

**EMC<sup>a</sup>**

energy market consulting associates

Energex and Ergon Energy 2025/26 to 2029/30 Regulatory  
Proposals

# **REVIEW OF CYBER SECURITY EXPENDITURE FORECAST**

Public Version



Report prepared for:  
**AUSTRALIAN ENERGY  
REGULATOR**  
August 2024

## **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 Ergon Energy and Energex, which are owned and managed by Energy Queensland Ltd (EQL or EQ) from 1st July 2025 to 30th June 2030. 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 EQ. 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 overarching purpose.*

*Except where specifically noted, this report was prepared based on information provided to us prior to 21 June 2024 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 EQ regulatory submissions or other documents due to rounding.*

Enquiries about this report should be directed to:

### **Paul Sell**

Managing Director  


### **Prepared by**

Mark de Laeter with input from Cesare Tizi, Scott Wallace and Paul Sell

### **Date saved**

12/09/2024 7:12 PM

### **Version**

Final v1

## **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  
contact@emca.com.au  
www.emca.com.au

### **Perth Office**

contact@emca.com.au  
www.emca.com.au

## TABLE OF CONTENTS

<b>ABBREVIATIONS</b> .....	<b>III</b>
<b>EXECUTIVE SUMMARY</b> .....	<b>V</b>
<b>1 INTRODUCTION</b> .....	<b>1</b>
1.1 Purpose of this report.....	1
1.2 Scope of requested work.....	1
1.3 Our review approach .....	2
1.4 This report.....	2
<b>2 RELEVANT CONTEXT TO OUR ASSESSMENT – CYBER SECURITY</b> .....	<b>4</b>
2.1 Cyber security threat in Australia .....	4
2.2 Critical infrastructure - changes to regulation.....	4
2.3 The Australian Energy Sector Cyber Security Framework (AESCSF) .....	6
2.4 AER Guidelines for non-network ICT assessment.....	8
2.5 Implications for our assessment.....	9
<b>3 EQ’S PROPOSED CYBER SECURITY EXPENDITURE</b> .....	<b>10</b>
3.1 Overview and summary of proposed expenditure.....	10
3.1 Summary of the basis for EQ’s proposed expenditure.....	12
<b>4 OUR ASSESSMENT</b> .....	<b>15</b>
4.1 EQ’s current state .....	15
4.2 EQ’s risk analysis .....	16
4.3 EQ’s options analysis .....	18
4.4 EQ’s cost forecasting methodology .....	22
4.5 EQ’s economic assessment.....	25
4.6 Top-down benchmarking.....	27
4.7 Our findings and implications .....	28

### LIST OF TABLES

Table 2.1: AESCSF Version 1 and Version 2 comparison – Security Profiles .....	7
Table 3.1: EQ’s SCS cyber security ‘uplift’ capex, \$m, FY25 (excluding capitalised overheads) .....	11
Table 4.1: Total cyber security cost breakdown for each option (\$m, real Dec 2022) .....	20
Table 4.2: EQ representation of its CBA for cyber security (\$m, 2022).....	26
Table 4.3: EQ vs combined Ausgrid and Essential Energy benchmark (\$2024).....	28

## LIST OF FIGURES

Figure 1.1: Scope of work covered by this report.....	1
Figure 2.1: AESCSF E-CAT criticality bands for electricity sector – DNSPs highlighted.....	7
Figure 3.1: EQ cyber security expenditure – actuals and forecast (\$m, 2022).....	12
Figure 3.2: Current state assessment – SoCI Act obligations pertaining to cyber security .....	13
Figure 3.3: Current state assessment – non-SOCI Act obligations pertaining to cyber security .....	14
Figure 4.1: EQ risk reduction assessment from investments in the current RCP .....	17
Figure 4.2: Structure of EQ’s cyber security options considered .....	19
Figure 4.3: EQ’s assessment of inherent and residual cyber risk for Option 3.....	22
Figure 4.4: EQ’s cost estimates for the six initiatives for the Capability Uplift preferred option (\$m, 2022) .....	22
Figure 4.5: EQ’s cost estimation principles.....	24

## ABBREVIATIONS

ACSC	Australian Cyber Security Centre
AEMO	Australian Energy Market Commission
AER	Australian Energy Regulator
AESCSF	Australian Energy Sector Cyber Security Framework
ASD	Australian Signals Directorate
BC	Business case
CBA	Cost Benefit Analysis
CIRMP	Critical Infrastructure Risk Management Plan
CUP	Capability Uplift Program
Current RCP	2025-30 regulatory control period
DNSP	Distribution Network Service Provider
E-CAT	Electricity sector criticality assessment tool
ECISO	Enhanced cyber security obligations
EEMM	Essential Eight Maturity Model
EQ	Energy Queensland
IFRS	International Financial Reporting Standards
IT/ICT	Information technology / Information and Communications Technology
MIL	Maturity Indicator Level
MIL-1	Meeting Maturity Indicator Level One
NER	National Electricity Rules
Next RCP	2025-30 regulatory control period
NPV	Net Present Value
NSP	Network Service Provider
OT	Operational Technology
P1, P2, P3, P4	Severity ratings with P1 being the highest (i.e. Priority 1)
QA	Quality Assurance
RCP	Regulatory Control Period
RP	Regulatory Proposal
RRP	Revised Regulatory Proposal
SCS	Standard Control Services
SLACI Act	Security Legislation Amendment (Critical Infrastructure) Act 2021
SLACIP Act	Security Legislation Amendment (Critical Infrastructure Protection) Act 2022

SOCI Act	Security of Critical Infrastructure Act 2018
SoNS	System of National Significance
SP	Security Profile



# EXECUTIVE SUMMARY

## Introduction and context

1. The AER has engaged EMCa to undertake a technical review of aspects of the expenditure that Ergon Energy (Ergon) and Energex have proposed in their regulatory proposals (RPs) for 2025-30 Regulatory Control Period (next RCP). The scope of our review, covered by this report, comprises the proposed capital expenditure for their cyber security capability uplift programs for the next RCP. Neither Energex nor Ergon have requested an operational expenditure step change for any aspects of their 2025-30 cyber security programs.
2. The assessment contained in this report is intended to assist the AER in its own analysis of the proposed capex allowance as an input to its draft determination on EQ's revenue requirements for the next RCP.

## Our assessment

### EQ documentation

**Energex and Ergon have presented nearly identical sets of documents in support of their respective proposals for cyber security expenditure**

3. Energex and Ergon have both provided nearly identical business cases and cost-benefit models in support of their respective shares of the proposed total \$100.7 million capex for the next RCP. This compares to a combined \$57.1 million capex in the current RCP. The capex allocation for the next RCP is \$48.4 million to Energex with the balance of \$52.3 million allocated to Ergon for a set of identical initiatives to be managed by a 'central' cyber security team.
4. We refer in this Executive Summary and in the majority of our report to 'Energy Queensland's (EQ) cyber security proposal and proposed expenditure, because it is only in apportioning to the two DNSPs under EQ that a distinction is made.
5. The investment in increasing EQ's cyber security capability program is based on improving existing controls and practices and adding new controls to offset the risk of cyber security breach from an expected increased cyber security threat landscape and EQ's increasing attack surface area.
6. The proposed cyber security capex for the next RCP is in addition to significant recurrent opex, primarily to support current operations, and non-recurrent opex that Energy Queensland will incur in implementing the new initiatives. However, EQ has not sought opex step changes for cyber security and accordingly, we have not been asked to review this.

### Demonstrating investment need and option selection

**EQ presents a compelling case for increased investment to offset the escalating cyber security threat landscape**

7. EQ has identified its regulatory compliance obligations and has presented its analysis of the current and future threat landscape, referencing available literature. The external analysis draws on recognised industry sources, which point to a relentless increase in cyber threats from increasingly sophisticated actors. EQ does not proffer evidence of escalating cyber security attack threat events affecting its business.

### EQ's strategy to manage cyber security risk escalation is to take a risk-based approach using targeted controls to uplift its capability

8. EQ references the superseded version of the Australian Energy Sector Cyber Security Framework (AESCSF), but it does not target a particular Security Profile (SP) under that framework. Rather, EQ proposes to continue to meet its existing cyber security obligations through its 'maintain operations' program and to take a risk-based approach to mitigating the increasing cyber threat through its 'uplift' program.
9. EQ has identified six sources of cyber security risk, with three of these rated as exposing EQ to █████ level of risk at the commencement of the next RCP (i.e. 2025). If there is no further investment in capability uplift, EQ forecasts a █████ level of cyber security risk by the end of the next RCP (i.e. 2030). EQ's target cyber risk level in 2030 is no higher than █████. Whilst we consider this to be a reasonable target, we consider that EQ may have under-estimated its projected overall inherent risk level in 2025 and its risk level by 2030 absent uplift. We have formed this view by comparing EQ's expected risk maturity level and █████ risk rating with ratings undertaken by its peers.
10. EQ has identified six initiatives and multiple projects within each initiative to address the gaps exposed within the six core risk areas. We have considered the justification for the investment in controls beyond EQ's compliance requirements. EQ has demonstrated to our satisfaction that the proposed additional controls are warranted and represent a prudent approach to mitigate increasing cyber security risk.

### EQ has selected a prudent option

11. EQ provided sufficient detail to support its proposed option, including the proposed breadth and depth of controls. However, its cost-benefit analysis is not compelling as presented. On the one hand, we are of the view that it has over-estimated the likelihood of major cyber breaches, but we also have identified risk-costs that it has failed to take into account and it has unnecessarily curtailed its study period at 5 years. In the course of our assessment, EQ replaced its CBA with an update that reduced the NPV of its preferred option from █████ million to █████ million (\$2022). In its updated CBA, the NPV ranking of the options was also reversed, with a higher-cost option showing a higher NPV than EQ's preferred option, though this appeared to result from an erroneous calculation in EQ's CBA modelling and, without acknowledging the implication of this result, EQ continued to propose the same 'preferred' option as previously.
12. On balance, we consider that EQ's CBA appropriately ascribes a positive NPV to its proposed option, though it likely underestimates this. Because EQ's updated CBA does not present a higher NPV for the preferred option, EQ has not evidenced application of the claimed risk-cost approach. However, we consider that its preferred approach is nevertheless the prudent option for the following reasons:
  - We consider that the controls that EQ has chosen and prioritised, are appropriate, and
  - We consider that EQ's presentation of an alternative option with a higher NPV (in its updated CBA) likely results from a calculation error which would, if corrected, revert the preferred option to a higher CBA ranking.
13. We conclude that EQ's proposed 'Uplift' capex is likely to satisfy the NER capex criteria.

## Demonstrating reasonableness of proposed cost

### EQ's cost forecasting methodology is sound

14. EQ's approach of identifying gaps and controls to manage the exposures throughout the course of the next RCP, and costing the controls via a combination of vendor input and external advice to supplement its in-house expertise is a sound approach. We consider that this approach will have resulted in a realistic cost estimate for the controls that it proposes to implement.



### A top-down benchmark provides a reasonable cross-check on EQ's proposed expenditure

15. Given the substantial differences between EQ's presentation of its cyber security risk levels, and issues described above with its CBA, we sought to cross-check its proposed aggregate expenditure by comparison with peers.
16. We identified that Ausgrid and Essential Energy together provide a broadly similar point of comparison, with broadly similar customer numbers and a broadly similar combined urban and regional customer base. We find that EQ cyber security expenditure over the next period (combining ongoing and uplift) is similar to the AER's combined allowance for 2024-29 for Ausgrid and Essential Energy, when we compare totex/user and totex/device. While this comparison is not definitive, and is not directly derived from EQ's proposal, we consider that it provides further validation that the proposed expenditure is within a reasonable range.

## Implications of our findings

17. EQ proposes \$48.4 million capex for Energex's cyber security uplift program and \$52.3 million capex for Ergon's cyber security uplift program. We consider that EQ's proposed capital expenditure is reasonable.

# 1 INTRODUCTION

The AER has asked us to review and provide advice on Energex and Ergon Energy's (Ergon) proposed allowances over the next Regulatory Control Period (next RCP) relating to cyber security. Our review is based on information that Energex and Ergon provided and on aspects of the National Electricity Rules (NER) relevant to assessment of expenditure allowances.

## 1.1 Purpose of this report

18. The purpose of this report is to provide the AER with a technical review of aspects of the expenditure that Energex and Ergon have proposed in their respective revenue proposals (RP) for the 2025-30 Regulatory Control Period (next RCP).
19. The assessment contained in this report is intended to assist the AER in its own analysis of the proposed capex and opex allowances as an input to its Draft Determination on Energex and Ergon revenue requirements for the next RCP.
20. Energex and Ergon have a common cyber security strategy, under the structure of parent company Energy Queensland (EQ). For this report, we will refer to 'EQ' rather than 'Energex and Ergon' when referring to the common cyber security strategy or other common elements of cyber security plans.

## 1.2 Scope of requested work

21. Our scope of work, covered by this report, is as defined by the AER. Relevant aspects of this are as summarised in Figure 1.1.

Figure 1.1: Scope of work covered by this report

**Scope of work covered by this report.**

The scope of this review, as requested by the AER, covers the following.

Capex (ex ante)

- Cyber security (ICT)
- Cyber Security (OT)

The scope includes the following specific requirements.

*In assessing expenditure to address cyber security risk, have regard to the Security Legislation Amendment (Critical Infrastructure Protection) Act 2022 which amended the Security of Critical Infrastructure Act 2018 to establish a regime for enhanced cyber security obligations to be applied to Systems of National Significance.*

## 1.3 Our review approach

### 1.3.1 Approach overview

22. In conducting this review, we first reviewed the RP documents that EQ has submitted to the AER. This includes a range of appendices and attachments to EQ's RP and certain Excel models which are relevant to our scope.
23. We next collated some information requests. The AER combined these with information request topics from its own review and sent these to EQ.
24. In conjunction with AER staff, our review team met with EQ at its offices on 13-15 May 2024. EQ presented to our team on the scoped topics and we had the opportunity to engage with EQ to consolidate our understanding of its proposal.
25. EQ provided the AER with responses to information requests and, where they added relevant information, these responses are referenced within this review.
26. We have subjected the findings presented in this report to our peer review and Quality Assurance (QA) processes and we presented summaries of our findings to the AER prior to finalising this report.
27. The limited nature of our review does not extend to advising on all options and alternatives that may be reasonably considered by EQ, or on all parts of the proposed forecast. We have included additional observations in some areas that we trust may assist the AER with its own assessment.

### 1.3.2 Technical review

28. Our assessments comprise a technical review. While we are aware of stakeholder inputs on aspects of what EQ has proposed, our technical assessment framework is based on engineering considerations and economics.
29. We have sought to assess EQ's expenditure proposal based on EQ's analysis and its 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 EQ may subsequently provide additional information or a varied proposal, our assessment may differ from the findings presented in the current report.
30. We have been provided with a range of reports, internal documents, responses to information requests and modelling in support of what EQ 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 EQ's regulatory submission documents as provided on its submission date, as the 'source of record' in respect of what we have assessed.

## 1.4 This report

### 1.4.1 Report structure

31. This report covers our ex ante review of cyber security ICT capex and cyber security operational technology (OT) capex for the next RCP.
32. We have presented:
  - an overview of the proposed expenditure and a summary of EQ's justification for that expenditure;
  - our assessment of the proposed cyber security capex, with observations made regarding proposed opex; and

- our findings and the implications of these findings for the expenditure allowances determined by the AER in its draft regulatory determination.
33. We have taken as read the material and analysis that EQ provided, and we have not sought to replicate this in our report except where we consider it to be directly relevant to our findings.

#### 1.4.2 Information sources

34. We have examined relevant documents that EQ has published and/or provided to the AER in support of the areas of focus and projects that the AER has designated for review. This included further information at onsite meetings and further documents in response to our information requests. These documents are referenced directly where they are relevant to our findings.
35. Except where specifically noted, this report was prepared based on information provided by AER staff prior to 21 June 2024 and any information provided subsequent to this time may not have been taken into account.
36. Unless otherwise stated, documents that we reference in this report are EQ documents comprising its regulatory proposal and including the various appendices and annexures to that proposal.
37. We also reference information responses, using the format IRXX being the reference numbering applied by AER. Noting the wider scope of AER's determination, AER has provided us with IR documents that it considered to be relevant to our review.

#### 1.4.3 Presentation of expenditure amounts

38. Expenditure is presented in this report in \$2025 real terms, unless stated otherwise. In some cases, we have converted to this basis from information provided by the business in other terms.
39. While we have endeavoured 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 – CYBER SECURITY

We have conducted our review of EQ's cyber security 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

Increasing threat level is reported by the ACSC

40. 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 (2022-23) it states that: *'The ACSC responded to over 1,100 cyber security incidents from Australian entities. Separately, nearly 94,000 reports were made to law enforcement through ReportCyber – around one every six minutes.'*<sup>1</sup>

State actors are focussed on critical infrastructure worldwide

41. The Australian Signals Directorate (ASD) states:

*Globally, government and critical infrastructure networks were targeted by state cyber actors as part of ongoing information-gathering campaigns or disruption activities...Cyber operations are increasingly the preferred vector for state actors to conduct espionage and foreign interference.*<sup>2</sup>

42. In September 2022 and May 2022, the ASD and its international partners published advisory notices which strongly encouraged Australian entities to review their networks for signs of malicious activity.

Australian critical infrastructure has been targeted

43. The 2022 Cyber Threat Report also reports that the ADS responded to 143 cyber security incidents related to critical infrastructure. It states that *'activity against these networks is likely to increase as networks grow in size and complexity.'*<sup>3</sup>
44. The annual Cyber Threat Report notes that critical infrastructure can be targeted by the mass scanning of networks for old and new vulnerabilities, citing the example of an Italian energy and water provider that was affected by ransomware.

### 2.2 Critical infrastructure - changes to regulation

#### 2.2.1 Amendments to the SOCI Act

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

---

<sup>1</sup> ASD Cyber Threat Report 2022-23. Executive Summary.

<sup>2</sup> ASD Cyber Threat Report 2022-23. Executive Summary.

<sup>3</sup> ASD Cyber Threat Report 2022-23. Executive Summary.

46. The Security Legislation Amendment (Critical Infrastructure) Act 2021 (SLACI Act) 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.
47. The amendments were made to respond to *'the deteriorating threat environment related to cyber attacks'*.<sup>4</sup> Electricity assets can be classed as critical infrastructure within the framework under the SoCI 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.
48. On 2 April 2022, additional 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 2022<sup>5</sup>
  - 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.<sup>6</sup>
49. The CIRMP is a written program that 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.<sup>7</sup>
50. The ECSO varies 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.<sup>8</sup>

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

51. Under the Security of Critical Infrastructure (Critical infrastructure risk management program) Rules 2022, a responsible entity must establish and maintain a process or system in the CIRMP to (i) comply with a framework contained in one of five documents referred to in the CIRMP, and (ii) meet the corresponding condition for that document.<sup>9</sup> 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.<sup>10</sup>

<sup>4</sup> <https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-soci-obligations.pdf>

<sup>5</sup> <https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-systems-of-national-significance-enhanced-cyber-security-obligations.pdf>

<sup>6</sup> <https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-systems-of-national-significance-enhanced-cyber-security-obligations.pdf>

<sup>7</sup> Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2022 – explanatory statement.

<sup>8</sup> <https://www.cisc.gov.au/resources-subsite/Documents/cisc-factsheet-systems-of-national-significance-enhanced-cyber-security-obligations.pdf>

<sup>9</sup> Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2022; subsection 8 (4).

<sup>10</sup> Federal Register of Legislation, Security of Critical Infrastructure (Critical infrastructure risk management program) Rules (LIN 23/006) 2022; subsection 4(2) and subsection 8(3).



52. The 2020-21 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 Network Service Providers (NSPs) must comply with if the NSP is defined as a responsible entity and selects the AESCSF as the cyber security framework.
53. 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 the NSP selects the EEMM as its cyber security framework.

### 2.2.3 Privacy Act amendments 2022<sup>11</sup>

54. 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.
55. 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 \$2.2m.
56. 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.'<sup>12</sup>

## 2.3 The Australian Energy Sector Cyber Security Framework (AESCSF)

### 2.3.1 AESCSF V1

57. In response to the Finkel National Electricity Market Review recommendation 2.10, in 2018 the Australian Energy Market Operator (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.<sup>13</sup> The AESCSF Version 1 (V1) is divided into 11 domains, ten C2M2<sup>14</sup> 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.<sup>15</sup> AESCSF V1 encompasses the 2018 and subsequent iterations up to and including the 2022 revision.
58. 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.
59. 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 DNSP criticality rating ranging between the High and Medium bands.

<sup>11</sup> [https://www.aph.gov.au/Parliamentary\\_Business/Bills\\_Legislation/Bills\\_Search\\_Results/Result?bld=r6940](https://www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bld=r6940).

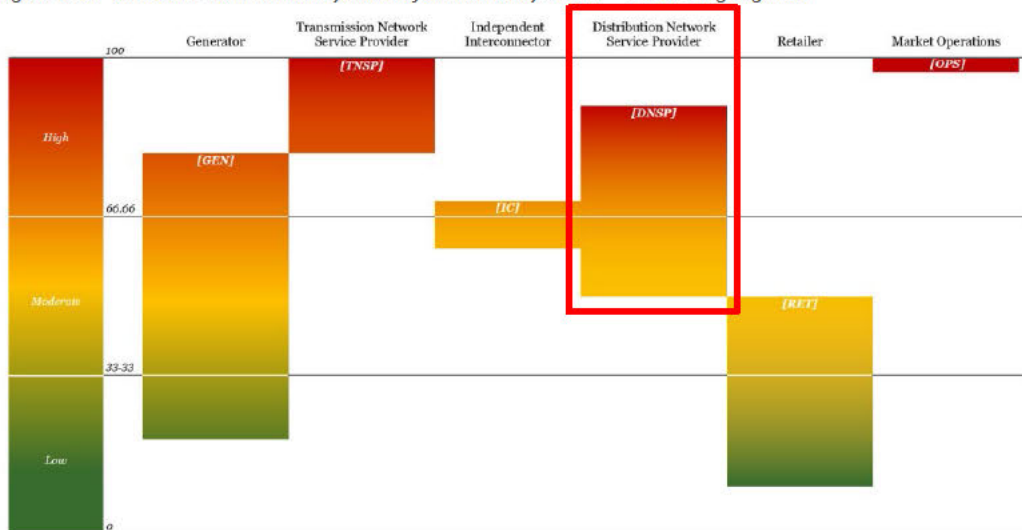
<sup>12</sup> Privacy Legislation Amendment (ENFORCEMENT and Other Measures) Bill 2022 EXPLANATORY MEMORANDUM, in reference to Section 13G – civil penalties. Paragraph 12.

<sup>13</sup> AESCSF Framework and Resources, AEMO, AEMO website.

<sup>14</sup> United States Department of Energy Cyber Security Capability Maturity Model.

<sup>15</sup> AEMO AESCSF Framework Overview – 2022 Program. Page 1.

Figure 2.1: AESCSF E-CAT criticality bands for electricity sector – DNSPs highlighted



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

### AESCSF Version 2 (V2)

- 60. 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 security requirements for the energy sector in line with escalating and evolving cyber threats.
- 61. The 2023 program intends to support AESCSF V2 assessment, AESCSF V1 (noting RMP minimum obligations), and a transition plan to ‘sunset’ AESCSF V1. AESCSF V2 was released in 2023. The update to AESCSF v2 has resulted in an additional 72 practices (i.e., 20 per cent additional practices). A summary of the difference between AESCSF V1 and V2 is summarised in v2.1 and AESCSF v2 is provided in Table 2.1. AEMO has stated previously 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.’<sup>16</sup>

Table 2.1: AESCSF Version 1 and Version 2 comparison – Security Profiles

Security Profile	Participant criticality	Total practices/anti-patterns required to achieve SP	
		AESCSF V1	AESCSF V2
SP-1	Low	88	123
SP-2	Medium	200 (88+112)	275 (123+152)
SP-3	High	282 (200+82)	354 (278+79)

Source: AEMO, AESCSF V2 Summary of Changes, page 4

- 62. To help organisations define roadmaps to improved cyber security maturity, the ACSC included guidance on ‘Priority Practices’ within each SP. The Priority Practices are recommended for completion first as part of any uplift program.

<sup>16</sup> AEMO AESCSF Framework Overview – 2022 Program. Page 3.

## 2.4 AER Guidelines for non-network ICT assessment

### 2.4.1 Assessment of non-network ICT capex

- 63. The scope of our assessment includes cyber security capex and is categorised as non-network ICT.
- 64. The AER's 2019 non-network ICT capex assessment approach guideline ('ICT assessment guideline') is relevant to EQ's proposed cyber security capex. The proposed expenditure is also 'non-recurrent'.
- 65. 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:<sup>17</sup>

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

- 66. 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.<sup>18</sup> 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 prudence) 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.<sup>19</sup>*

#### **Complying with new / altered regulatory obligations / requirements**

- 67. 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 providers [sic], the costs and merits of these should be compared.<sup>20</sup>*

#### **New or expanded ICT capability, functions and services**

- 68. 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.*

*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 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.*

<sup>17</sup> 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.

<sup>18</sup> The only exception will be where the business can demonstrate that any unquantified/intangible benefits of an option can support the decision to not choose the highest NPV option.

<sup>19</sup> AER, Non-network ICT capex assessment approach, November 2019. Page 11.

<sup>20</sup> AER, Non-network ICT capex assessment approach, November 2019. Page 11.

*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.<sup>21</sup>*

## 2.5 Implications for our assessment

### Increasing threat landscape and attack surface mean cyber risk is increasing

69. 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.
70. In our assessment we have sought to understand how EQ 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

71. 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
  - CIRMP, which requires completion of all the practices (and absence of anti-patterns) required to achieve SP-1 noting that SP-1 is the least onerous of the security profiles under the AESCSF.
72. If NSPs are classified as a SoNS, then ESCOs apply and which are applied on a case-by-case basis to the NSPs.
73. Further the civil penalties for a breach(es) of the Privacy Act have been increased in 2022 from \$2.2 million to \$50.0 million (maximum) with the expectation from the Federal government via the amendment that organisations such as EQ will act accordingly to undertake robust privacy and security practices which we interpret to include cyber security-related practices.
74. We have assessed how EQ has responded to its common and specific cyber security compliance obligations, cognisant of:
- the worsening threat landscape and attack surface issues; and
  - its expected cyber security compliance position at the end of the current RCP.
75. We have also considered:
- whether EQ has identified any other relevant obligations.
76. In addition to its minimum compliance obligations, we consider the controls EQ has proposed (and the cost of them) to manage the increasing cyber security threat landscape. A useful reference is the SP practices expected to be in place by the end of the current RCP and the projected SP practices it is likely to achieve with the proposed investment by the end of the next RCP (if available).

<sup>21</sup> AER, Non-network ICT capex assessment approach, November 2019, Page 12.

## 3 EQ'S PROPOSED CYBER SECURITY EXPENDITURE

EQ has presented its expenditure requirements in two 'tranches' – an underlying program of recurrent opex to 'maintain' its current operations and its 'Uplift' cyber security investment comprising largely of capex initiatives to implement controls to address identified gaps in its cyber security capability.

We have been asked by the AER to assessment EQ's cyber security capex forecast, noting that EQ does not propose an opex step change for either its 'maintain operations' nor for its uplift in cyber security capability.

EQ has proposed \$100.7 million SCS capex for cyber security uplift in the next RCP. Of this \$48.4 million is designated for Energex and \$52.3 million is designated for Ergon. Across the two businesses, \$53.4 million is for ICT cyber security while \$47.4 million is for OT-related cyber security uplift.

### 3.1 Overview and summary of proposed expenditure

#### 3.1.1 Documents supporting EQ's proposed cyber security program

77. EQ initially provided two sets of near identical core documents to support its cyber security strategy, initiatives and investment at a whole-of-business level, one set for Energex and one set for Ergon. The Energex documents are:
- (SOC1 Information) Energex - 5.8.01 - Non-network ICT Plan - January 2024 – confidential
  - (SOC1 Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential
  - (SOC1 Information) Energex - 5.8.11 - Non-network ICT Forecast Model - January 2024 -confidential.
78. These documents were supplemented by information provided in response to written information requests and from presentation material and by discussions at an on-site meeting with EQ representatives and representatives of the AER between 13 and 15 May 2024.

#### 3.1.2 What EQ proposes in its RP

##### **EQ's cyber security capex is directed to capability uplift throughout the next RCP**

79. EQ propose two tranches of cyber security investment over the next RCP:
- A 'maintain operations' program which is 100% opex and for which EQ does not propose an opex step change – we do not consider this further in this report
  - A 'capability uplift' program which is primarily capex to respond to increasing cyber threat – this is the focus of this report.<sup>22</sup>

<sup>22</sup> EQ does not seek an opex step change for the opex it identifies for its capability uplift program of work



**EQ proposes a significant expenditure on capability uplift in cyber security in the next RCP**

- 80. As shown in Table 3.1, the respective standard control services (SCS) capex models from Ergon and Energex show a combined \$100.7 million capex for the next RCP on the capability uplift. Energex is allocated \$48.4 million across three projects and \$52.3 million is allocated to Ergon across three similarly named projects.
- 81. We note that Ergon has classified its OT cyber security replacement project as repex, whereas Energex has designated it as augex. No explanation of the difference is provided. Across the two businesses, \$53.4 million of the proposed capex is for ICT cyber security while \$47.4 million is for OT-related cyber security uplift programs.

Table 3.1: EQ's SCS cyber security 'uplift' capex, \$m, FY25 (excluding capitalised overheads)

EQL entity	ID	RIN Category	FY26	FY27	FY28	FY29	FY30	Total
<b>Energex</b>								
[REDACTED]	[REDACTED]	ICT	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	23.98
[REDACTED]	[REDACTED]	Augex	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	13.79
[REDACTED]	[REDACTED]	Augex	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	10.67
<i>Sub-total</i>			[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	48.44
<b>Ergon</b>								
[REDACTED]	[REDACTED]	ICT	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	29.43
[REDACTED]	[REDACTED]	Augex	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	9.00
[REDACTED]	[REDACTED]	Repex	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	13.85
<i>Subtotal</i>			[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	52.28
<b>TOTAL</b>			[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]	100.72

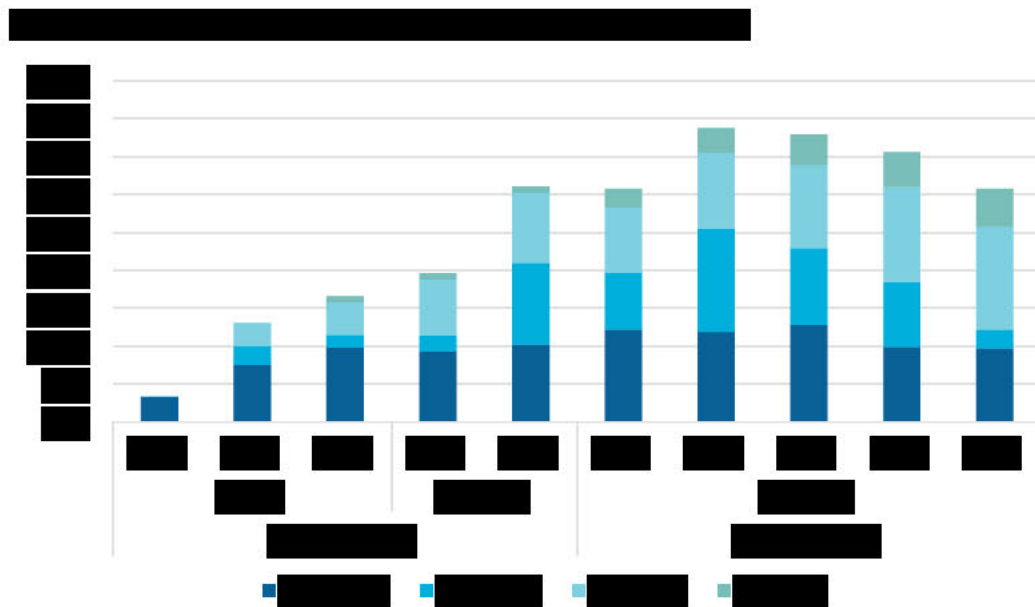
Source: Ergon - 5.2.01 - Model - SCS Capex Model - January 2024 – public; Energex - 5.2.01 - Model - SCS Capex Model - January 2024

- 82. EQ's capability uplift capex is part of a wider cyber security program, with EQ also forecasting 'maintain operations' expenditure, which we show in Table 4.1. The expenditure forecast to maintain operations is accounted for as opex. EQ has not sought an opex step change for its forecast opex and therefore our scope does not include assessment of this amount.

**Capex for the next RCP is significantly higher than in the current period**

- 83. In Figure 3.1 we show a whole-of-business 'totex' profile over the current RCP and next RCP. A clear totex uplift in average annual expenditure is proposed due to the combination of opex required to 'maintain current operations' and to 'uplift' cyber security capability. As can be seen from this profile, EQ's proposal for the next RCP also represents a significant uplift on the capex in the current period, with the majority of the increase being for an OT capex uplift program starting in FY25.





Source: Ergon - IR#037 - Response Cyber onsite follow up - 20240606 – Confidential Page 8; (SOCl Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential, Table 6

### Modelling error

84. Ergon advised in a response to an information request that it made a modelling error in entering the OT SCS capex, where \$20.15 million (\$2022) was incorrectly entered rather than \$21.2 million.<sup>23</sup> As part of this advice, Ergon also provided updated annual expenditure profiles for both OT projects which differ markedly from its RP SCS model. Ergon has advised that it will correct the modelling in its Revised RP (RRP). For the purposes of our assessment, we have referred to the ‘as provided’ RP spreadsheets.

### The business cases are nearly identical and cover the whole of EQ business

85. The two ‘ICT business case 5’ documents referred to in Table 3.1 (which is how EQ refers to them in the respective Ergon and Energex non-network ICT forecast models<sup>24</sup>) cover the whole-of-business cyber security expenditure forecast, that is ICT *and* OT (or non-network and network) expenditure, with cost allocations to Energex and Ergon SCS presented in an appendix. The business cases themselves (i.e. one for Ergon and one for Energex) are called ‘Business Case Cyber Security.’<sup>25</sup> The business cases incorporate multiple initiatives and projects, including the OT/OTE augex/replacement projects separately identified in Table 3.2 (sourced from the respective SCS capex models).

## 3.1 Summary of the basis for EQ’s proposed expenditure

### 3.1.1 Problem definition – risk and obligations

#### EQ has demonstrated that it understands the increasing cyber security risk and its SOCI Act obligations

86. From the information provided in its business case it is clear that EQ has a good understanding of its legislative obligations.

<sup>23</sup> Ergon - IR#037 - Response Cyber onsite follow up - 20240606 – Confidential. Page 6. Table 5.

<sup>24</sup> (SOCl Information) Energex - 5.8.11 - Non-network ICT Forecast Model - January 2024 -confidential (SOCl Information) and the equivalent Ergon model.

<sup>25</sup> Ergon - 5.8.04 - Business Case Cyber Security - January 2024 - confidential is also a whole of EQ business case and includes allocations to the two DNSPs and SCS in an appendix; there is an equivalent Energex business case.

87. The drivers for change enunciated in EQ's business cases are aligned to the ASD's cyber security Threat Report 2023, stressing the increasing complexity, prevalence, and targeted nature of cyber security threats on its business.

**EQ's cyber security objective and strategy**

88. Our understanding is that EQ's cyber security objective is to maintain cyber security risks within the Board's Risk Appetite. EQ states that:

*...current security capabilities and controls will become less effective over time as threat actors improve their tactics, techniques, and procedures in an increasingly integrated landscape. Energy Queensland will therefore need to continually invest in updating existing capabilities and introducing new capabilities to ensure that Cyber Security risks continue to be managed within the acceptable risk appetite and are aligned to stakeholder expectations and regulations.<sup>26</sup>*

89. We consider that maintaining cyber risks within the Board's risk appetite is a reasonable objective. The focus of our assessment is whether the proposed SCS capex satisfies the NER capex criteria.

**EQ's cyber security current state**

90. Figure 3.2 and Figure 3.3 present EQ's self-assessment of its current cyber security state

[REDACTED]

[REDACTED]

[REDACTED]

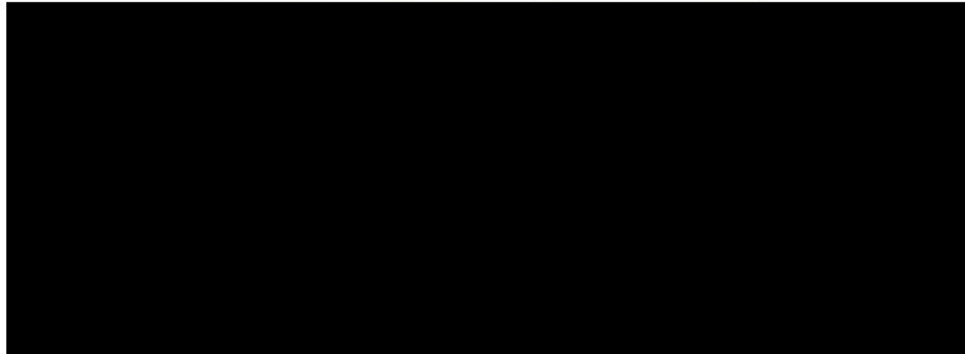
[REDACTED]

<sup>26</sup> (SOCI Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential. Page 9.

Figure 3.3: Current state assessment – non-SOCI Act obligations pertaining to cyber security

Privacy Law	Compliant Y/N
Obligations under the Australian Privacy Act 1988	Y
Privacy Legislation amendment (2022)	Y

### AESCSF Current State Assessment



## 4 OUR ASSESSMENT

EQ's proposed cyber security capex represents a significant uplift from the current RCP in response to increasing cyber security risk, both from the increasing threat level from state actors and others and from its increasing surface attack area. We consider it reasonable that EQ is responding to this risk outlook with increased expenditure.

We consider that EQ has an optimistic view of its likely cyber security risk exposure at the commencement of the next RCP. Its peers are typically rating their inherent cyber security risk materially higher than EQ, noting that EQ does not identify as having a higher level of cyber security maturity than its peers. However, like EQ, its peers are typically proposing significant investments to maintain their cyber security risk at the starting level (or somewhat improve upon it) through to the course of the next RCP.

To develop its 'uplift' program, EQ has taken a risk-based approach to developing its planned initiatives. EQ has not targeted a specific AESCSF Security Profile. A risk-based approach is appropriate provided that the proposed new or enhanced controls are demonstrated to align to current and foreseen gaps in capability.

EQ has identified its core risk exposures and has proposed controls to address them, considering three options with increasing investment. The controls and the cost estimates for the preferred controls have been developed with external advice and to a level of detail commensurate with the stage of the project lifecycle.

EQ has provided a cost-benefit analysis which shows a positive NPV for its program. We have concerns with a number of aspects of this claimed analysis, which we describe in this section. However, we consider that EQ's assessment and determination of its proposed controls, provides reasonable evidence of the risk-cost approach that it has applied, we consider that its cost estimate to uplift these proposed controls is reasonably based and we consider that it is valid to conclude that its proposed uplift expenditure has a positive NPV.

We also undertook a high level benchmarking exercise, comparing EQ's proposed expenditure with a proxy for a peer organisation of a similar size, by aggregating Ausgrid's and Essential Energy's cyber security spends. The normalised benchmarks indicate that EQ's proposed expenditure is reasonable.

On these bases, we therefore consider that EQ's proposed cyber security capex is reasonable forecast of its requirements.

### 4.1 EQ's current state

91. We asked EQ for an assessment of its current state maturity against the AESCSF to help us understand the level of completion of the current RCP. Its response was that as measured against the AESCSF V1:<sup>27</sup>

<sup>27</sup> Ergon - IR#037 - Response Cyber onsite follow up - 20240606 – Confidential, Page 15.



- It expects to achieve AESCSF SP-2 by 2025 against AESCSF V1
- [REDACTED]
- [REDACTED]
- [REDACTED]

92. Whilst it is reasonable to assume that EQ’s overall cyber security capability will be improved by the end of the current RCP, from our experience EQ will likely not be more progressed than its peers. However, it is likely to have achieved its SOCI Act obligations.

## 4.2 EQ’s risk analysis

EQ has appraised the cyber security risk landscape and its cyber security obligations

93. From the information provided in its business case it is clear that EQ has a good understanding of the external and internal sources of cyber security risks it faces as a critical infrastructure owner operator.
94. It has also provided sufficient analysis of the SOCI Act to lead us to conclude that it has a good understanding of what its compliance obligations are and how to meet them.

### 4.2.2 EQ’s identified sources of risk and responses in the current RCP

EQ has identified and prioritised six major cyber security risks

95. EQ’s current Capability Uplift Program (CUP) and the extension of it proposed for the next RCP is based on addressing six sources of risks:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

96. In our experience, this list is largely consistent with the risk assessment of other DNSPs. We would therefore expect EQ to identify the gaps in its cyber security defences using a risk framework such as the AESCSF and/or using a combination of internal and external advice.

EQ is implementing a cyber security ‘Capability Uplift Program’ in the current RCP

97. In response to the increasing cyber threat level and its obligations under the SOCI Act, EQ developed a Cyber Security Capability Uplift Program (CUP) which it is implementing in the current RCP. EQ advises that it prioritises risk-based initiatives and expected compliance obligations under the SOCI Act.<sup>28</sup>
98. It has implemented [REDACTED] initiatives in the period FY22-FY24 with a further [REDACTED] initiatives identified for implementation in FY25.<sup>29</sup> EQ does not provide any statistics regarding the impact of its CUP on cyber security breaches (i.e. including the severity of the incident), which would have been useful in understanding the effectiveness or otherwise of the CUP.

<sup>28</sup> (SOCI Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential. Page 7.

<sup>29</sup> EMCa\_AER Presentation - 13 to 15 May 2024 (Day 3)\_provided to AER. Slide 70.

EQ does however provide Figure 4.1 as a qualitative representation of the cyber security risk reduction over the current RCP from its CUP, with six key risks 'remaining within the risk appetite of the Energy Queensland Board.'<sup>30</sup>



EQ's risk appetite interpretation does not appear to align with the requirements of the NER

99. Our understanding from the information provided, is that the directive to EQ from its Board is that the two businesses 'must maintain risks within the Board's risk appetite, even with internal and external change.'<sup>31</sup> EQ's risk appetite is summarised as:

- For business critical information assets:
  - Very low risk with high degree of certainty
  - Demonstrate SFARP<sup>32</sup> (in line with the requirements of the SOCI Act); and
- For other information assets:
  - Decisions based on cost effectiveness, priorities and potential outcomes
  - Some tolerance for uncertainty.<sup>33</sup>

100. [Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]<sup>34</sup>

101. We have assessed EQ's expenditure with reference to the NER expenditure criteria for network (OT) and non-network (ICT) capex, and the AER's guidance (see Section 2.5).

<sup>30</sup> (SOCI Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential. Page 8.  
<sup>31</sup> EMCa\_AER Presentation - 13 to 15 May 2024 (Day 3)\_provided to AER. Slide 76.  
<sup>32</sup> So Far As Reasonably Practical  
<sup>33</sup> EMCa\_AER Presentation - 13 to 15 May 2024 (Day 3)\_provided to AER. Slide 76.  
<sup>34</sup> Ergon - IR#037 - Response Cyber onsite follow up - 20240606 – Confidential, response to question 5. Page 10.



Among other things, expenditure that is designed to maintain levels of risk needs to demonstrably be cost efficient. ICT expenditure that provides increased functionality needs to be shown to be at least NPV positive.

**EQ's projected cyber risk in 2025 appears to be optimistic**

102. As shown in Figure 4.1, EQ has forecast that [REDACTED] as a result of implementing its CUP.

103. [REDACTED]

104. We do not have sufficient evidence to be certain about either position, but the benefit of measuring cyber security maturity against a framework such as the AESCSF is that it provides an auditable benchmark. By this measure, EQ would appear to be somewhat optimistic in its assessment of risk and, if correct, this would suggest that it requires less investment than its peers to mitigate the rising cyber risk profile in the next RCP. On balance, however, we tend to the interpretation that EQ's risk assessment is optimistic and that it is reasonable for it to require further uplift and associated investment that is broadly commensurate with its peers., not considerably less.

105. From an assessment perspective, whether EQ is seeking to improve its risk profile or maintain it is important, with the former requiring demonstration of a positive NPV. EQ has presented a cost-benefit analysis as part of its options analysis, which we review.

**EQ estimates that its cyber security risk will be high by the end of the next RCP unless it takes further action**

106. EQ's qualitative assessment is that its cyber risk will be [REDACTED] in 2030 if it does nothing more than maintain its 2025 level of cyber security capability.<sup>35</sup> This is a reasonable assessment, noting that some of its peer DNSPs rate cyber security risk increasing to [REDACTED] for the 'do nothing more' scenario.

107. Despite EQ's generally optimistic ratings, the relevant matter for application of the AER Guidelines is the extent to which increased investment is required in order to maintain the current risk rating. We consider that it is reasonable to conclude, as EQ has, that such investment is required to respond to the increasing threat landscape.

## 4.3 EQ's options analysis

### 4.3.1 Defining the options

**EQ identifies five options for managing cyber security obligations and risks**

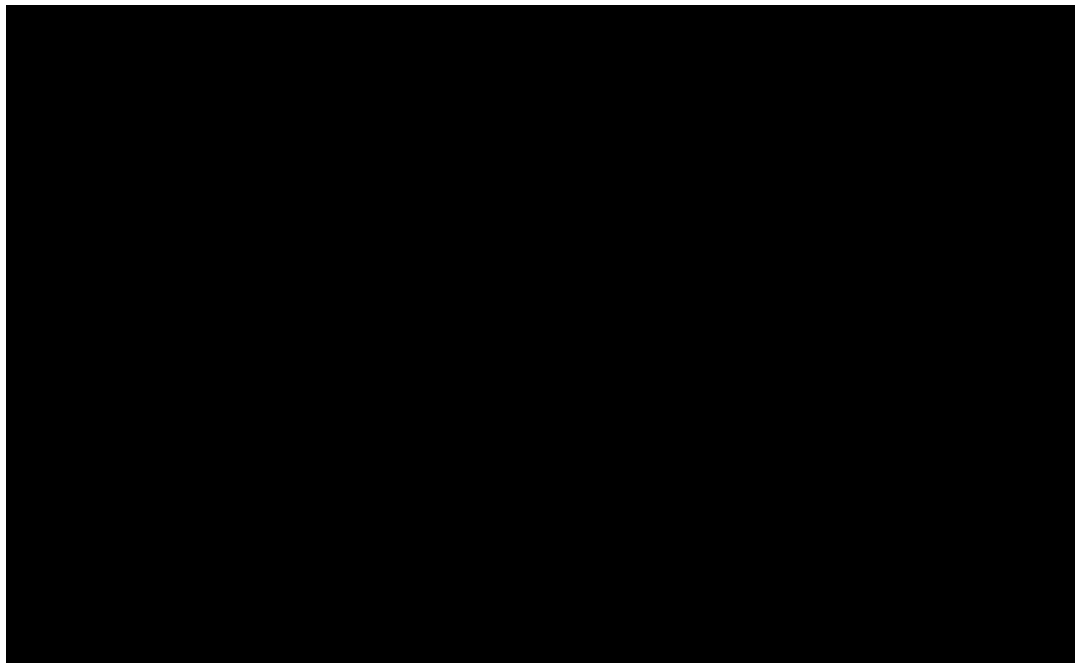
108. EQ states that it initially identified five 'scenarios' to manage its cyber security risk through the next RCP, but discarded two because they would not address the rising risk profile –

<sup>35</sup> Ergon – IR#037 – Attachment 2 – Cyber security presentation – 20240606 – Confidential.

- Scenario 1: 'maintain operations' (aka 'spend nothing more on capability uplift') and
  - Scenario 2: target SP-3.
109. EQ rejects Scenario 1 because it does not address increased risks. It rejects Scenario 2 because it determined through cost-benefit analysis that it was not likely to be superior to the other scenarios.
110. EQ therefore focusses on Scenarios 3-5, which it re-labels as options 1 to 3.<sup>36</sup>

After discarding two 'scenarios' EQ subjects the remaining three to further assessment

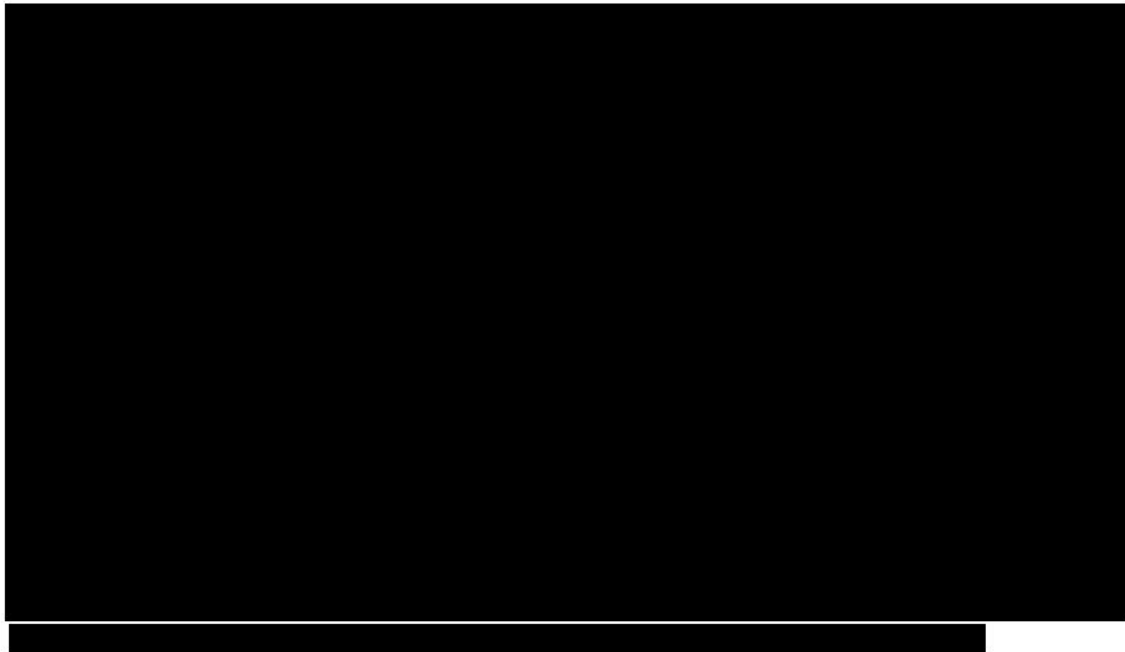
111. As shown in Figure 4.2, and contrary to the other statements in EQ's business case, we find that EQ has in fact retained Scenario 1 as a fundamental component of each of Options 1-3, because Option 2 builds on Option 1 and Option 3 builds on Option 2. Thus, the underlying opex for maintaining operations is a foundational component of each option and which we understand to mainly cover the cost of its dedicated and relatively large cyber security operations team.
112. Whilst we accept that Scenario 2 is unlikely to be superior to EQ's preferred Option 3, for completeness our view is that EQ should have included it in its detailed analysis.



113. Table 4.1 shows the breakdown of total cyber security costs for each of the three options analysed by EQ. Noting that the total expenditure for each option includes \$57.3 million (\$2022) on the common 'maintain operations' program, the uplift program for EQ's proposed option (Business Case Option 3) is \$116.5 million totex (in \$2022), of which \$98.8 million (\$2022) is the capability uplift capex.

---

<sup>36</sup> (SOCI Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential, Page 18.



114. We consider each option in turn in sections 4.3.2 to 4.3.4.

### 4.3.2 Option 1 Evolve current cyber security capabilities

#### Option 1 is unlikely to be the prudent response

115. Option 1 is predicated on maintaining compliant cyber security operations and technology platforms and addressing the risks of

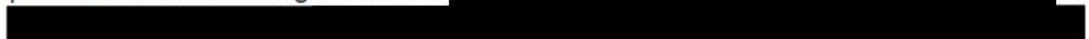


116. In its business case, EQ estimates an NPV of [redacted] million (\$2022) for this option based on assumptions we discuss in Section 4.5. The NPV as stated in the business case is the lowest of the three options.

### 4.3.3 Option 2: Evolve current cyber security capabilities and provide basic capability uplift to support grid evolution

#### Option 2 addresses [redacted] of the six identified risks but is unlikely to be the prudent option

117. Option 2 is predicated on maintaining compliant cyber security operations and technology platforms and addressing the risks of



118. EQ states that this option would maintain 'just enough' cyber security capability to remain compliant with the likely future cyber security regulatory obligations of the SoCI Act on the assumption that during the next RCP, changes to the SoCI Act will invoke an obligation to achieve at least AESCSF SP-2 maturity.<sup>37</sup>



<sup>37</sup> (SOC1 Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential. Page 26.

<sup>38</sup> (SOC1 Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential. Page 19.



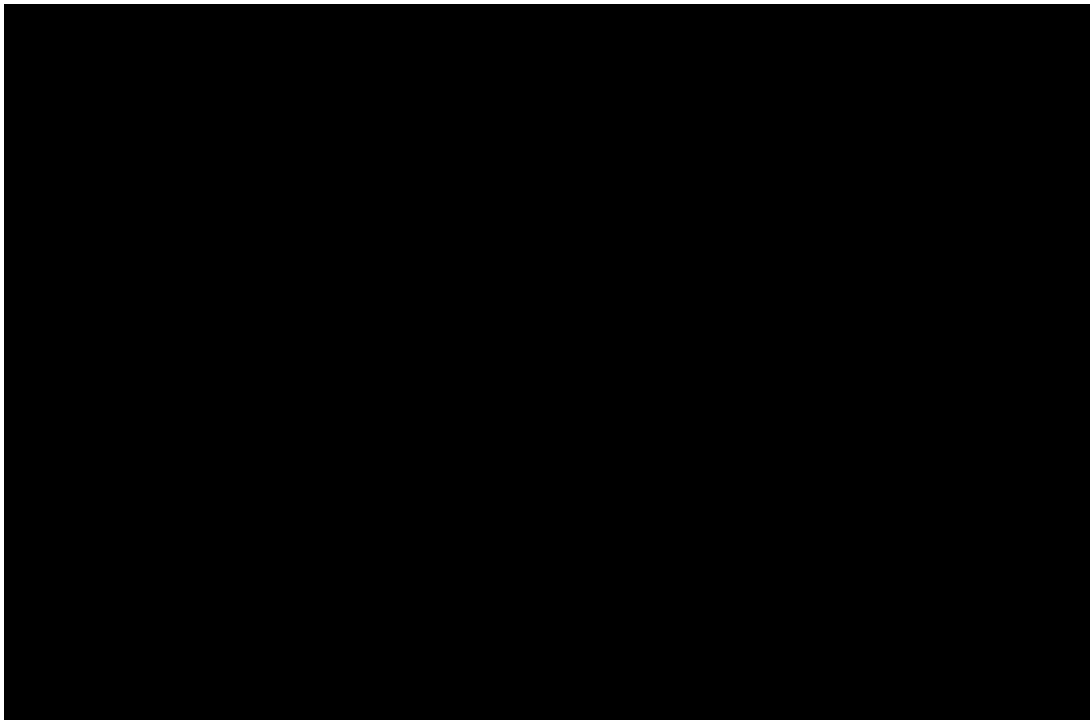
119. EQ rejects this option because risks [REDACTED] would not be addressed.
120. To us, the logical scope for Option 2 would be to include measures to address its [REDACTED]. However, the way EQ has scoped the initiatives, the incremental cost for mitigating the risk posed by all six sources in Option 3 compared to Option 2 is relatively low (+ [REDACTED]), so as discussed below, we consider Option 3 to be the prudent choice regardless.
121. In its business case, EQ estimates an NPV of [REDACTED] million (\$2022) for this option.<sup>39</sup> This is the second lowest NPV of the three options EQ presents but is only marginally higher than Option 1's NPV.
122. Whilst we have some concerns regarding EQ's economic analysis (refer to section 4.5), we nonetheless consider Option 2 to be superior to option 1 and inferior to Option 3, as discussed below.

#### 4.3.4 Option 3 Strengthen all current and build new cyber security capabilities (EQ proposed)

123. In addition to the initiatives referred to in Options 1 and 2, the following Cyber Security initiatives form part of this option:
- [REDACTED]
  - [REDACTED]
124. EQ proposes that this option will provide [REDACTED]. As with Options 1 and 2, it will address EQ's minimum requirements from the SOCI Act and it will satisfy the EQ Board's cyber security risk appetite. It implements stronger cyber security controls in [REDACTED] than the other options.
125. As shown in Figure 4.3, EQ predicts the residual risk (2030) from implementing Option 3 will be the [REDACTED] based on its qualitative analysis.
126. In its original business case, EQ has estimated an NPV of [REDACTED] million (\$2022) for this option.<sup>40</sup> which is [REDACTED] higher than for Option 2 for a 6% capex uplift. Whilst we have concerns about EQ's qualitative risk assessment (overly optimistic) and its economic analysis (refer to section 4.5), we consider that Option 3 is the prudent selection.

<sup>39</sup> (SOCI Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential. Table 5.

<sup>40</sup> (SOCI Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential. Table 5.

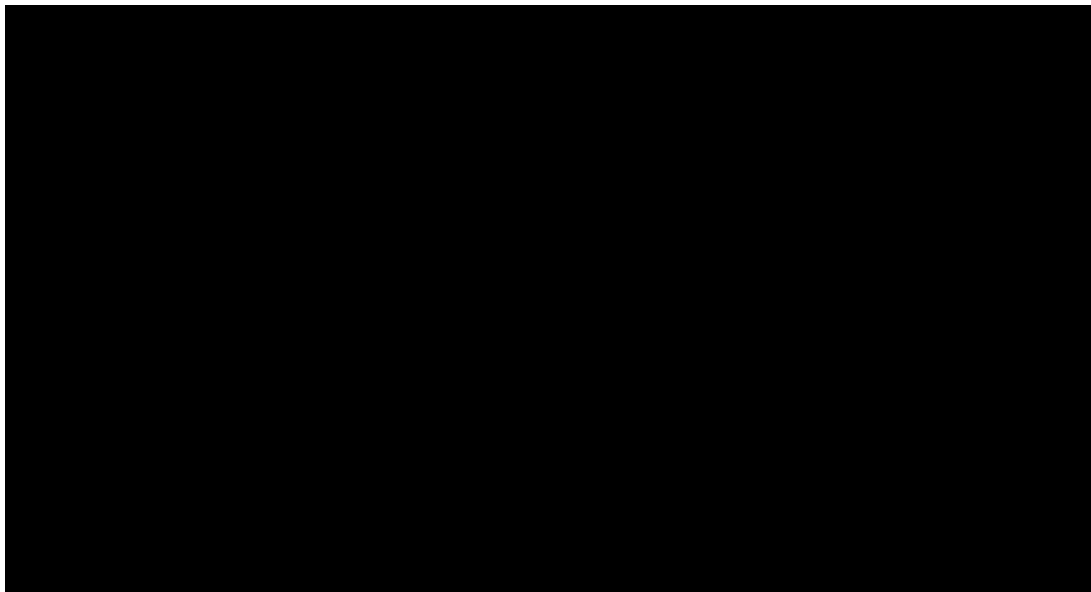


## 4.4 EQ's cost forecasting methodology

127. In this section we consider EQ's approach to estimating the cost for the required controls for its 'uplift' cyber security program of work, implemented via six initiatives.

### 4.4.1 EQ's proposed initiatives

128. Figure 4.4 summarises EQ's costing for the six initiatives designed to address its register of six core risks. These initiatives are for the 'capability uplift' aspect of EQ's proposed expenditure and the totex aligns with the expenditure shown in Table 4.1 for EQ's proposed option (business case Option 3) capability uplift program. For each of these initiatives there are a number of defined projects; in total the program comprises 35 'capability uplift' projects within the next RCP.



The [REDACTED] initiative requires [REDACTED] of 'uplift' capex in the next RCP

129. Options 1-3 all include the initiative to 'evolve existing cyber security capabilities and risk controls' which requires a significant proportion of the total proposed cost uplift across the next RCP. The capex alone is \$53.0 million (\$2022). We were not clear about the scope of work nor therefore the basis for the cost estimate from EQ's business case, so we asked for more information. The response was that the 'evolution' of the capabilities and controls is proposed as an extension of the approach used in the current RCP (and which helped EQ benchmark its overall cost estimation). EQ further describes the scope of this initiative as comprising three workstreams:<sup>41</sup>

- [REDACTED]
- [REDACTED]
- [REDACTED]

130. There appears to us to be a degree of overlap between the last and the first workstream. However, our concerns are largely alleviated by the advice received in response to another information request<sup>42</sup> that EQ has spent (or will) \$57.1 million (\$2022) on non-recurrent ICT and OT capex in the current RCP. We infer from the information provided that this is the cost of the current approach that EQ refers to in forecasting the cost of the initiative for the next RCP (i.e. the capex is similar). Given (i) both OT and ICT controls are covered within this initiative, and (ii) our acceptance of EQ's cost estimation methodology (see section 4.4.2), we are satisfied that the cost of the initiative is reasonable.

Keeping cyber security technology platforms current and in line with industry trends is the second most expensive initiative

131. The initiative with the second highest capex in Figure 4.4 is [REDACTED]  
[REDACTED]  
[REDACTED] This is a common and reasonable approach to help minimise risk.

The remaining initiatives appear to be reasonably derived with two minor exceptions

132. The scope and cost of the remaining initiatives contain projects which, as described, are aligned with the investments in building cyber security maturity that we would expect to see and align to managing the core risks identified by EQ.

133. Two relatively minor exceptions are:

- [REDACTED]
- [REDACTED]

134. As these are minor projects within the \$100.3 million proposed capex, and which in turn is likely no more than ±20% accurate at this stage of the project development lifecycle, they do not detract from our conclusion that the initiatives and projects that EQ has based its costing on, are reasonable.

<sup>41</sup> Ergon - IR#037 - Response Cyber onsite follow up - 20240606 – Confidential, answer to question 2.

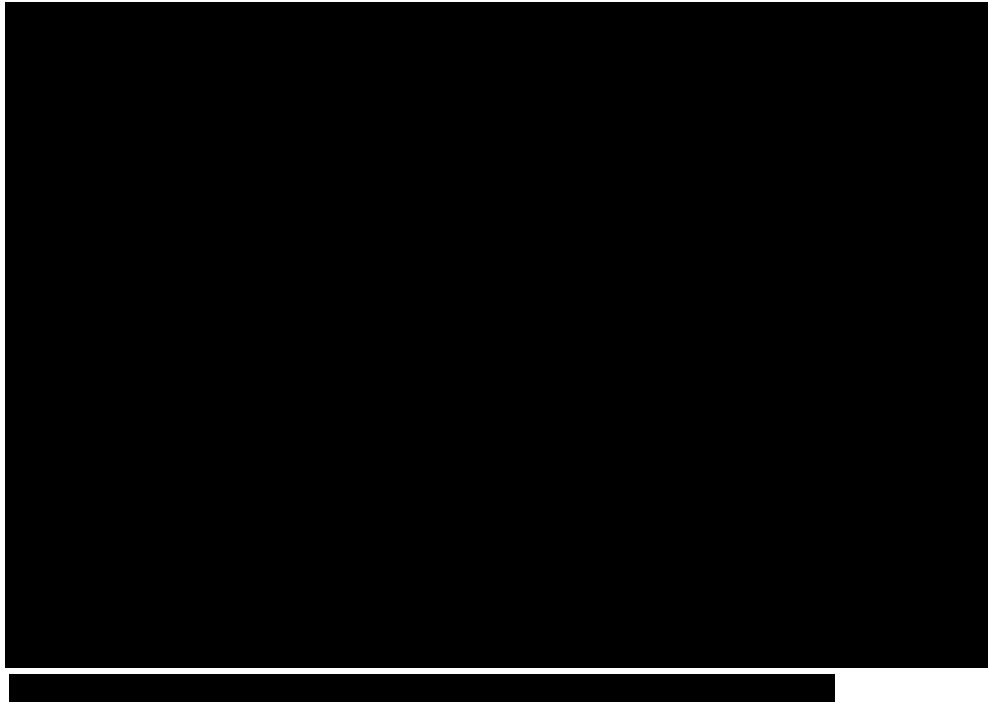
<sup>42</sup> Ergon - IR#037 - Response Cyber onsite follow up - 20240606 – Confidential, answer to question 4.



## 4.4.2 EQ's cost estimation methodology

### EQ's cost estimation principles are sound

135. Figure 4.5 shows the cost estimation principles that EQ has applied in developing its cost forecast for the cyber security program for 2025-30. These principles are consistent with good industry practice.



136. EQ's spreadsheet provides a cost estimate for each year of the next RCP for each of the projects under the [REDACTED]. Whilst the cost estimates are obviously quite approximate, the level of detail and the quantum of each are sufficient for us to conclude that the cost estimates are reasonably derived.

### The ratio of capex to opex is relatively high

137. In our other reviews for the AER of NSPs' cyber security expenditure forecasts, we have seen a consistent transfer from capex to opex from a combination of moving controls to cloud based applications and systems (i.e. Software as a Service) and from no longer capitalising aspects of opex incurred during project development.
138. We observe that EQ's ratio of capex to opex remains relatively high. The IFRS requirement is not mentioned in the business case, however it appears that EQ is transitioning to cloud environments (including hybrid approaches).
139. This does not affect our assessment, which starts from consideration of the totex that EQ has estimated. Any transfer from capex to opex may result in a lower capex spend but, having not proposed an opex step change, EQ would need to absorb the additional opex that might result from such a transfer.

## 4.5 EQ's economic assessment

### 4.5.1 EQ's benefits assessment

#### EQ identifies three event or breach scenarios

140. EQ identifies three adverse event scenarios which have been modelled as cost avoidance benefits compared to the counterfactual of Maintaining operations (i.e. 'doing nothing more' throughout the next RCP to mitigate the assumed increasing risk):

█ [REDACTED]

█ [REDACTED]

█ [REDACTED]

141. We consider these scenarios to be high impact scenarios – what others refer to as P1 cyber security breaches.

#### Likelihood of severe breaches is not adequately justified

142. EQ assumes that the likelihood of these P1 events occurring is one in five years – that is, a 100% chance that each form of P1 breach will occur. EQ has provided rationale for this assumption in addition to its qualitative risk assessment. However, from our experience we consider that this is a pessimistic outlook in the absence of quantitative assessment. EQ could have sought to evidence this assumption from literature scans and evidence from cyber-attack threats on its own business or other DNSPs but has not done so.
143. In our experience, for an entity with the controls and practices in place that EQ states that it will have by 2025, one (central case) or possibly two (high case) of these events in the next RCP is a more reasonable assumption. In saying this we have also considered the positive and material benefit that EQ will enjoy from its ICT replacement and upgrade projects, which are typically designed to avoid technology obsolescence, and thereby take advantage of the latest cyber security defences that are incorporated into successive application/system version releases.

#### EQ's estimation of consequences arising from the breaches is likely to be understated

144. EQ states that it has based the consequence quantification for the P1 events on (i) █  
█
145. We had to ask EQ to provide more detail to understand how it applied these assumptions in practice, including how it estimated the recovery costs.
146. We consider that EQ's approach to quantifying the financial impact of the three forms of P1 breach lacks rigour when we compare it to the analysis of some of its peers. Whilst the construct of its consequence modelling is sound in principle, based on our experience with other DNSP's approaches, we consider the likely consequence cost may be understated – for example, █

#### EQ has not countenanced the impact of lower severity but higher frequency breaches

147. We also note that EQ has not included in its benefit analysis the avoidance of cost impacts of lesser cyber events. Others refer to these as P2-P4 events (similar to the asset

<sup>43</sup> (SOCI Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential. Page 37.

<sup>44</sup> (SOCI Information) Energex - 5.8.04 - Business Case Cyber Security - January 2024 – confidential. Page 37.

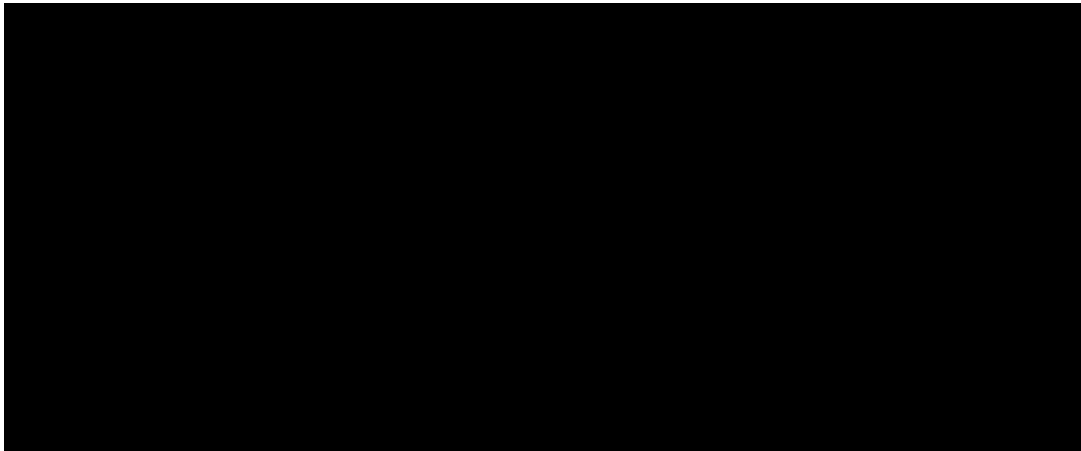
management nomenclature for classifying severity) with much higher numbers of these lower level breaches experienced compared to P1 breaches. Nonetheless, the aggregate contribution of these higher volume/lower cost per event can over five years can represent a considerable contribution to cyber breach risk-cost.

#### EQ's counterfactual cyber security cost is likely to be understated

148. Despite our view that EQ's assumption regarding the likelihood of occurrence of its three event scenarios (referred to us as P1 events) is overstated in the absence of supporting analysis, we consider its consequence analysis to significantly understate the potential avoided cost from implementing Options 1-3.
149. We take this into account in our assessment of EQ's economic analysis which follows.

### 4.5.2 Economic analysis provided by EQ

150. In its non-network ICT forecast model, EQ provides cost benefit analysis (CBA) of its proposed IT initiatives, including its cyber security program. For each such initiative, a CBA is shown for three options and the results of this analysis are presented in the relevant business cases, in support of the proposed option. EQ's objective with this modelling was to evidence its claim that it has adopted a risk-based approach in establishing the extent of its cyber security program, and that it has chosen a prudent option.
151. EQ provided a version of this model with its RP.<sup>45</sup> In early June, in response to an information request, EQ provided an updated CBA for cyber with some costs presented differently, with significantly reduced costs, significantly reduced benefits and a significantly reduced NPV for all options.<sup>46</sup> EQ nevertheless claims that this analysis still supports the option that it originally proposed in its business case.



152. As can be seen in the table, in its updated CBA, the ranking is now changed, and the 'alternative option' now has both a lower cost and a higher NPV. In its response to IR037, EQ refers to the modelling having been updated and presents the now-reduced NPV of [REDACTED],<sup>48</sup> but its response does not appear to recognise that this option is no longer the highest ranked in its updated modelling (to the extent that NPV is the deciding criterion).

<sup>45</sup> (SOCI Information) Energex – 5.8.11 – Non-network ICT Forecast Model – January 2024 (confidential). An identical Ergon workbook is provided, and each represents the business case for EQ in total.

<sup>46</sup> EQ in response to IR037. Attachment 5 – Non-network ICT Forecast Model -20240606.

<sup>47</sup> In its Business Case, EQ's chosen option is presented as 'Option 3'. In its models, 'business case Option 3' is labelled as 'Option 2 (recommended)'. In the models, business case Option 2 comes under a label of 'High Case' although this too is confusing as for cyber security this 'alternative' case has a lower cost, as can be seen in the table. To avoid confusion, we refer in this table and subsequent text to business case Option 2 as the 'proposed option' and business case Option 3 as the 'alternative option'.

<sup>48</sup> Response to IR037. Question 6.

153. In reducing the PV of costs in its updated assessment, EQ removed the costs of its 'maintain operations' program. In itself, this is valid as the objective of the CBA is to validate the uplift program and inclusion of the 'maintain operations' program expenditure in the original version of the CBA was incorrect. However, we find it surprising that the benefit calculations were also reduced so significantly, that the NPVs also reduced.

### 4.5.3 EQ's CBA methodology

154. While EQ's CBA notionally spans 20 years, costs and benefits have been entered only for the next 5 years. This is far from realistic, as the benefits of any 'uplift' will continue and likely be larger beyond the next RCP period, but the recurrent costs will also continue. We expect that EQ's analysis likely understates the NPV of the program, but, absent such analysis, we consider it to be of no value in supporting the choice of the proposed option.

### 4.5.4 Modelling issues with EQ's benefits

155. Relative to assessments that we have reviewed from other NSPs, the EQ CBA is simplistic and we consider that it is not 'fit for purpose'. We comment above on specific aspects of EQ's assumed benefits, but with regard to the analysis itself we note the following:
- The benefits assessment was provided to us only in response to our IR, and (as noted above) it differs significantly from the benefits assessment presented in the EQ business case. It is reasonable to conclude, therefore, that EQ's determination of a cyber security program based on a prudent level of risk mitigation, was not based on the benefits assessment now provided.
  - EQ's benefit assessment for its proposed option has a deduction for assumed insurance coverage, whereas in its modelling, this same deduction has not been made in its formula for its alternative option. This provides what we assume to be an unintended disbenefit to the proposed option and which could explain why, with the updated assumptions, the alternative option now presents as having a higher NPV than EQ's proposed option.
  - There is relatively little difference between the benefits as presented for each option. Whereas the difference between the base case and the highest benefit option above is of the order of 40%, we observe differences of several times between options, in similar analyses presented by other NSPs. We consider that this is partly attributable to a failure to distinguish adequately between the benefit outcomes of the options, but this is also exacerbated by the shortened analysis period.

### 4.5.5 Findings of EQ CBA

156. We are generally supportive of a risk-based assessment to assist with determining a prudent level of cyber security risk mitigation. However, we consider that the CBA that EQ has presented does not appear to have formed the basis for EQ to determine the prudence of the program that it has proposed and, as now presented in EQ's updated CBA, it does not support the option that EQ has proposed. Except in that the CBA does show a positive NPV for EQ's proposed option, we have essentially disregarded EQ's CBA in our assessment and findings.

## 4.6 Top-down benchmarking

157. A top-down benchmark provides a potential cross-check on EQ's proposed expenditure. Given the substantial differences between EQ's presentation of its cyber security risk levels, and issues described above with its CBA, we sought to cross-check its proposed aggregate expenditure by comparison with peers.
158. In response to an information request, EQ provided a spreadsheet and summary analysis with its benchmark analysis, comparing its cyber security expenditure with its peers,



normalising by user numbers and device numbers.<sup>49</sup> Acknowledging the limitations of benchmarking analysis, which we also recognise, EQ concluded from comparison with six other NSPs that:

█ [REDACTED]

█ [REDACTED]

- 159. We took a different approach by considering the combined EQ expenditure and comparing it with Ausgrid and Essential Energy together, because together they provide a broadly similar point of comparison, with broadly similar customer numbers<sup>50</sup> and a broadly similar combined urban and regional customer base.
- 160. Referring to Table 4.3, EQ's proposed cyber security uplift expenditure over the next period is similar to the AER's combined allowances for 2024-29 for Ausgrid and Essential Energy. Comparing EQ's totex (i.e. including its 'maintain operations' expenditure as well as its uplift expenditure), EQ's proposed expenditure is within a reasonable range when we compare totex/user and totex/device.
- 161. While this comparison is not definitive, we consider that it provides further validation that expenditure that EQ has proposed is within a reasonable range.

[REDACTED]

## 4.7 Our findings and implications

### 4.7.1 Summary of our findings

**EQ's qualitative risk analysis appears to be overly optimistic and its quantitative assessment is likely to understate its risk-cost over the next RCP**

- 162. EQ has rated its core cyber security risk sources as likely to be [REDACTED] at the end of the current RCP. This is lower than any other DNSP we have reviewed over the last few years, [REDACTED]. Nevertheless, the objective that we infer from EQ's analysis is that it is seeking to maintain its current risk level over the period, in the face of rising threats and that it will need to uplift cyber security investment to achieve this objective. This is an appropriate objective.

<sup>49</sup> Ergon – IR#037 – Attachment 7 – Cyber Benchmarking – 20240606 – Public and Ergon - IR#037 - Response Cyber onsite follow up - 20240606 – Confidential, Pages 13-14.

<sup>50</sup> Ausgrid and Essential serve around 1.8 million and 0.9 million customers respectively = 2.7 million total. Ergon and Energex serve around 0.8 million and 1.6 million = 2.4 million total. (Information from DNSP websites).

<sup>51</sup> AER – Final Decision Attachment 5 – Capital Expenditure – Ausgrid – 2024-29 Distribution revenue proposal – April 2024. Table A.3.

<sup>52</sup> For Essential Energy's proposed cyber security expenditure for the 2024-29 RCP we referred to information provided to us as part of our technical review for the AER (noting that this is SOCI\_CONFIDENTIAL).



#### EQ's CBA is substandard and does not assist in supporting EQ's proposal

163. EQ's CBA contains a number of deficiencies which render it of little value in supporting EQ's proposal. We consider that EQ has overstated certain risks but has ignored other risks that are material in other DNSPs' analyses. Overall we consider that it has likely understated the benefits and insufficiently distinguished between the benefits of the options that it has considered. Its analysis, which is over only five years, fails to capture the enduring benefits of the program that it proposes. In the course of our assessment, EQ provided an 'updated' CBA that differs considerably from the business case that it had provided, with much lower NPVs and a reversed (though we consider erroneous) ranking between its options.
164. Except to the extent that we consider that EQ's CBA does evidence a positive NPV for its proposal, we have not relied on EQ's CBA in our assessment as we consider that it is not fit for purpose.

#### EQ has selected a risk-based approach and from this has selected the appropriate option

165. Despite issues we have identified with EQ's qualitative and quantitative risk assessments, with its cost-benefit analysis, we consider that EQ has identified the appropriate initiatives that it needs to undertake and has defined a series of projects under these initiatives which collectively are intended to provide it with the necessary additional controls to manage its increasing risks. The identified risk sources are adequately recognised and defined and the controls to mitigate those risks are common and suitable approaches, based on our experience.

#### EQ's cost forecasting methodology and cost forecast for its preferred option is reasonable

166. The costs for the controls have been developed on a reasonable basis, using a combination of vendor information, external advice, and in-house experience.
167. Additional, top-down benchmarking we undertook indicates that EQ's proposed expenditure is within a reasonable range.

### 4.7.2 Implications of our findings

168. We consider that EQ's proposed cyber security capex for the 2025-30 RCP, as shown in Table 3.1, is reasonable.