgrid has determined the Likelihood of each event for Options 1-3.

106. From the descriptions of the events and the derivations of the likelihoods and consequences, we consider that risks 1, 4, 5 and 6 are linked. We discuss the interrelationships below as part of discussion of Ausgrid's quantification of consequences.

107. Our assessment of Ausgrid's Likelihood quantification for Option 1 at the end of the next RCP is:

- Risks 1 and 6: Ausgrid assumes 0.44% likelihood, which is equivalent to the event occurring on average once every 227 years
  - the derivation of 0.44% is not apparent to us in the information provided,[44] however given that the scenario is a 24hr outage of the whole Ausgrid network, we consider that the Likelihood estimate is of the right order
  - this likelihood would be classified as 'Rare' on Ausgrid's qualitative scale and would lead to a risk rating of no more than 'High' using Ausgrid's risk matrix;
- Risks 2 and 3: Ausgrid assumes 44%-47% likelihood, which is equivalent to the event occurring once every 2.2 years on average, which is approximately 100 times more frequently than the 24-hour system blackout scenario
  - again, the derivation of the likelihood of the risks manifesting is not apparent to us, however for the denoted consequences, we consider the likelihood to be of the right order
  - this likelihood falls between Ausgrid's 'Likely' and 'Possible' quantitative classifications and would lead to a risk rating of 'High' or 'Extreme' using Ausgrid's risk matrix, depending on the consequence rating;
- Risks 4 and 5: Ausgrid assumes 44% likelihood, which is equivalent to the consequence occurring every 2.7 years on average, and which is approximately 100 times more frequently than the source event (the Ausgrid network being black for 24 hours)
  - the derivation of the likelihood of the risks manifesting is not apparent to us, however for the denoted consequences, we consider that 0.44% is a more reasonable likelihood for these risks because our understanding is that the consequences arise from the same outage scenario as risks 1 and 6[45]
  - this likelihood would be classified as 'Rare' on Ausgrid's qualitative scale and would lead to a risk rating of no more than 'High' using Ausgrid's risk matrix; and
- Risks 7 and 8 were not quantified by Ausgrid.

---

43 Whilst we consider that a 100% likelihood (1 per year) is too high for the cyber risks denoted, an alternative definition that has been applied by others for 'Likely' that is '*Has occurred in the last few years in this organisation or has occurred recently in similar organisations'* which we think is more applicable given the recent successful cyber-attacks in Australia

44 This figure and all the Likelihood percentages applied in Ausgrid's CBA are hard coded (Ausgrid - Att. 5.9.i - Cyber security CBA model - 31 Jan 2023 – Public)

45 Ausgrid - EMCa Technical Review - 17 Apr 2023, slide 20

Table 4.2: Ausgrid's cyber event consequence examples

Consequence description	Consequence value	Source of impact	Likelihood Option 1
1. Unplanned local supply outage	$2,900m	Unplanned outage for 24 hours, average cost/customer = $1,597	0.44%
2. Delays in being able to publish key data to market	$4m	Restoration costs Fines	44%
3. Unauthorised access to, or use of, personal data	$0.42m	Restoration costs Fines	47%
4. Lost staff productivity due to reduced access to key corporate or operational systems	$44m	Restoration costs Lost productivity	44%
5. Delays to planned maintenance	$34m	Restoration costs Lost productivity	44%
6. Manual control of the grid	$29m	Restoration costs	0.44%
7. Unauthorised access to or use of network data	Not quantified	Restoration costs Fines	Not quantified
8. Life support customers at risk of outages without support	Not quantified	Restoration costs Fines	Not quantified

Source: Ausgrid – IR011 - Risk Matrix – 20230428 - Confidential

Ausgrid's quantification of the consequences of some events appear to be excessive

108. Table 4.2 shows Ausgrid's consequence values for six scenarios. In response to an Information Request, Ausgrid provided more detail regarding the derivation of the consequence values for risks 1, 4, 5, and 6, which are all linked to the following scenario:[46]

> *'Threat actor attacks corporate network with malware and disables core ICT systems then moves laterally to the OT control network, and deposits malware that disables the control system as part of an attack on Australia's critical infrastructure resulting in a total network shutdown and power outage in the Sydney CBD.'*

109. Taking the extra information into account, we consider that the majority of Ausgrid's consequence values are overstated for the following reasons:

- Unplanned outage cost: 24 hrs system black for loss of 67 million kWh at a blended VCR of about $43/kWh;[47]
  - in our view a more reasonable estimate is based on assuming that 30% to 50% of the supply would be restored through manual intervention or by other means,[48] which reduces the consequence value;
- Lost staff productivity: disruption for 20 days, reducing staff productivity to 40% at a cost of $44m;

[46] Ausgrid – IR011 - Risk Matrix – 20230428 – Confidential and Ausgrid - Att. 5.9.i - Cyber security CBA model - 31 Jan 2023 - Public

[47] IR011 Ausgrid - q.11 - Cyber calculation - 1 day _ 1 hr VCR - 20230414 - Public

[48] A common assumption in power supply interruptions analysis is that a proportion of the lost supply will be restored (typically 50%) by the mid-point of the full duration of the supply interruption by deploying operational controls; in the 24 hr Ausgrid outage scenario cause by cyber-attack, we consider that it is reasonable to assume that manual restoration of the Sydney CBD and other high priority customers would likely proceed according to predetermined and practiced emergency response procedures, restoring supply to somewhere between 30% and 50% of demand within 12 hours; the restoration of the rest of the customers would likely take another 12 hours and perhaps a bit longer for the last customers

  - again, the relevant assumptions underpinning the 20 days and the 40% are hard-coded in Ausgrid's cybersecurity cost-benefit analysis, but we understand that the duration was derived by Ausgrid's subject matter experts (SME);
  - we appreciate that some assumptions need to be made to estimate the impact for the purposes of risk assessment, however we consider that a more reasonable assumption is that there would be a declining negative impact on productivity over the 20 days as supply restoration progresses, so we consider that a 30% to 50% factor should be applied to this consequence value also;
- Cost of manual control: 400 staff required to operate the network manually for 4 weeks until the IT/OT systems are fully restored:
  - for the same reasons described above, we consider a 30% to 50% factor should be applied to this consequence value; and
- Cost of Ausgrid planned maintenance: four weeks disruption to planned maintenance
  - for the same reasons described above, we consider a 30% to 50% factor should be applied this consequence value.

110. The cost of delays to publishing data and the cost of unauthorised data access are reasonable in our view.

Ausgrid's probabilistic risk cost under Option 1 is overstated

111. In Table 4.3 we summarise the difference between Ausgrid's quantified risk and our adjustments for what we consider to be more reasonable Likelihood and Consequence values for Option 1. The mid-point of the range that we assess is approximately $50m.

Table 4.3: EMCa's adjustment of Ausgrid's Option 1 risk-cost analysis

	Ausgrid			EMCa		
Consequence description	Value	Likelihood	Risk cost (pa)	Value range	Likelihood	Risk cost range (pa)
Unplanned outage	$2.9b	0.44%	$25.1m*	$1.5b-$2.0b	0.44%	$6.6m - $8.8m
Delays to data publishing	$4m	44%	$1.8m	$4m	44%	$1.8m
Unauthorised data access	$0.4m	47%	$0.2m	$0.4m	47%	$0.2m
Lost staff productivity	$44m	44%	$19.2m	$22m-$31m	0.44%	$0.1m-$0.15m
Maintenance delays	$34m	44%	$14.9m	$17m-$24m	0.44%	$0.1m
Manual control of grid	$29m	0.44%	$0.1m	$15m-$20m	0.44%	$0.1m
Total risk cost p.a.			**$61.3m**			**$8.9m-$11.2m**
Risk cost over 5 years			**$307m**			**$44.5m-$56m**

Source: EMCa analysis of Ausgrid's modelled risks in Ausgrid – IR011 - Risk Matrix – 20230428 – Confidential

** This value is presented in Ausgrid's table on slide 2, however there appears to be an error – with $2.9m consequence cost at a probability of occurrence of 0.44%, the risk-cost is $12.8m*

Avoided recovery costs could be included in Ausgrid's risk-cost assessment

112. In addition to Ausgrid's identified sources of cost accruing from a significant successful cyber-attack, we consider it would be reasonable to include costs for the following recovery imperatives:

- Sanitising and rebuilding systems, including the required forensic analysis; and
- Remediation of security gaps.

113. For a business of Ausgrid's size and complexity, we estimate the cost to be approximately $10m, which it is reasonable to assume is likely to be required once every five years on average if there was no further investment in building Ausgrid's cyber security maturity level. Therefore, the risk-cost of this element for the next RCP would be an estimated $10m.

Our estimate of the benefit of avoiding a successful cyber-attack is $60m ±20%

114. Combining our revised estimate of Ausgrid's risk-cost calculation with our supplementary avoided cost estimate, we conclude that a more reasonable estimate of the 5-year cumulative risk-cost associated with Option 1 would be of the order of $60m ±20%[49] (i.e.$48m to $72m). This is significantly less than the $307m risk-cost estimated by Ausgrid (which is reduced to $243m if its calculation error is corrected).[50]

4.3 Ausgrid's cyber-related objective

Ausgrid's investment objective is appropriate as long as the investment is demonstrated to be prudent and efficient

115. As discussed in section 3.2.3, Ausgrid's cyber security objective is to enhance its cyber security controls to prevent and/or detect malicious or unintentional security incidents. We consider this to be a reasonable objective and we further note that Ausgrid confirms in its cyber security strategy the need to mitigate the risk *prudently and efficiently*.[51]

Ausgrid's selection of SP-3 is based on its risk assessment and the AESCSF criticality assessment

116. Ausgrid states that it is risk averse in relation to cyber security and that being exposed to a 'High' or 'Extreme' risk rating is not within its risk appetite. Referring to Figure 4.3, some overall risk ratings of High are acceptable to Ausgrid (e.g. for Possible/Major events) but others are not (for example, Likely/Moderate events).

117. Furthermore, it considers that as it has a 'High' criticality rating from the E-CAT, its cyber security strategy needs to support meeting the '*requirement of the AESCSF*'[52] which it links to achievement of SP-3.

We consider that an AESCSF criticality of High does not create an obligation on DNSPs to achieve SP-3

118. The AESCSF does not create an obligation for any NSP, which AEMO states on page 3 of its AESCSF Framework Overview – 2022 Program. Rather, the AESCSF is intended to provide guidance to NSPs (and others) and whilst the AESCSF indicates that Ausgrid would benefit from SP-3 practices given its criticality, under the NER in the absence of a legislative or regulatory obligation, the prudency as well as the efficiency of the proposed investments to address risk must be demonstrated by the NSP.

---

49 A range is appropriate to help account for the simplifying assumptions made in our alternative assessment.

50 The risk-cost for the 24-hour outage should be $12.6m (yearly) using Ausgrid's assumptions.

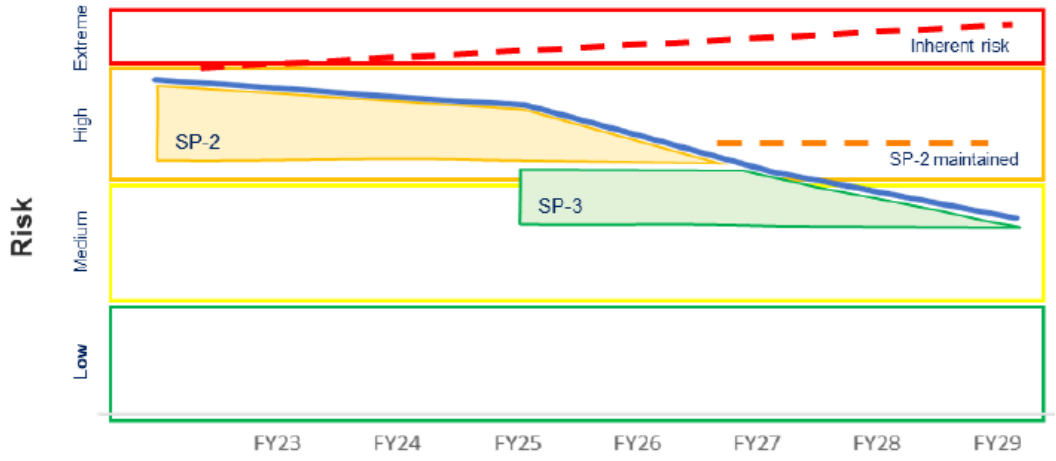
51 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 16

52 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 16

Ausgrid plans to reduce its cyber risk level from Extreme to Medium over the course of the next RCP

119. The figure below illustrates Ausgrid's intent to reduce its assumed cyber security risk over time to 'Medium' by investing to achieve fully implemented SP-3 practices by FY29, rather than maintain its risk level at 'High' (as assessed by Ausgrid).

Figure 4.5: Ausgrid's proposed 'risk buy-down'



Source: Ausgrid – IR011 - Risk Matrix – 20230428 – Confidential

120. We note from Ausgrid's qualitative assessment represented in Figure 11 in its Cyber Security Program document that the residual risk of the events with the most significant consequences are rated by Ausgrid as High (i.e. no overall reduction in qualitative risk over the next RCP from the start of the next RCP).

121. However, our assessment of Ausgrid's quantitative risk analysis indicates that, with its proposed investment, it considers that the residual risk will be reduced to 'Medium' (Unlikely or Rare/Moderate).

122. In accordance with the AER - Expenditure forecast assessment guideline - distribution - August 2022, this objective requires that Ausgrid demonstrates that the investment is likely to achieve a positive net benefit. We consider this further in section 4.5.4.

4.4 Ausgrid's cost forecasting methodology

Ausgrid has provided a detailed bottom-up build of its cost estimates but without adequate supporting information

123. Ausgrid states in its Cyber security program that:

> *The costs of each option have been estimated based on a cost build up for each individual project, based on typical delivery team resource requirements, delivery partner costs and licences.*

124. In response to an Information Request, Ausgrid provided a copy of its 'cost-build up' spreadsheet which is very useful in understanding the differences between its three options and provides insights into the resource requirements, delivery partner costs, and licence costs.

125. However, overall there is very little justification provided for the costs incurred. We have therefore largely relied upon a combination of our own experience and benchmarking against Ausgrid's peers to help assess whether its costs are reasonable – as discussed in section 4.5.

4.5 Ausgrid's options analysis

4.5.1 Overview of options

126. Ausgrid presents three options in its Cyber Security Program document. Option 2 builds on Option 1 and Option 3 builds on Option 2.

127. Ausgrid does not present a 'Do Nothing' / 'Business as Usual' option. In our view, inclusion of a BAU option is consistent with good industry practice, particularly as it can be positioned as the counterfactual for economic analysis of the options. Instead, Ausgrid has positioned Option 2 as its Base Case but it is not used as a counterfactual for its comparative analysis.

4.5.2 Option 1: Maintain cyber security maturity level

128. Option 1 is based on no extension of AESCSF maturity beyond existing activities (i.e. maintain our SP-1 position and undertakes no further activities towards SP-2 and SP-3).[53]

Ausgrid's residual risk under Option 1 is overstated

129. For reasons outlined in section 4.2, we consider that Ausgrid's residual risk (i.e. at the end of FY29) is more reasonably assessed as 'High' under Option 1 by the end of the next RCP.

Option 1 base line cyber maturity will be well above SP-1

130. Option 1 is designed to maintain SP-1 which is apparently at odds with its 12 month plan. In section 4.1 we note that Ausgrid (i) is already well above SP-1 and (ii) intends to be further advanced by the end of the current RCP.

131. Under the AESCSF, a business cannot claim to be at SP-2 unless all 200 practices are achieved, so we assume that Option 1 to be considered as not investing in further cyber security maturity and thereby *maintaining its cyber security maturity level as at FY24* (over the course of the next RCP).

Option 1 is estimated to cost $34.1m which appears to be very high for a 'no significant investment' strategy

132. The figure below shows the expenditure profile for Option 1. Given the description of the option by Ausgrid that 'No significant investments will be undertaken in our cyber security systems and practices in the 2024-29 regulatory control period, with investment deferral until the next period (2030-34)',[54] we expected much less investment throughout the RCP.

133. Of the $34.1m, $9.0m is identified by Ausgrid as ongoing new opex (aka an opex step change). The 'key drivers' of the opex step change are:[55]

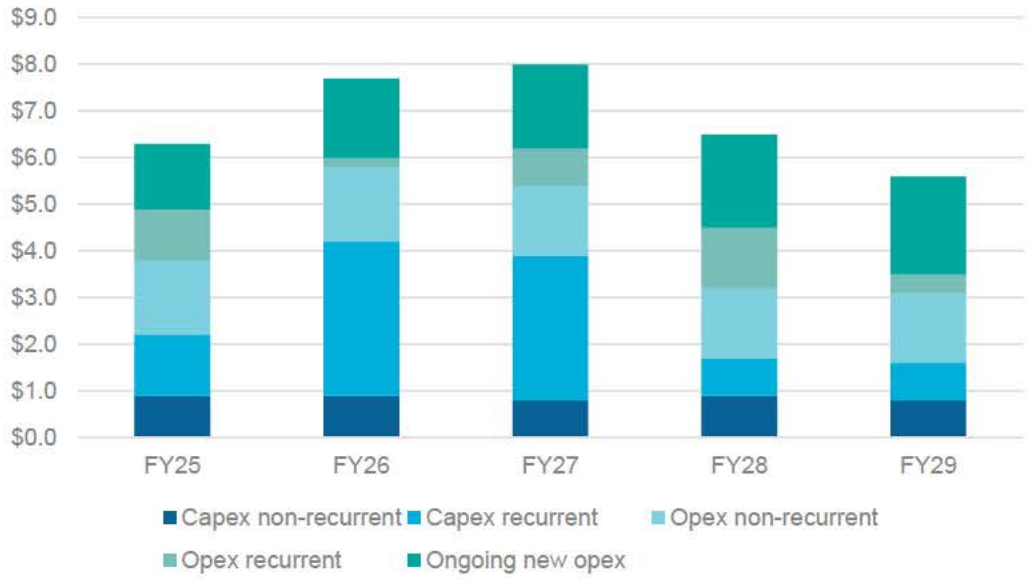
- Managed service – implement 24x7 Security Operations; and
- Ongoing licensing – cloud security product re-platform; vulnerability management (modules for new technologies/threats).

[53] Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 19

[54] Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 19

[55] Ausgrid - EMCa Technical Review - 17 Apr 2023, slide 23

Figure 4.6: Option 1 expenditure profile



Source: Ausgrid – Att. 5.9.c – Cyber security program – 31 Jan 2023 – Confidential, Tables 5, 6

An analysis of the bottom-up estimate reveals apparent anomalies in the allocation of costs to Option 1

134. Option 1 expenditure is reported by Ausgrid as being directed to four areas across ten projects:[56]

- Replacement, 'uplifts', and upgrades of systems/applications (SaaS or IaaS opex) – seven projects:
  - the costs of four of the projects are attributed to licence charges,[57] however the majority of the expenditure is for direct labour and contract services
  - justification for the upgrades under Option 1 is not apparent given that (i) it is positioned as an investment deferral option; and (ii) XaaS subscription costs typically include application refreshes;
- Cyber security compliance:
  - this is the largest Option 1 expenditure item at $8.1m (50% non-recurrent capex and 50% non-recurrent opex)
  - the purpose of this project is not clear given that Ausgrid is (or will be by the end of FY24) fully compliant with all existing obligations
    - if it is a provision for the introduction of AESCSF V2, then we do not consider it appropriate to include the cost forecast in Option 1;
- Vulnerability management – described as being for licensing charges for new 'discovery modules to address new technologies':
  - again, this project does not appear to align with the Option 1 precept
  - the majority of the expenditure is for direct labour and contracted services; and
- New ongoing opex (aka opex step change):
  - linked to five of the ten Option 1 projects, with $7.6m of the $9.4m Option 1 component of the opex step change attributed to the 'Security operations center (SOC) Tools & Capability automation & uplift' project

[56] Ausgrid – IR011 – Cyber projects, objectives and details – 20230428 – Confidential

[57] Data security uplift, IAM replacement & upgrades, SOC tools and capability automation and uplift, Vulnerability management, Web security replacement

- this project and indeed all opex step changes linked to Option 1 appear to be inconsistent with the Option 1 precept.

135. In summary, the projects allocated to Option 1 appear to include at least some that do not align with the precepts of Option 1, the project costs appear high, and are not adequately justified.

Option 1 is rejected by Ausgrid because it does not meet Ausgrid's risk management objectives

136. Ausgrid states that:[58]

> *'Maintaining current minimum compliance and maturity level SP-1 comes at considerable risk. Failure to maintain current functionality and a minimum capability to adequately address cyber security risks would result in an unacceptable level of risk to our network operations, staff, customers, and the community more broadly. Option 1 is unlikely to be the prudent option.'*

Ausgrid's cost-benefit analysis results in a negative NPV

137. Ausgrid states in its Cyber Security Program document that it has not identified any quantified benefits from Option 1, with the NPV of -$72m comprising of the forecast costs to be incurred.[59]

138. In its CBA model the net present cost (NPC) comprises $22.8m PV of costs and $49.1m PV of Efficiency Benefits Sharing Scheme (EBSS) dis-benefits determined over the 13 year study period. Ongoing opex of $2.1m p.a. from FY30 to FY37 is the major contributor to the EBSS dis-benefit.[60]

139. As discussed above, we consider the costs forecast by Ausgrid for Option 1 to be excessive and therefore that the NPC is overstated.

Option 1 is not the prudent selection given the increasing cyber risk profile over the next RCP

140. Whilst we consider that Ausgrid (i) has overstated its inherent and residual risk under Option 1, and (ii) has not provided sufficient information to substantiate what we consider to be excessively high Option 1 costs, we also consider that Ausgrid should invest to at least maintain its risk profile in the face of rising risk.

141. On this basis we do not consider Option 1 to be the prudent selection.

4.5.3 Option 2 – Enhanced cyber security maturity level

142. Option 2 is described by Ausgrid as its Base Case and is designed to achieve SP-2. Ausgrid notes that SP-2 is designed for moderate-criticality organisations and includes 112 additional practices on top of the 88 practices from SP-1.

Ausgrid rejects Option 2 because it considers that SP-2 will maintain its cyber risk level at 'High' and that it has an obligation to achieve SP-3

143. Ausgrid states that:[61]

> *'Ausgrid considered SP-2 as a viable target state for Cyber Security capability. While SP-2 is an appropriate level of Cyber Security capability that is commensurate to Ausgrid's risk appetite and the level of Cyber threat exposed to Ausgrid, this option was not*

58 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 20

59 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 22

60 Ausgrid – Att.5.9.i – Cyber security CBA model – 31 Jan 2023 - Public

61 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 22

preferred due to expected material residual risk and the level of cyber threat exposed to Ausgrid by 2029.'

SP-2 is an appropriate target state by 2024, however the material risks exposed to Ausgrid and the level of Cyber threat increases the likelihood of a Cyber incident occurring that will ***require*** *SP-3 capability to counter anticipated cyber threats by 2029.' [emphasis added]*

144. From the quote above, Ausgrid essentially states that a residual risk of 'High' after implementing and sustaining SP-2 practices (per Table 4.1) is acceptable. However, Ausgrid also states that the residual risk of 'High' (Likely/Major) is 'Not Within Appetite' (refer to Figure 4.3). This contradiction is not resolved.[62]

145. Also, Ausgrid's opinion is that it is *required* by the AESCSF to achieve SP-3[63] (which, from its assessment, will reduce the residual cyber risk to 'Medium', as discussed in section 4.5.4), which is another reason Ausgrid rejects Option 2.

146. As we discuss in section 4.3, we do not consider that Ausgrid's interpretation of the AESCSF in this regard is valid.

Option 2 is estimated to cost $84.8m which appears to be very high for moving from Ausgrid's likely maturity level at the end of the current RCP to SP-2

147. Option 2 builds off the costs included in Option 1, adding 22 new projects to the ten Option 1 projects. The incremental cost from moving from its FY24 projected maturity level of what we refer to as 'SP-1 Plus' to SP-2 is $50.8m, including $19.3m ongoing new opex (i.e. opex step change, an increase of $10.3m from Option 1).[64]

148. The incremental opex step change is primarily for licencing charges associated with ten of the 22 SP-2 projects.

149. Based on our experience and benchmarking, the cost of Ausgrid's Option 2 appears to be excessive. Even the incremental 'project investment' of $47.8m is far in excess of Ausgrid's peers' forecasts for improve from SP-1 or SP-1 Plus to SP-2. We discuss this further in section 4.5.4, in which we summarise a cost benchmarking study with Ausgrid's peers.

Given Ausgrid's services include the Sydney CBD and many other significant customers we consider SP-2 may not be adequate by the end of the next RCP

150. Whilst we have concerns with Ausgrid's risk analysis, when we take into account the *guidance* from the AESCSF regarding High criticality organisations (i.e. SP-3 is recommended) and Ausgrid's service area profile, we consider that SP-2 is likely not to be the prudent level to appropriately mitigate Ausgrid's cyber risks.

4.5.4 Option 3

151. Option 3 is to achieve SP-3 by the end of the next RCP, building on achievement of SP-2 by the end of FY25 at a cost of $111.7m, including $20.6m ongoing new opex (i.e. opex step change). The incremental cost of Option 3 compared to Option 2 is $26.9m including an incremental $1.5m opex step change.

Ausgrid's case for achieving full implementation of SP-3 is not compelling

152. In summary, Ausgrid bases its case for improving its cyber security risk profile from 'High' in FY24 to 'Medium' on the following: [65]

---

62 We also note that the commentary in Table 19 (Option 2) in the column 'Nature of Mitigation' is a copy of the equivalent column in Table 18 (Option 1) and is therefore an error

63 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 22

64 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, Tables 6 and 7

65 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 26

- SP-3 is designed for high-criticality organisations under the AESCSF;
- [redacted]
- It expects its obligations to expand [over the course of the next RCP]; and
- A residual risk appetite of 'High' (as it has assessed Option 2) does not align with its corporate risk appetite – a 'Medium' risk is acceptable to Ausgrid's Board for cyber risk management.

153. We have already discussed why we consider that the AESCSF guidance does not constitute an obligation to fully implement SP-3.

154. Ausgrid's second point is at odds with its advice that it is fully compliant with its cyber security obligations. Furthermore, the ECSO are enacted by the SOCI Act amendments (2 April 2022) and based on our experience, achievement of all four obligations does not require fully implemented SP-3 practices.

155. The possibility of future obligations arising should not be taken into account in expenditure forecasts for regulatory resets – rather if new obligations arise, NSPs have recourse to the AER for additional costs. However, it is likely that the AESCSF will expand to include more practices to achieve SP-3, so we consider that it is reasonable for Ausgrid to take this into account in its expenditure forecast.

156. Finally, whilst we consider that it is likely to be prudent for Ausgrid to invest to achieve more than SP-2 level of cyber maturity, it does not have an obligation to do so. Therefore, it must demonstrate that improving its cyber security risk level to 'Medium' generates a net benefit. We discuss this aspect of Ausgrid's proposal in our assessment of Ausgrid's cost-benefit analysis in section 4.5.5.

A reasonable target for Ausgrid should be less than fully implemented SP-3

157. As shown in our assessment of Ausgrid's quantified risk analysis summarised in Table 4.3, we consider that the avoided probabilistic risk cost of moving from its projected cyber maturity level at the end of the current RCP to fully implemented SP-3 is much less than Ausgrid's estimate of $307m. Our estimate of around $60m ±20% for the 'avoided risk' would suggest to us that, indicatively, the cost of Ausgrid's program should not be more than this amount, or $72m as a maximum amount that could conceivably represent a prudent level of expenditure.

158. To help reduce the cost impost that an allowance based on fully-implemented SP-3 requires, we propose that Ausgrid's allowance is based on a risk-prioritised approach for implementing SP-3 practices, investing only in (i) completing and sustaining the SP-2 practices, and (ii) achieving and sustaining largely-implemented or fully-implemented SP-3 practices that provide significant risk reduction. We consider that a risk-prioritised approach is a prudent compromise between SP-2 and SP-3 levels of risk, cognisant of the criticality of Ausgrid's network and the NER capex and opex criteria.

159. To test the reasonableness of the cost estimate, we undertook a cost benchmarking analysis, which we discuss in section 4.5.6.

4.5.5 Ausgrid's cost-benefit analysis

Ausgrid derives a positive NPV of $126.1m for Option 3

160. Ausgrid did not provide a cost-benefit model to support the NPV analysis it presents for each of its three options, however it describes its approach, and the results. For Option 3, Ausgrid claims a NPV of $126.1m, with probabilistic benefits of $325.9m offset by $199.7m of costs.[66] The annual benefit is derived from Ausgrid's estimate of the reduction in probabilistic risk-cost from fully implementing SP-3 practices.

[66] Ausgrid - Att. 5.9.c - Cyber security program - 31 Jan 2023 – Confidential, Figure 8

Based on our evaluation of the avoided risk-cost, the NPV will be negative unless the cost is significantly reduced

161. As discussed in sections 4.2 and 4.5.4, we consider a more reasonable estimate of the avoided risk-cost (i.e. the benefit from Option 3) to be less than about $60m over the next five years, noting that a moderate risk-cost will remain after implementation of the remaining SP-2 and more SP-3 practices. We have not undertaken our own NPV analysis, however with Ausgrid's proposed cost of $111.7m over the next five years (which we consider to be excessive) it is unlikely that the NPV will be positive without a significant cost reduction.

162. We consider Ausgrid's proposed costs further in the following section.

4.5.6 EMCa's cost benchmark analysis

Objective of benchmark cost analysis

163. In accordance with our scope, we are required to provide an alternative cost estimate if we consider that the proposed cost is not reasonable.

164. Our opportunity for engagement with Ausgrid in this review was limited due to lengthy delays while confidentiality considerations were addressed between AER and Ausgrid. We have not had the opportunity to engage with Ausgrid on its cost estimate to a level where we could provide a bottom-up alternative assessment by considering alternative parameters in Ausgrid's own costing. However, we have had access to alternative cost estimate information provided by other DNSPs and this has facilitated a 'benchmarking' approach which we describe in the current section, and which we consider provides a reasonable basis for the alternative estimate that we propose in section 4.6.2.

Definitions

165. In this section we have used benchmark information from Ausgrid's peers to construct what we consider to be a reasonable cost estimate for Ausgrid to improve its cyber maturity level from 'SP-1 Plus' to 'SP-3 Minus'. In our analysis, reference to SP-X Plus or Minus should be interpreted as follows:

- SP-X Plus infers that more than 100% SP-X practices are in place, but less than 50% of the higher maturity practices, for example,
  - SP-2 Plus infers that (i) all of the 88 SP-1 practices and all of the 112 SP-2 practices under the AESCSF have been implemented and resources are established to sustain them and (ii) up to about 50% of the 82 SP-3 practices and anti-patterns are implemented; and
- SP-X Minus infers more than 50% of the SP-X practices are in place, but not 100%, for example,
  - SP-3 Minus infers that more than 50% of the 82 SP-3 practices are largely implemented (as opposed to fully implemented).

166. In both instances above, we also assume a risk-based prioritisation approach; therefore, it can be assumed that implementing 50% of practices for a given SP level would require less than 50% of the cost of fully implementing that practice.

167. SP-3 Minus (with a focus on implementing the highest impact practices) is what we recommend for Ausgrid, and which therefore is a relevant benchmark in our analysis.

Assessment

Size of Ausgrid's cyber security team is much larger than required

168. In response to an Information Request in which we asked for the current and proposed size of its cyber security resources, Ausgrid provided its 'cyber operating model.'[67] It comprises

[67] Ausgrid – IR011 – Operating model – 20230428 – Confidential

of 26 FTEs, with 18 opex positions and 8 'investment positions'. In addition, Ausgrid's model identifies external resources for:

- Phishing simulations, penetration testing, incident response, threat intelligence, and end-user computing and mobile security; and
- Managed services – end user computing, infrastructure management and application and cloud management.

169. A hybrid model[68] for implementing and sustaining robust cyber security measures is a strategy common within the industry. Similarly, hosted services are now commonplace.

170. It is not clear from Ausgrid's operating model diagram nor from Ausgrid's response to our question asking it to identify the current and proposed cyber security team structure [69] whether the team is or will be fully implemented by the start of the next RCP.

171. If new staff were being added in the next RCP, we would expect the ongoing cost to be included as part of the claimed opex step change. However, in its descriptions of the opex step changes,[70] there is no indication from Ausgrid that it is adding cyber security staff. For example, references to enhancements to the Security Operations Centre (SOC) attribute opex 'uplifts' to:

- 'Managed services for independent attack management assessment and control tools, together with Purple team exercises held yearly
  - noting that managed services are provided by external partners (as shown in the operating model diagram); and
- 'Licensing for SIEM Monitoring & Logging and SOC Case Management tools. Managed services for 24x7 eyes-on-glass security monitoring'

172. So whilst the operating model diagram includes four FTEs in the SOC, we assume that these FTEs are already in their roles or will be by the start of the next RCP.

173. Based on our experience and noting the size of the cyber security teams in other NSPs we have recently reviewed for the AER, we consider that an optimal team size is likely to be in the range of 12-15 FTEs, depending on the starting point maturity level and the organisation's investment program (i.e. target maturity level). In our opinion, when fully established, Ausgrid's planned cyber security team appears to have about ten FTEs more than is an efficient level. At an assumed average annual cost of $200k/FTE, this creates a substantial additional cost above what we consider to be an efficient level. We have taken this into account in our benchmarking analysis.

No cyber security project recurrent opex is included in the Base Year

174. Although Ausgrid has an established cyber security program, $0.0m SCS cyber security recurrent project opex is recognised in its Base Year.[71]

175. In response to a subsequent Information Request in which we asked Ausgrid to provide the annual cyber security capex and opex from FY20 to FY29, it provided a spreadsheet from which we have derived the following graph.

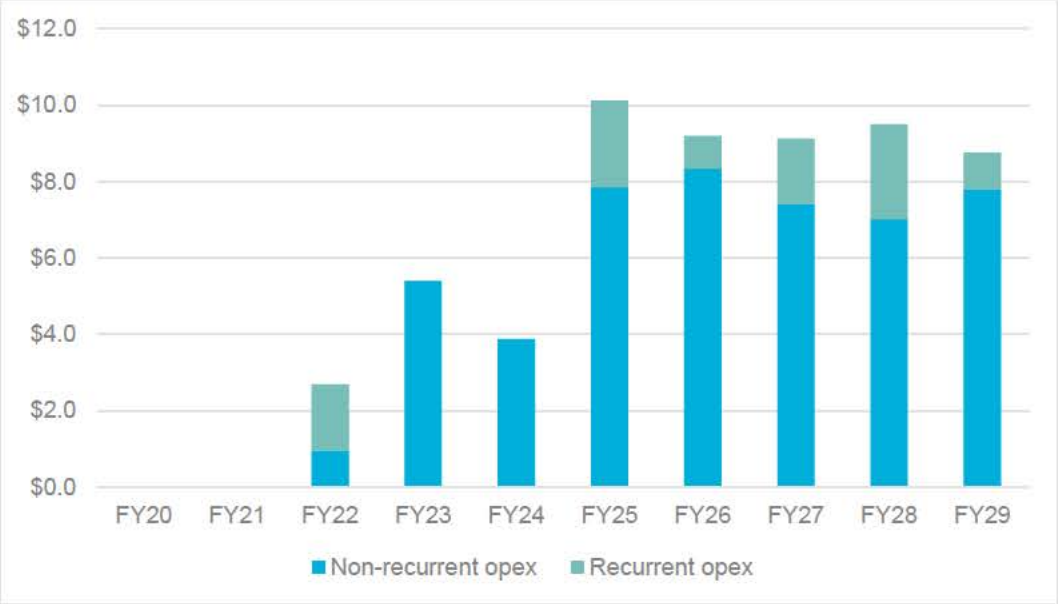
68 A mixture of internal and external resources

69 Ausgrid - IR011 (Part 2) - Cyber Security Proposal - 20230414 – Confidential, response to question 6

70 Ausgrid – IR011 – Cyber projects, objectives and details – 20230428 – Confidential, Cyber projects tab

71 Ausgrid - Att. 6.1.b - Step changes model - 31 Jan 2023 - Public

Figure 4.7: Ausgrid actual and forecast 'cyber security project investment opex' ($m, real 2024)



Source: EMCa analysis of IR011 Ausgrid – 1.b. Cyber Expenditure – 20230414 - Public

176. This aligns with Ausgrid's step change calculation in its Step changes model[72] which states that it incurred no cyber security recurrent opex in the Base Year. We note that:

- Ausgrid qualifies the opex in the 'chart' (which we assume refers to the table provided) as being for SaaS configuration costs only and does not include 'business as usual' non-recurrent opex;
- The numbers in the spreadsheet provided are hard-coded;
- Opex in the Base Year is classified as 100% non-recurrent, which is compatible with a project-driven investment;
- $1.7m recurrent 'project opex' was incurred in FY22, but none is forecast for FY23 and FY24;
- The forecast cyber security 'project investment' opex of $46.7m for the next RCP[73] reconciles exactly with the 'investment opex in the bottom-up cost estimate shown in another spreadsheet provided by Ausgrid.[74]

177. We would expect Base Year opex to include recurrent expenditure on the cyber security team, licence fees for applications/systems, and managed services. However, due to our limited opportunity for engagement with Ausgrid, we were not able to explore the reasons for the absence of such costs prior to finalising this report.

178. Ausgrid states that its proposed opex step change is 'driven by the need for resources with specialist skills, further protection through new cyber software capability, and investing in evolving cyber awareness training programs for staff to protect themselves and the organisation from cyber-attacks.'[75]

179. Whilst these are common cyber security related investments, it is difficult to understand from the information provided in the RP why Ausgrid showed no cyber security opex in the Base Year (2023).

72 Ausgrid - Att. 6.1.b - Step changes model - 31 Jan 2023 - Public

73 IR011 Ausgrid – 1.b. Cyber Expenditure – 20230414 - Public

74 Ausgrid – IR011 – Cyber projects, objectives and details – 20230428 – Confidential

75 Ausgrid- Att. 5.9.c -Cyber security program – 31 Jan 2023, page 26

We have applied other benchmark information from Ausgrid's peers to test the reasonableness of Ausgrid's cost build-up

180. We have recently completed reviews of three DNSPs' proposed cyber security expenditure. As a result, we have insight into recent proposed costs for:

- Sustaining the current level of cyber security;
- Moving from SP-1 to SP-2;
- Moving from SP-1 Plus to SP-2;
- Moving from SP-1 to SP-3; and
- Moving from SP-2 and SP-2 Plus to SP-3 and SP-3 Minus.

181. We benchmarked costs using four methodologies, summarised in the table below.

Table 4.4: EMCa cyber security cost benchmarking study - summary

Method Description	Cost estimate ($m)	Comments
1. Peer cost for SP-2 Minus to SP-3	73.0	*We recommend that Ausgrid does not extend to SP-3 so this would be on the high side*
2. Peer cost for SP-1 to SP-2 Plus *Less 20% as Ausgrid is at SP-2 Minus* *Add peer cost for SP-2 Plus to SP-3 Minus*	67.2	*20% is based on an EMCa estimate of costs avoided by Ausgrid as it will already be at SP-2 Minus*
3. Ausgrid cost for SP-1 Plus to SP-3 *Less excess Ausgrid team cost* *Less peer cost SP-2 to SP-3 Minus*	67.1	*EMCa estimate of Ausgrid team excess cost of $10m over five years*
4. Peer cost SP-1 Plus to SP-3 *Less excess Ausgrid team cost* *Less excess Ausgrid SP-1 Plus to SP-2* *Less excess Ausgrid SP-2 Plus to SP-3*	74.1	*Deductions based on EMCa experience and peer analysis*
Average benchmarked cost for Ausgrid to achieve SP-3 Minus*	**70.3**	*±20% (approximately $55m to $85m)*

Source: EMCa analysis; all costs are assumed to include opex step change provisions
** EMCa's proposed target level for Ausgrid by the end of the next RCP*

182. We observe the following from the benchmarking exercise with some of Ausgrid's peers:[76]

- We have based the cost benchmark for Ausgrid on a target that we assume to be SP-3 Minus, not fully-implemented SP-3;
- The benchmarking exercise is an approximation, so averages have been used to reduce the reliance on a single benchmark;
  - at approximately $70.3m ±20%, the result is about $41.5m or 37% less than Ausgrid's proposed expenditure;
- Ausgrid's estimated $34.1m to sustain what we have denoted as SP-2 Minus is more than ten times another NSP's estimate[77]
  - This is a key factor in our consideration that Ausgrid requires significantly less than it has proposed;

[76] Costs include ongoing opex (i.e. proposed opex step change)

[77] The peer NSP's cyber maturity level appears to be approximately the same as Ausgrid's at the commencement of the next RCP (i.e. SP-2 Minus)

- Ausgrid's estimated $50.7m to move from SP-2 Minus to SP-2 (its Option 2) appears to be well above what would be reasonable to implement the 40-60 SP-2 practices required based on our experience and considering Ausgrid's peers' proposals;
  - This is also a significant factor in our consideration that Ausgrid will require less than it has proposed;
- A peer NSP has estimated $73.0m to improve its cyber maturity from SP-2 Minus to SP-3, whereas Ausgrid estimates a similar implementation task to cost $111.7k or 53% more – this does not seem reasonable, even after taking into account the customer base disparity;
- A peer NSP estimates it would need $54m to move from SP-1 Plus maturity to SP3 maturity, which is 48% of Ausgrid's estimate to move from a higher maturity level at the start of the next RCP to SP-3 – again this indicates that Ausgrid's estimate is significantly overstated; and
- In our benchmarking calculations we used costs proposed to AER by the peer organisations. However, from our reviews, our findings are that these proposed amounts are to differing extents also higher than is required. If this was taken into account, then it could be argued that the cost benchmark for Ausgrid should also be lower than the $70.3m shown in Table 4.4.

At $111.7m Ausgrid's cyber security program is not justified as economically prudent

183. Our estimate of a reasonable cost being in the range of approximately $55m to $85m overlaps with our risk-cost estimate of a benefit in the range of $48m-$72m.[78] We consider that Ausgrid's proposed $111.7m cost for fully implemented SP-3 over the next RCP plus ongoing opex of approximately $5.1m p.a. is not economically justified.

184. We consider that, a risk-prioritised cyber program which prioritises essential, high impact SP-3 practices[79] is likely to stabilise / maintain Ausgrid's risk level over the course of the next RCP. From the indicative cost benchmarking information available to us, we consider that a program with a net economic benefit on this basis, is achievable.

4.5.7 Deliverability of Ausgrid's cyber program

We have no significant concerns with Ausgrid's delivery risk

185. Ausgrid presents a summary of its delivery risks in Table 13 of its Cyber security program document. The risk controls are appropriate. Ausgrid's 'Program assumptions' in Section 5.3 of the same document are also reasonable.

4.6 Our findings and implications

4.6.1 Summary of our findings

Ausgrid is likely to face a significant increase in its cyber risk profile over the next RCP

186. Like other NSPs, we are satisfied that Ausgrid is likely to face a material increase in its cyber risk profile during the course of the next RCP in the absence of proactive investment in improving its cyber security maturity. The increased risk is from the combination of:

- A worsening threat landscape; and
- An increasing attack surface.

78 i.e. $60m +/- 20%. Refer to section 4.5.6

79 In addition to completing and sustaining the SP-2 practices

187. As is the case with other DNSPs, it is reasonable to assume that further investment will be required in order to maintain the current risk level, in the face of this increasing threat risk.

Ausgrid proposes to reduce its cyber risk level from 'high' to 'medium' but it has not justified the cost of its proposed approach

188. Ausgrid's cyber security investment strategy is predicated on reducing its cyber security risk level from 'High' to 'Medium' during the next RCP. However, the investment beyond that required to maintain the risk level at High requires economic justification. Ausgrid has not demonstrated that its proposed expenditure is economically justified.

189. We consider that Ausgrid's derivation of its risk cost of $307m over the next RCP is overstated because of its assumptions regarding likelihood and consequence, both of which are biased. Our calculation based on applying what we consider to be more reasonable likelihood and consequence assumptions is an avoided risk-cost of the order of $48m-$72m over this period. This is an estimate of the potential benefit (i.e. avoided cost) from Ausgrid's proposed investment in reducing cyber risk and would tend to suggest an upper limit to economically-justifiable expenditure.

Ausgrid's proposed cyber security cost is too high

190. Our benchmarking analysis combined with our own experience suggests that Ausgrid's proposed $111.7m totex for the next RCP and its ongoing opex is unreasonably high. We consider an amount of at most $70m would represent an efficient level for a business of Ausgrid's criticality, size, and complexity.

191. This is based on our position that Ausgrid should adopt a risk-prioritised approach to designing its cyber security investment program over the next RCP with only the highest impact SP-3 practices implemented, and that the cyber security team it has assumed, is larger than necessary.

4.6.2 Implications of our findings for proposed expenditure

192. We propose an alternative allowance as shown in Table 4.5, with:

- The opex step change derived from the average of three peer organisations;
- The project totex of $52m derived from the benchmark totex of $70m less the benchmarked opex step change;
- The cyber security capex and SaaS opex proportionately adjusted from the ratio of Ausgrid's project totex forecast of $91.1m and our proposed adjusted project totex of $52m; and
- Proposed allowances rounded from the adjusted costs, cognisant that the derived numbers are based on a series of assumptions.

193. The adjusted costs are derived from analysis that we described in section 4.5.6.

Table 4.5: EMCa proposed adjustment to Ausgrid's cyber security SCS totex ($m, real 2024)

Cost component	Ausgrid proposed	EMCa adjusted costs	EMCa recommended adjusted allowance
Cyber security capex	44.40	25.4	25.00
Cyber security SaaS opex	46.70	26.7	27.00
Project totex	**91.10**	**52.1**	**52.00**
Opex step change	20.60	18.3	18.00
Totex	**111.70**	**70.3**	**70 ± 20%**

Source: EMCa analysis

194. We consider that Ausgrid's proposed expenditure of $111.7m is $41.7m higher than what we consider to be a reasonable estimate of the efficient cost.

195. The annual adjustments are shown in the table below.

Table 4.6: EMCa proposed adjustment to Ausgrid's proposed cyber security expenditure in the next RCP ($m real 2024)

	2025	2026	2027	2028	2029	Total
Non-recurrent ICT – cyber security capex*	9.0	9.0	9.0	8.0	9.0	44.0
Less EMCa adjustment	*-3.9*	*-3.9*	*-3.9*	*-3.5*	*-3.9*	*-19.0*
EMCa adjusted cyber security capex	**5.1**	**5.1**	**5.1**	**4.5**	**5.1**	**25.0**
Non-recurrent SaaS opex*	10.0	9.0	9.0	10.0	9.0	47.0
Less EMCa adjustment	*-4.3*	*-3.8*	*-3.8*	*-4.3*	*-3.8*	*-20.0*
EMCa adjusted SaaS opex	**5.7**	**5.2**	**5.2**	**5.7**	**5.2**	**27.0**
Opex step change – ICT cyber security*	2.4	4.0	4.4	4.7	5.1	20.6
Less EMCa adjustment	*-0.3*	*-0.5*	*-0.6*	*-0.6*	*-0.6*	*-2.6*
EMCa adjusted Opex step change	**2.1**	**3.5**	**3.8**	**4.1**	**4.5**	**18.0**
Ausgrid proposed cyber security totex	21.4	22.0	22.4	22.7	23.1	**111.7**
EMCa adjusted cyber security totex	**13.0**	**13.8**	**14.1**	**14.4**	**14.7**	**70.0**

**Source: Ausgrid RP document, Figure 5.9.2 and Opex model (Attachment 6.1.b)*