



# Cyber Security

## Business Case

25 January 2024



Part of the Energy Queensland Group

## CONTENTS

1	EXECUTIVE SUMMARY .....	4
2	DOCUMENT BACKGROUND .....	5
	2.1 Purpose of Document .....	5
	2.2 References .....	5
	2.3 Document History .....	5
	2.4 Approvals .....	6
3	STRATEGIC CONTEXT .....	7
	3.1 Background .....	7
	3.2 Electric Life 2032 and Investment Drivers .....	10
	3.3 Drivers and Challenges .....	11
	3.4 Way Forward and Benefits .....	13
	3.5 Initiatives and Outcomes .....	15
4	INVESTMENT OPTIONS .....	18
	4.1 Options Description .....	18
	Option 1: Evolve current Cyber Security capabilities .....	19
	Option 2: Evolve current Cyber Security capabilities and provide basic capability uplift to support grid evolution .....	20
	Option 3: Strengthen all current, and build new, Cyber Security capabilities .....	22
	4.2 Criteria Description .....	23
	4.3 Summary of Options Analysis .....	24
	4.4 Recommended Option .....	26
5	IMPLEMENTATION OF RECOMMENDED OPTION .....	28
	5.1 Governance Arrangements .....	28
	5.2 Change Impact .....	28
	5.3 Delivery Roadmap .....	29
	5.4 Investment Benefits .....	31
	5.5 Investment Costs .....	31
	5.6 Financial Summary .....	31
6	APPENDICES .....	33
	6.1 Applicable Compliance Requirements .....	33

---

6.2	Options Analysis .....	34
	Compliance expectations addressed by option .....	34
	Risk mitigation associated with option .....	35
	Financial benefits associated with option .....	37
	Non-financial/not-quantified benefits associated with option .....	38
	Costs associated with option .....	39
6.3	Alignment with the National Electricity Rules.....	40
6.4	Assumptions.....	41
6.5	Dependencies .....	42
6.6	Delivery Risks and Controls.....	43
6.7	Reconciliation Table.....	44

## 1 EXECUTIVE SUMMARY

Title	Non-Network ICT – Cyber Security												
Application	All Energy Queensland lines of business.												
Expenditure category	<input checked="" type="checkbox"/> Replacement <input checked="" type="checkbox"/> Augmentation <input type="checkbox"/> Connections <input type="checkbox"/> Tools and Equipment <input checked="" type="checkbox"/> Non-network ICT <input type="checkbox"/> Property <input type="checkbox"/> Fleet												
Identified need	<input checked="" type="checkbox"/> Network resilience <input type="checkbox"/> Facilitate customer and community opportunities <input type="checkbox"/> Evolving grid infrastructure <input type="checkbox"/> Safe, efficient and affordable operations  This business case addresses the network, and non-network ICT investment required to support the key investment driver 'Network resilience'. Energy Queensland is committed to providing a secure, dynamic and reliable electricity network for a rapidly changing operating environment. Growing digitalisation of our grid, interconnectedness of our systems and services, and a dynamic external threat landscape increasingly create resilience challenges. The Cyber Security ICT business case ensures our services are resilient and protected against security threats and provide improved capacity, response and recovery communications for customers and communities.  It is important to note that while Network resilience has been selected as the key investment driver, this business case is also critical in enabling the remaining drivers.												
Benefits	This business case realises four benefit categories: Cost avoidance, risk and compliance, future proof capabilities, and effective cyber operations.  The quantitative benefits to be realised from this investment are \$262.8M (present value \$213.8M).												
Recommended option	Option 3 'Strengthen all current, and build new, Cyber Security Capabilities' is the recommended option, as it provides the most prudent and efficient long-term investment outcome when securing Energy Queensland's critical infrastructure assets and data in line with customer and community expectations. This option will also ensure Energy Queensland's cyber risks remain within risk appetite (all six risks sit within Board risk appetite) by delivering the outcomes from all the identified initiatives.  This option also best enables Energy Queensland's core Cyber Security capabilities so that it will be compliant with its legislative obligations and is adaptive and flexible to the ever-changing threat landscape and requirements of the future energy grid.												
Expenditure <sup>1</sup>	The total investment costs associated with the recommended option (\$M). <table border="1" style="width: 100%; text-align: center;"> <thead> <tr> <th>FY26</th> <th>FY27</th> <th>FY28</th> <th>FY29</th> <th>FY30</th> <th>Total 2025-30</th> </tr> </thead> <tbody> <tr> <td style="background-color: black; color: yellow;">█</td> <td style="background-color: black; color: yellow;">█</td> <td style="background-color: black; color: yellow;">█</td> <td style="background-color: black; color: yellow;">█</td> <td style="background-color: black; color: yellow;">█</td> <td>173.8</td> </tr> </tbody> </table>	FY26	FY27	FY28	FY29	FY30	Total 2025-30	█	█	█	█	█	173.8
FY26	FY27	FY28	FY29	FY30	Total 2025-30								
█	█	█	█	█	173.8								

<sup>1</sup> All financial figures have been rounded and shown in dollars million (\$M) throughout this document, shown using the costing approach for non-network ICT expenditure described in the Non-network ICT Plan 2025-30, section 7.1.

## 2 DOCUMENT BACKGROUND

### 2.1 Purpose of Document

The purpose of this document is to outline Energy Queensland’s proposed program of work pertaining to the Cyber Security business capabilities for the next regulatory control period from 1 July 2025 to 30 June 2030 (2025-30). This business case includes both non-network and network Information and Communication Technology (ICT) Cyber Security programs, benefits and costs.

### 2.2 References

**Table 1: Related Documents**

Date	Name	Type
19/04/2023	Energex Business Narrative Ergon Energy Network Business Narrative	Direction
25/01/2024	Non-network ICT Plan 2025-30 (Attachment 5.8.01)	Document
25/01/2024	Non-network ICT Common Glossary (Attachment 5.8.10)	Document
31/10/2023	RDP 2025 Project – Shared Assumptions	Assumptions Document
25/01/2024	All other non-network ICT business cases (Attachments 5.8.02 to 5.8.08)	Documents

### 2.3 Document History

**Table 2: Document History**

Version Number	Change Detail	Date	Updated by
0.1	Review and develop initial document templates	July to August 2022	EY
0.2	Scoped proposal, assessed costs and benefits, and developed options Draft 1 completed	September 2022 to January 2023 31 January 2023	Energy Queensland EY
0.3	Continued refinement of messages, format and content including incorporating feedback from RRG Session 1 Draft 2 completed	February to June 2023 30 June 2023	Energy Queensland

Version Number	Change Detail	Date	Updated by
0.4	Updated based on feedback from RRG Session 2, Residential Focus Groups, Draft Plan consultation and Strategic Review by Deloitte Draft 3 completed	July to November 2023 24 November 2023	Energy Queensland
0.5	Strengthened strategic narrative, benefits and options analysis Draft 4 completed	December 2023 to January 2024 25 January 2024	Energy Queensland Deloitte
1.0	Final submitted to the Australian Energy Regulator	31 January 2024	Energy Queensland

## 2.4 Approvals

**Table 3: Document Approvals**

Position	Name/s	Signature	Date
<b>Approver: General Manager</b> GM Cyber and Information Security			30/01/2024
<b>Approver: General Manager</b> GM Grid Technology			30/01/2024
<b>Final Approver: EGM</b> A/Chief Information Officer			30/01/2024
<b>Final Approver: EGM</b> Chief Engineer			30/01/2024

## 3 STRATEGIC CONTEXT

### 3.1 Background

During the current 2020-25 regulatory control period, Energy Queensland established a dedicated Cyber Security Uplift Program (CUP). The program prioritises risk-based initiatives and expected compliance obligations under the *Security of Critical Infrastructure* (SoCI) Act.

Energy Queensland and other critical infrastructure service providers face growing cyber threats due to the technological trends for increased connectivity, increased adoption of energy storage, big data and cyber-physical assets (Internet of Things (IoT)), digitisation and automation of business models, and increased use of data analytics.

These trends will see continued growth in cyber-security threats through 2025 and beyond, including:

- **Ransomware** attacks have the potential to cause severe operational disruptions (including for operational technology (OT)) as well as significant financial and reputational harm. The 2021 attack on the ICT network of Queensland Government owned CS Energy caused major impact to the corporate network and requiring the connection to their OT network to be severed. The disruption affected core systems and processes for many weeks and required several months of recovery efforts<sup>2</sup>.
- **Malicious threat actors** continue to refine techniques to exploit the growing energy ecosystem and to take advantage of emerging technology and mobility<sup>3,4</sup>. Malicious threat actors are exploiting the rise of IoT and smart devices in the energy ecosystem, expanding their potential access points and potential to exploit vulnerabilities in internet-accessible devices (e.g., unpatched).
- **Data exfiltration** of personal data for extortion purposes or resale on the Dark Web. The recent number of high-profile data breaches in 2022 has heightened customer expectations on the privacy and security of their data, prompting regulators to respond with increasing obligations on, and penalties for, organisations holding customer personal data.
- **Supply-chain/third-party risk** as both criminal and state sponsored threat actors seek to leverage trusted access to targets within the energy supply chain. The electrification boom is expected to increase utility partnerships by 30%, attracting new start-ups and technology newcomers. This expansion could increase third-party attacks targeting vulnerable suppliers with weak security postures and infiltrating partner organisations through insufficient security standards, unmonitored access to sensitive information, and unsecured information systems.

Considering the dynamic threat landscape, the cyber-security trends anticipated to continue through 2025-30, and Energy Queensland's threat and risk assessments performed to-date,

<sup>2</sup> ACSC: URL: ACSC Annual Cyber Threat Report, July 2021 to June 2022 | Cyber.gov.au, 2022

<sup>3</sup> S. Acharya, Y. Dvorkin and R. Karri, 'Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable? ', 2020

<sup>4</sup> S. Soltan, P. Mittal and H. V. Poor, 'BlackIoT: IoT Botnet of High Wattage Devices Can Disrupt the Power Grid ', 2018

Energy Queensland has identified and prioritised the following major Cyber Security risks, shown in Table 4 below:

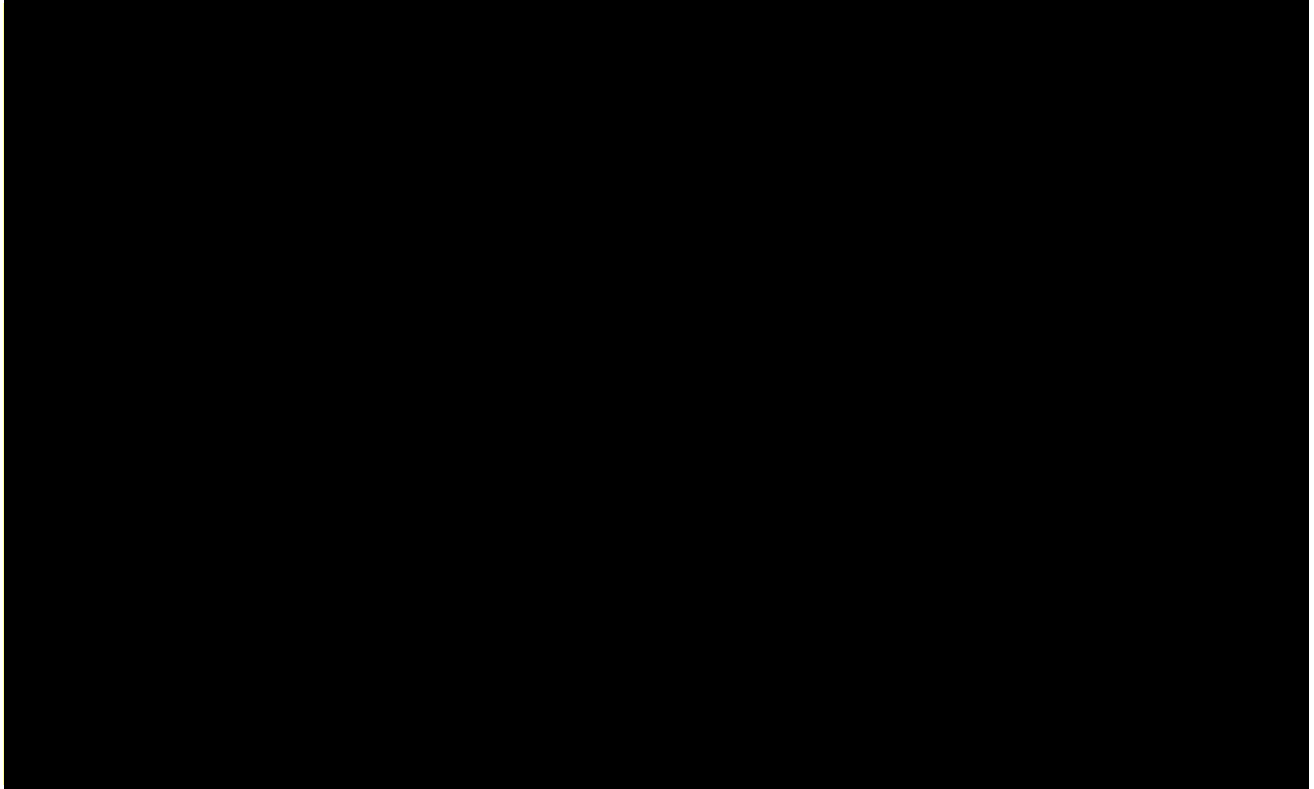
**Table 4: Current Energy Queensland Cyber Security Risks**

ID	Risk	Description of Risk
1	Ransomware	Energy Queensland business systems are unavailable for an extended period due to a ransomware attack, resulting in reputational damage, productivity and efficiency loss over several months.
2	Malicious critical infrastructure attack	Energex and Ergon Energy Network are unable to operate distribution networks safely or reliably because of cyber-attack on operational systems, resulting in network outages, reputational damage and extended manual network operations for several months.
3	Sensitive information loss	Sensitive information is stolen by a threat actor exploiting unauthorised access, damaging Energy Queensland's reputation and adversely affecting commercial activities, and exposing Energy Queensland to privacy and critical infrastructure compliance risk.
4	Technology supply chain compromise	A malicious threat actor leverages access via a trusted supply chain to execute a cyber-attack, resulting in network disruptions, commercial losses, safety incidents, reputational damage, privacy and/or critical infrastructure compliance breaches.
5	Insider threat	Confidential information is accessed or released publicly by a malicious insider using authorised access, harming Energy Queensland's reputation and commercial activities.
6	Long-term and undetected presence	A threat actor maintains persistence in Energy Queensland's digital environment eventually leveraging that access to deploy a cyber-attack, resulting in network disruptions, commercial losses, safety incidents, reputational damage, privacy and/or critical infrastructure compliance risk.

The CUP has prioritised those risk-based initiatives that will build resilient Cyber Security foundations and capabilities so that data and network services remain safe and reliable for customers, stakeholders, and the broader community. These initiatives have resulted in the active management of the Energy Queensland Cyber Security Risks with the improved forecast risk position at the end of this funding period to remain within the risk appetite of the Energy Queensland Board, as shown in Figure 1 below.



**Figure 1: Risk Reduction – 2020-25**



However, 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.

Furthermore, Energex and Ergon Energy Network are also required to meet regulatory and compliance obligations in relation to Cyber Security, as set out in Appendix 6.1, and the National Electricity Rules, as set out in Appendix 6.3.

This business case proposes a Cyber Security program for 2025-30, building upon CUP to maintain effective and appropriate security posture and aligning with Energex's and Ergon Energy Network's 2025-30 Regulatory Proposals. The CUP will continue to address both network and non-network ICT Cyber Security risks.

### 3.2 Electric Life 2032 and Investment Drivers

There are four investment drivers that underpin Energy Queensland's Electric Life 2032 ambition, vision and strategic priorities which will inform development of our expenditure plans and forecasts for the 2025-30 regulatory control period, as identified in Figure 2 and which are reflected in our Non-network ICT Plan 2025-30. The investment drivers are reliant on investment in information technology (IT) to deliver the information, infrastructure, security and capability across the breadth of our customer base, and to support the ecosystem of employees, contractors and suppliers who deliver the services that customers expect.

**Figure 2: Energy Queensland's Strategic Framework**

Ambition	#electriclife2032						
Vision	We energise Queensland communities						
Purpose	To safely deliver secure, affordable and sustainable energy solutions with our communities and customers						
Values	Safe	Knowledgeable	Innovative	Leading	Listening	Engaged	Diverse
Strategic building blocks & priorities	Enable				Evolve		
	<b>People &amp; culture</b> Continue to build a capable & productive workforce to ensure we deliver EQLs electric life ambition	<b>Keep the lights on</b> We will design, build and maintain a safe and reliable electricity network	<b>Financial sustainability</b> We will ensure funds spent are done so prudently and we will grow our revenue streams	<b>Safe</b> The safety of our people, customers and communities is our first priority	<b>Engage</b> Engaging our people, stakeholders, customers and communities	<b>Electrification</b> Further electrification of new loads and enabling the integration of renewables and energy solutions	<b>Environment</b> Reducing EQLs emissions, moving towards 70% renewables by 2032 and ensuring our assets are resilient
	Network resilience		Safe, efficient & affordable operations		Facilitate customer & community opportunities		Evolving grid infrastructure

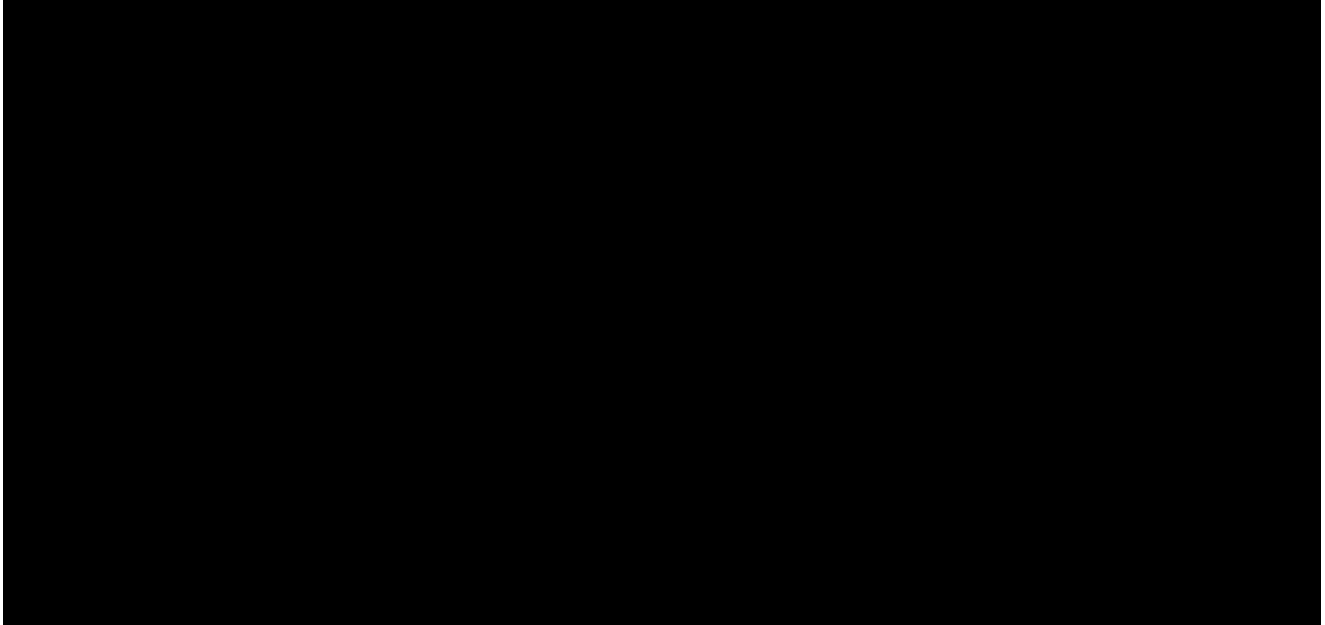
This business case addresses the network, and non-network ICT investment required to support the key investment driver 'Network resilience'. Energy Queensland is committed to providing a secure, dynamic and reliable electricity network for a rapidly changing operating environment and increased resilience to external factors that influence our planning decisions, including climate change and severe weather events. The Cyber Security ICT business case ensures our services are resilient and protected against security threats and provide improved capacity, response and recovery communications for customers and communities.

It is important to note that while Network resilience has been selected as the key investment driver, this business case is also critical in enabling the remaining drivers, 'Facilitate customer and community opportunities', 'Evolving grid infrastructure', and enabling 'Safe, efficient and affordable operations', none of which can be effective without appropriate Cyber Security capability uplift.

This business case identifies three sub-drivers within the key investment driver. For each of these sub-drivers, we have identified the challenges for investment, the benefits that can be realised, the objectives that can be met and outcomes achieved through the delivery of a strategic response (i.e., programs). The benefits and underpinning initiatives can be equally applied to the other investment drivers identified earlier in this business case.

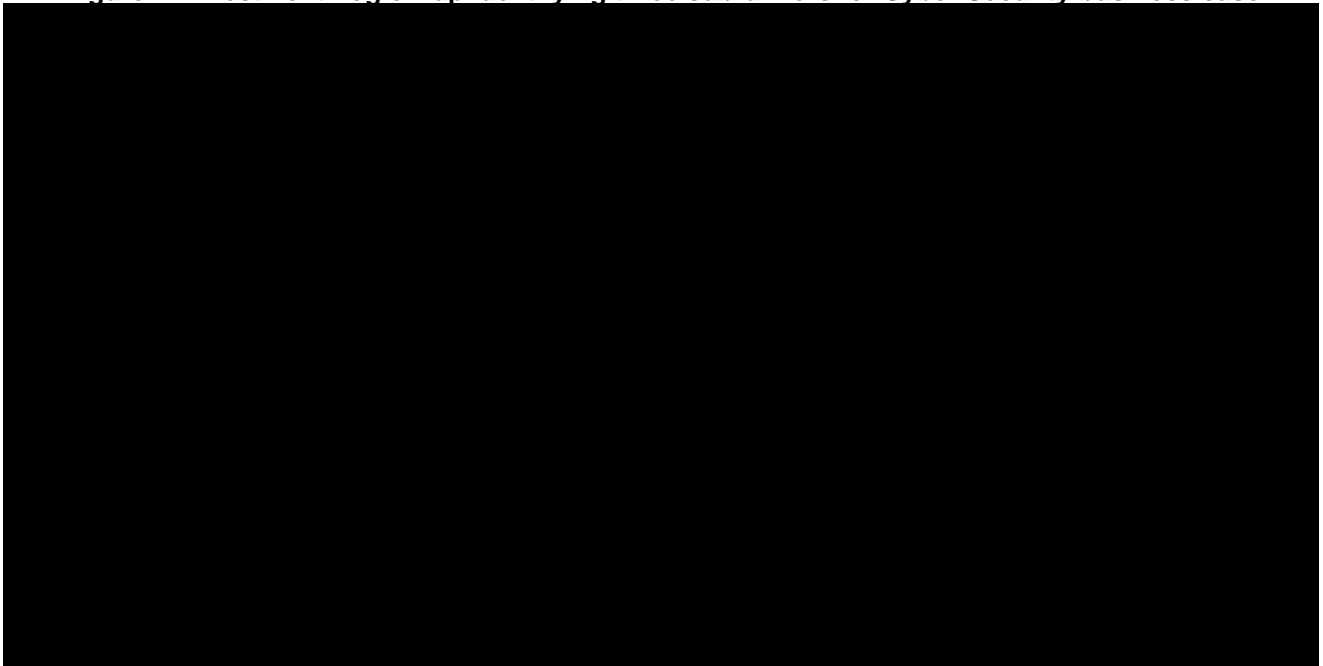
---

**Figure 3: Investment Logic Map for Cyber Security business case**



### 3.3 Drivers and Challenges

**Figure 4: Investment Logic Map identifying three sub-drivers for Cyber Security business case**



---

The three sub-drivers for investment for this business case are:

- **Maintaining critical service provision.** The electricity network is a critical asset, enabling economic activity and community safety, and must therefore be resilient and secure for Energy Queensland to continue to provide critical services to the community. This cyber-resilience and security must extend from the systems Energy Queensland uses to operate energy networks to the digital systems and information that underpin and enable safe and effective business operations.
- **Supporting evolution of the electricity grid.** The network has and continues to undergo major transformation in the digitisation, automation, and optimisation of critical energy systems (through adoption of emerging technologies incl. artificial intelligence, predictive analytics, robotics), and increasing participation of energy consumers turned ‘prosumers’ through adoption of distributed energy resources (DER) and uptake of energy storage. This is resulting in larger, more comprehensive data sets and digital surfaces, providing new and more complex opportunities for cyberattacks. Energy Queensland must ensure it has the secure, adaptable Cyber Security capabilities across both, IT and OT, so we can safely and confidently leverage intelligent grid solutions for the operational management of distribution network stability, reliability, and power quality.
- **Addressing increasingly more sophisticated and malicious attacks.** Increasing interconnectedness and digitalisation is driving more possible attack vectors, with the number of cyber-attacks on critical infrastructure (8% of all incidents responded to by the Australian Cyber Security Centre (ACSC) in 2021-22)<sup>5</sup> on the rise, exacerbated by state actors weaponising critical infrastructure in political conflicts regionally and globally. Top-tier ransomware groups are continuing to target high-profile/high-value Australian entities, which can cause extensive disruption to core systems and processes, corporate and OT networks.

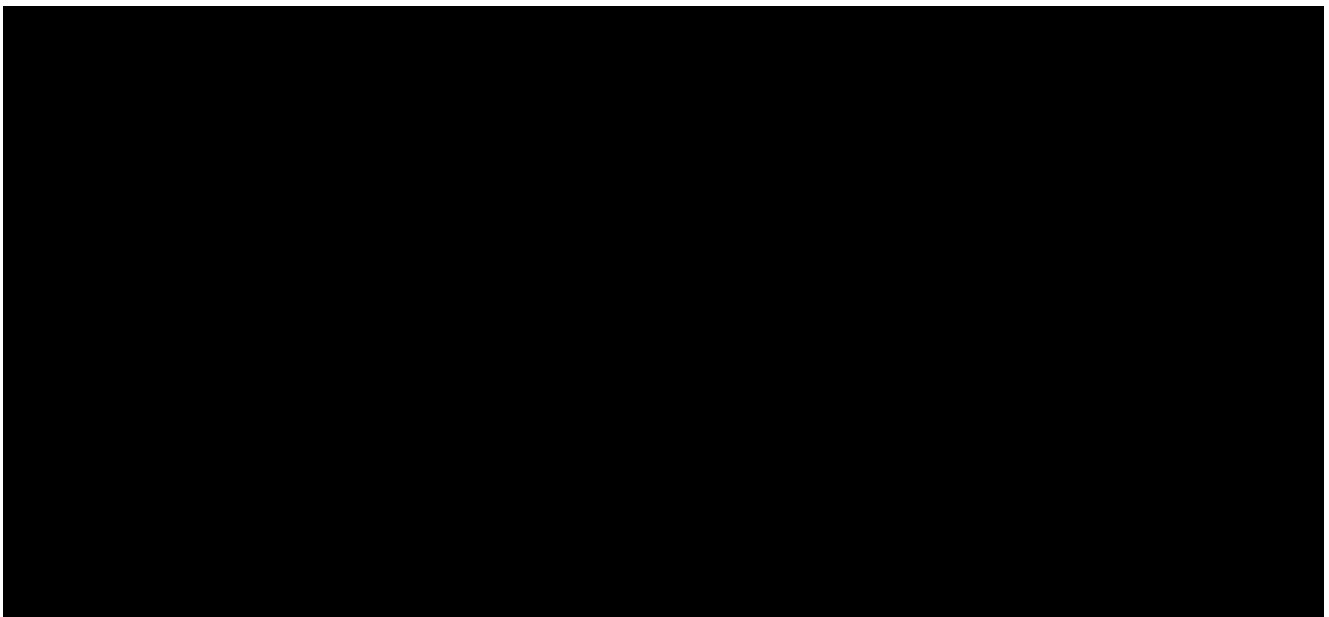
At the same time, Energy Queensland must be prepared for and respond to changes in its regulatory environment, particularly in relation to Cyber Security and resilience. The recently introduced Security of Critical Infrastructure Act and the Cyber Security obligations on entities is expected to continue to be tightened throughout 2025-30.

---

<sup>5</sup> CyberArk, The Identity Security Company: URL: Australia’s Growing Focus on Critical Infrastructure Cybersecurity in 2023 | <https://www.cyberark.com/>, 2023

### 3.4 Way Forward and Benefits

Figure 5: Investment Logic Map identifying four benefit categories that address the drivers



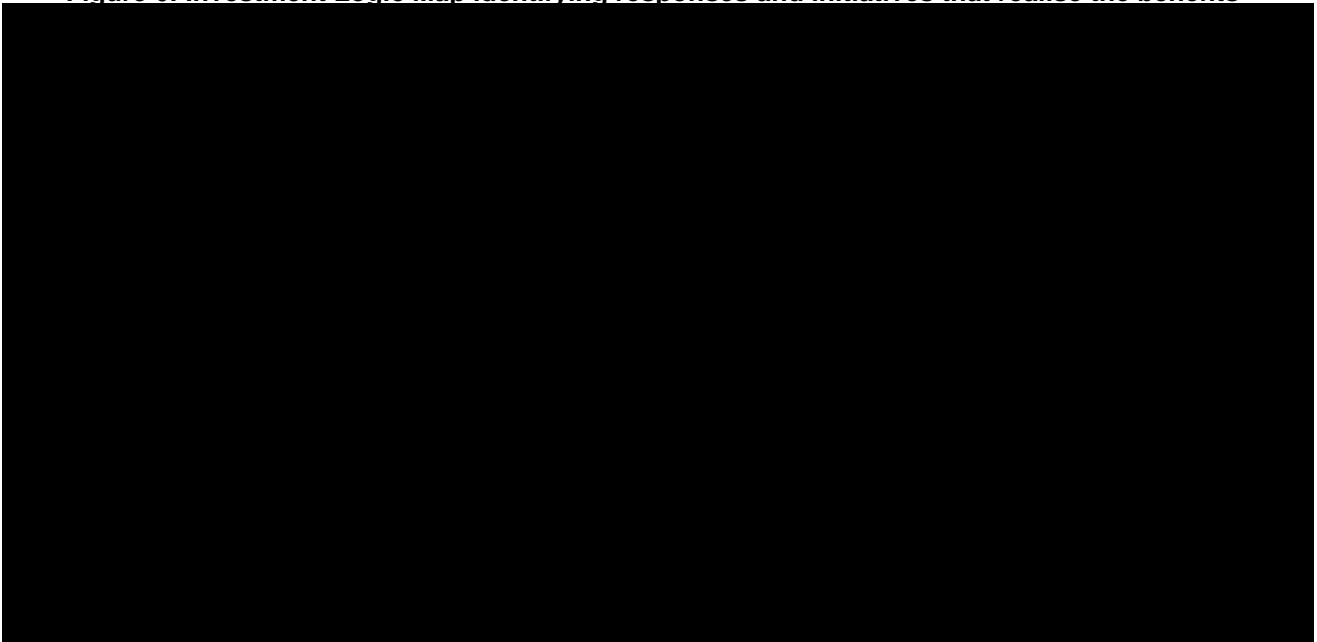
We have identified the following benefit categories that can be realised in response to the identified driver and sub-drivers. Please refer to section 4.3 and 6.2 for an analysis of the quantifiable and qualitative benefits associated with the investment.

- **Cost Avoidance.** Investment in Cyber Security can avoid or reduce the magnitude of cyber incidents. Reducing the likelihood or consequences of Cyber Security incidents reduces direct costs such as productivity loss and restoration costs and indirect costs such as service disruptions, regulatory fines or penalties and the cost of implementing business continuity arrangements.
- **Risk and Compliance.** Energy Queensland has a conservative approach to cyber risk and Cyber Security investment is critical to maintaining cyber risk within appetite. As both an operator of critical infrastructure and the custodian of a significant volume of personal data, Energy Queensland must also maintain compliance with security regulations.
  - Preparedness for regulatory change: We anticipate, through our preferred option, that we will meet future compliance obligations related to critical infrastructure assets so far as reasonably practical.
  - Integration of Cyber Security risk: Cyber risk will be fully integrated as part of business risk and continuously assured and managed to within appetite through the Cyber program of work.

- 
- **Future Proof Capabilities.** Energy Queensland's Cyber Security arrangements must move at pace with the consumer-led transformation of the electricity supply system and address a complex and challenging Cyber Security environment:
    - Secure enablement of future grid: Ability to enable and support future grid securely (e.g., data sharing, new connection).
    - Improved organisational resilience: Organisational resilience delivered through further development of incident response scenarios and tooling to enhance situational awareness, organisational response and recovery will occur.
    - Ability to anticipate and respond to changes in the threat landscape: Ability to adapt to a growing and largely unknown threat landscape as threat actors become more sophisticated and Energy Queensland's attack surface area expands.
  - **Effective Cyber Operations.** Essential to the Cyber Security and resilience of Energy Queensland's digital and intelligent grid ecosystems, and to enable Energy Queensland's digital transformation.
    - Increase in risk detection and reduction in response times: Significant focus on automation of controls and the use of Artificial Intelligence will significantly reduce detection and response times despite the increased ecosystem.
    - Protection of Energy Queensland assets: Energy Queensland assets in customer homes and businesses will be protected despite growing threats and exposure and the ability to transform the distribution network safely will maximise service reliability.
    - Promotion of cyber aware culture: There will be a continued development of a cyber aware and resilient organisational culture.
    - Real-time situational awareness: Convergence of Security and Operations centres will provide real time situational awareness across the ecosystem with faster time to detect, respond, and contain.
    - Supportability of systems: Existing Cyber Security systems remain reliable, maintained, patched, and supported.
    - Protection of customer data: Customer data will be protected at rest and in transit with enhanced identity controls and methods to monitor and prevent data exfiltration.

### 3.5 Initiatives and Outcomes

Figure 6: Investment Logic Map identifying responses and initiatives that realise the benefits



The following initiatives are proposed to meet our investment drivers, address the development challenges, and realise the benefits identified.

- **Capability evolution.** Maintain pace with internal and external environment.
  - Maintain operations: [Redacted]
  - Keep Cyber Security technology platforms current and in line with industry trends: [Redacted]

- 
- Evolve existing Cyber Security capabilities and risk controls: [REDACTED]
    - [REDACTED]
    - [REDACTED]
    - [REDACTED]
  - **Securing intelligent grids.** Cyber security will need to 'step up' and secure the vast volumes of information, intelligent devices, automated decision making at scale accounting for the wide range of third parties that will characterise intelligent grids.
    - Enhance machine, energy partner, and supply chain identity and access management capabilities: [REDACTED]
    - Enhance customer identity and access management capabilities: [REDACTED]



- 
- **Securing digital ecosystems.** Cyber security will need to enable digital transformation by securing complex hybrid environments, a mobile workforce, and large volumes of information.

- Strengthen Cyber Security capabilities to support intelligent grid resilience:

[Redacted content]

- Converge the Cyber Security Operations Centre capabilities across Information Technology and Operational Technology:

[Redacted content]

---

## 4 INVESTMENT OPTIONS

### 4.1 Options Description

Energy Queensland conducted an initial analysis of Cyber Security risk exposure, identifying five scenarios to set an aspirational target for cyber control maturity.

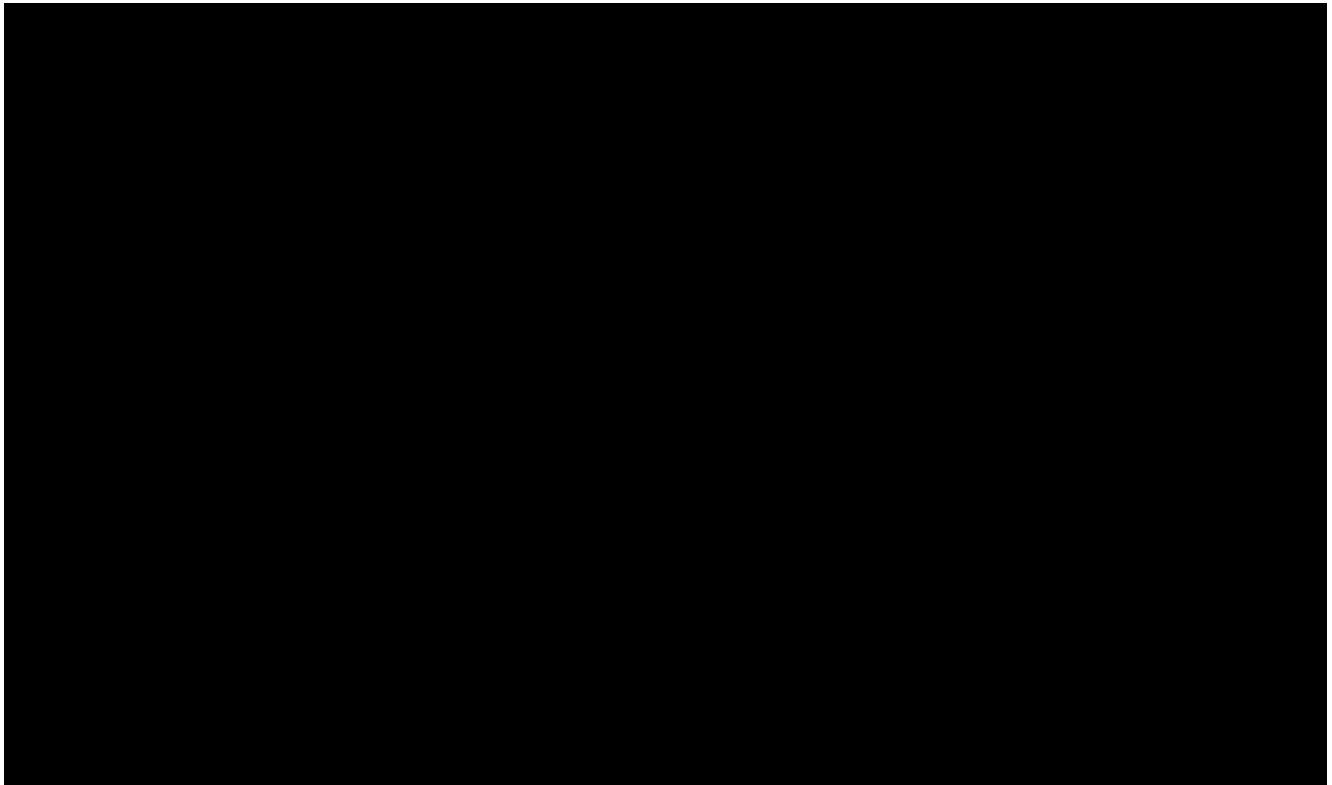
Scenario 1 was a minimal investment scenario, maintaining only existing Cyber Security capabilities. However, as Cyber Security threats mature, Energy Queensland's risks become unaddressed. Additionally, increased regulatory obligations and inadequate investment in controls could result in non-compliance with SoCI regulations during 2025-30, thus discarding this scenario.

Scenario 2 aimed to achieve Security Profile 3 under the Australian Energy Sector Cyber Security Framework (AESCSF) by targeting high cyber control maturity across all assets. However, a cost and benefit analysis revealed this scenario was unfavourable, compared to other scenarios and was discarded from consideration.

The remaining three scenarios were developed into the three options for consideration in this business case. These three options address the drivers outlined earlier, and deliver on the benefits described above, for this business case.

- Option 1: Evolve current Cyber Security capabilities.
- Option 2: Evolve current Cyber Security capabilities and provide basic capability uplift to support grid evolution and
- Option 3: Strengthen all current, and build new, Cyber Security capabilities.

**Figure 7: Initiatives mapped to options**



**Option 1: Evolve current Cyber Security capabilities**

The focus of this option is to maintain compliant Cyber Security operations and technology platforms and address the risks of ransomware and malicious critical infrastructure attack, to ensure these are kept within the Board's risk appetite.

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted]

[Redacted]

[Redacted]

### Option 2: Evolve current Cyber Security capabilities and provide basic capability uplift to support grid evolution

The focus of this option is to maintain compliant Cyber Security operations and technology platforms and address the risks of [Redacted], to ensure these are kept within the Board's risk appetite.

[Redacted]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

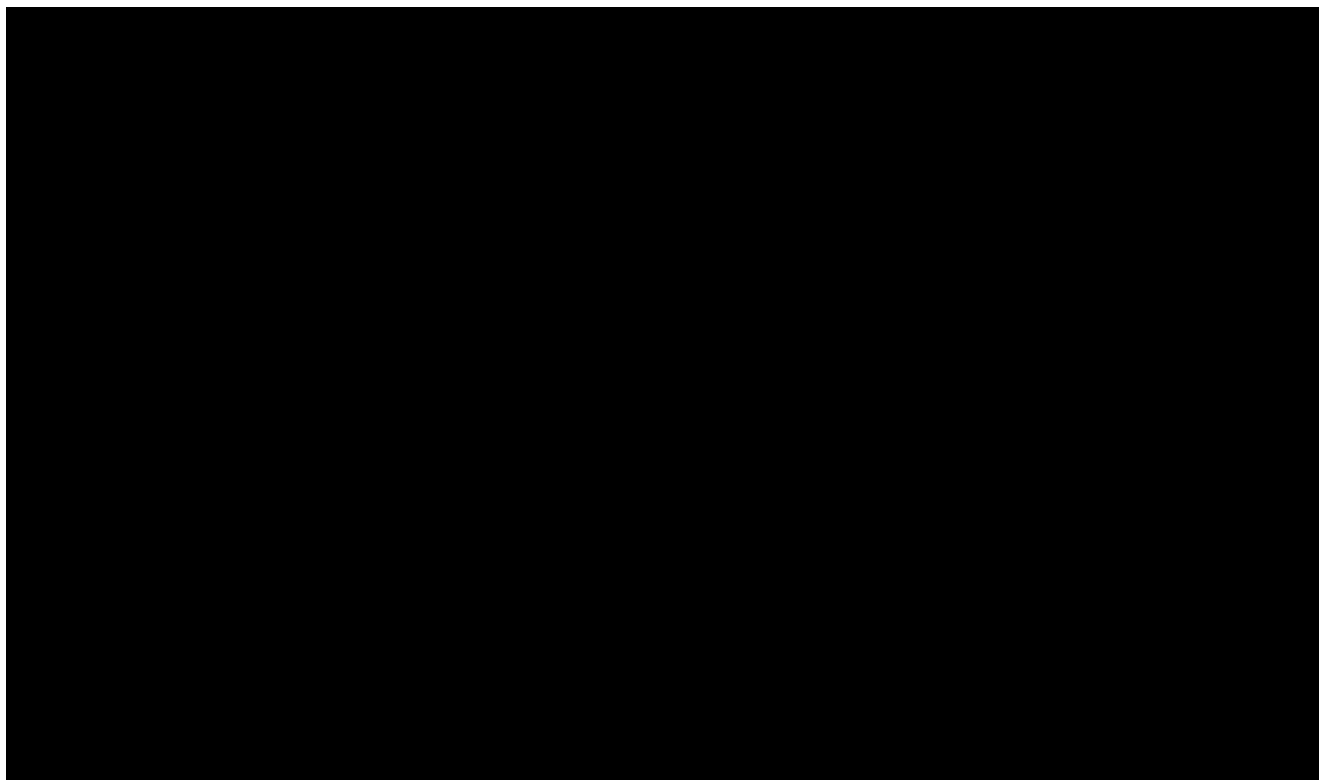
[Large redacted text block]

---

### Option 3: Strengthen all current, and build new, Cyber Security capabilities

The focus of this option is to strengthen all Cyber Security capabilities and enable effective risk management within appetite, into the future, across all services.

[Redacted content]



## 4.2 Criteria Description

The options were reviewed across the following five criteria to arrive at an overall assessment.

- **Compliance expectations addressed by option:** Assesses the ability to meet expected Cyber Security regulations and readiness for future regulatory changes. For this criterion, a yes or no scoring is provided.
- **Risk mitigation associated with option:** Assesses the qualitative likelihood of each option mitigating Energy Queensland corporate risks (i.e., probability of risk occurring). For this criterion, a high / medium / low risk mitigation scoring is provided.
- **Financial benefits associated with option:** Assesses the financial benefits delivered to Energy Queensland, and the broader community from each option. For this criterion, only the total value of the financial benefits is included (if any).
- **Non-financial/non-quantified benefits associated with option:** Assesses the non-financial/not-quantified benefits delivered to Energy Queensland, and the broader community from each option. For this criterion, a limited / partial / full benefit realisation scoring is provided.
- **Costs associated with option:** Assesses the quantitative non-recurrent and recurrent (capital and operating) costs associated with each option. For this criterion, only the total value of expenditure is included.

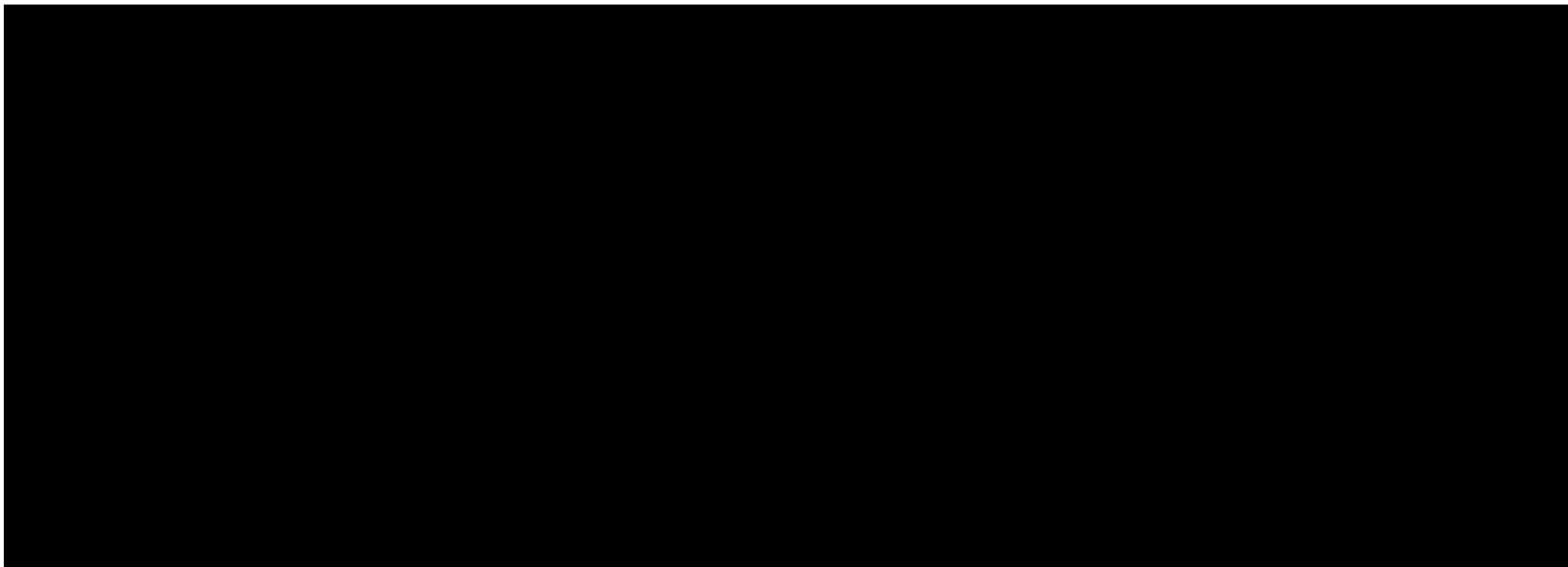
Table 5 provides a summary of the assessment of the three options, to demonstrate the recommended option for investment.

---

### 4.3 Summary of Options Analysis

Table 5 summarises the analysis of the three options. Detailed analysis of each option against the criteria is in the Appendix.

**Table 5: Summary of Options Analysis**



The content of Table 5 is redacted with a large black rectangle.





## 4.4 Recommended Option

The primary objective of the Cyber Security operation is to maintain critical service provision, support the evolution of the electricity grid and address the increasingly more sophisticated and malicious attacks on critical infrastructure.

Option 3 'Strengthen all current, and build new, Cyber Security Capabilities' is the recommended option, as it provides the most prudent and efficient long-term investment outcome when securing Energy Queensland's critical infrastructure assets and data in line with customer and community expectations.

This option also best enables Energy Queensland's core Cyber Security capabilities so that it will be compliant with its legislative obligations and is adaptive and flexible to the ever-changing threat landscape and requirements of the future energy grid. This option also best underpins all four investment drivers identified in the Electric Life Strategy, not just Network Resilience.

While Option 3 is recommended, it is dependent upon:

- The Data & Intelligence business case for the data classification governance, management and sharing capabilities that complement the Cyber Security controls to ensure that our information is safe and secure.
- The Digital Foundations business case for the infrastructure, technologies, integration and service management platforms underpinning all other non-network ICT business cases; investments to improve data protection in hybrid cloud environments and IoT device management; and DevOps, monitoring, and service management capabilities integrated with Cyber Security operations.
- All other non-network ICT business cases for the ICT asset management activities (e.g., system upgrades and legacy system replacements) that are required to ensure that contemporary Cyber Security controls can continue to be applied effectively, to keep our customers, digital systems, our staff and our distribution network safe.

- 
- Network business cases for OT asset management / renewal to ensure that contemporary Cyber Security controls, as defined in the AESCSF and NIST Frameworks, can continue to be applied effectively, and that our Network remains reliable, secure, and is safe from Cyber Security attacks.

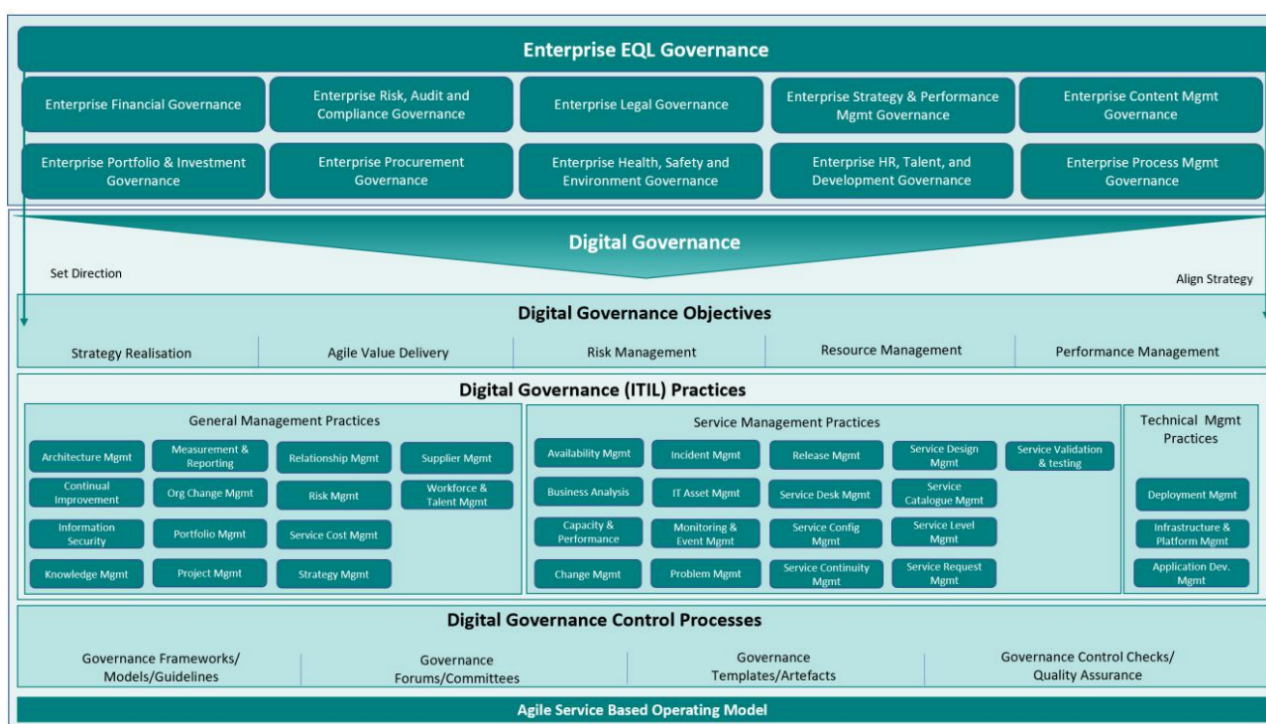
## 5 IMPLEMENTATION OF RECOMMENDED OPTION

To realise the significant benefits identified through Option 3, we will implement this investment in line with our standard governance and operating models, as described below.

### 5.1 Governance Arrangements

The initiatives will comply with the Digital Governance Framework (an element of the Corporate Governance Model). For further details, please refer to the Non-network ICT Plan 2025-30.

**Figure 11: Digital Governance Model**



In addition to this, the Digital Operating Model also incorporates the Scaled Agile Framework ways of working, which provides the approach to the day-to-day delivery of IT services (the how), and incorporates layers of operational governance to Digital planning, prioritisation, and execution activities. This links through to the governance objective of 'Agile Value Delivery'. For further details, please refer to the Non-network ICT Plan 2025-30.

### 5.2 Change Impact

The magnitude of the change impact of the initiatives in this business case will depend on how the step changes are planned. Our iterative agile program delivery approach will break the step changes down into small to medium change increments, each of which will require consultation, process changes and upskilling of affected internal and external stakeholders. The integrated design and delivery approach will support a smooth transition of new capabilities into BAU processes to ensure uninterrupted service delivery to our customers.

Specific key change impacts are:

- [Redacted]
- [Redacted]
- [Redacted]

### 5.3 Delivery Roadmap

The delivery of the recommended program of work will be managed through the establishment of a Cyber Program which will be based on the same principles as Energy Queensland’s Cyber Uplift Program (CUP) which has been running since 2021.

All existing initiatives in CUP are underpinned and prioritised by a risk-based approach which is revalidated regularly, meaning that initiatives that help mitigate higher risks are prioritised for delivery first. Delivery of CUP includes a combination of both internal and external delivery resources and implementation partners led by a dedicated program director and has included the embedding managed service operations for ongoing support.

Because CUP’s approach to Cyber Security initiatives is risk-based, it enables the program to pivot and respond to heightened risks in a changing threat landscape.

The initiatives in this business case will deliver value and mitigate risk using a continuous iterative agile project management methodology. Business Owners, Platform Managers and Platform Architects across both non-Network and Network areas will consciously and continuously prioritise the initiatives through continuous review of the risk profile as well as enabling continuous delivery of customer value. Key priorities and decisions are also discussed and decided on in the monthly Strategic Security and Resilience Committee Meeting chaired by the CEO and attended by selected members of the Executive Leadership Team.

An important component of successfully embedding Cyber Security changes in the organisation is to establish

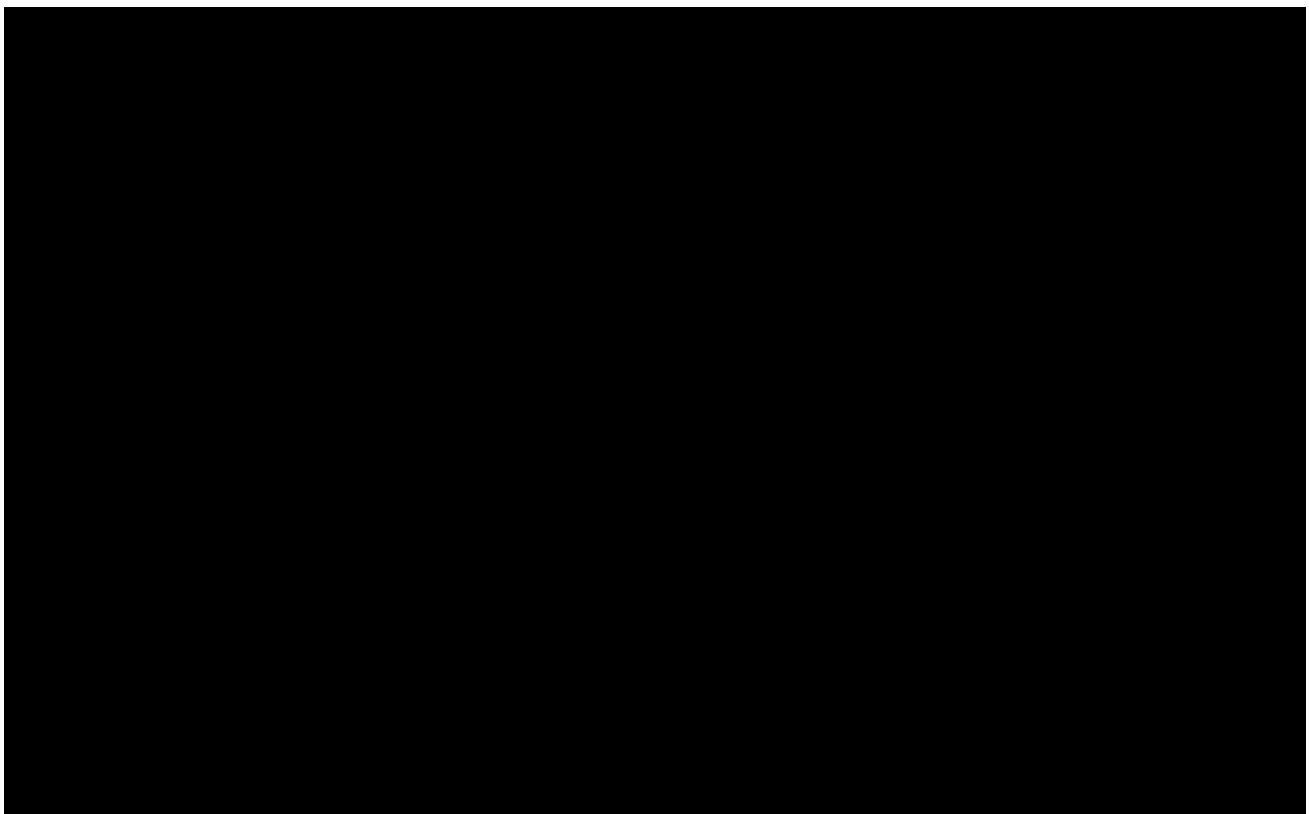


The below planning roadmap represents the current view of how these initiatives will be prioritised and delivered over the 2025-30 regulatory control period. This planning roadmap will be continuously refined throughout the regulatory control period.

While assumptions of the expected external drivers, triggers, timing, and growth indicators in this industry transition are documented, Energy Queensland plans to reassess and implement the initiatives within this business case in anticipation of the actual customer, business, and industry needs.

Refer to Appendix 6.5 Delivery Risks and Controls, for an overview of the delivery risks, associated consequences, and proposed controls attached to the recommended option.

**Figure 12: Planning Roadmap for Cyber Security**



<sup>6</sup> Australian Government, Department of Climate Change, Energy, the Environment and Water, 'Australian Energy Sector Cyber Security Framework – Domain 'Workforce Management' ', 2023

## 5.4 Investment Benefits

The recommended option delivers all the benefits described in section 3.4.

The quantitative benefits to be realised from this investment are \$262.8M (present value \$213.8M). Please refer to Section 6.2 for a detailed description of the financial and non-financial benefits.

## 5.5 Investment Costs

The categories of investment are shown in Table 6.

**Table 6: Total Costs Overview (\$M, real December 2022)**

Category	Type	FY26	FY27	FY28	FY29	FY30	TOTAL	NPV
ICT capex	Recurrent	█	█	█	█	█	4.6	4.0
ICT capex	Non-recurrent	█	█	█	█	█	51.8	43.7
Network capex	Recurrent	█	█	█	█	█	13.9	11.7
Network capex	Non-recurrent	█	█	█	█	█	28.5	24.5
ICT opex	N/A	█	█	█	█	█	55.7	46.5
Network opex	N/A	█	█	█	█	█	19.4	16.2
<b>TOTAL</b>		█	█	█	█	█	<b>173.8</b>	<b>146.6</b>

## 5.6 Financial Summary

Table 7 summarises the overall financial position of the recommended option (Option 3), with NPV sensitivity analysis captured in Table 8.

**Table 7: NPV Overview (\$M, real December 2022)**

Net Present Value	Type	Option 3
ICT capex	Recurrent	(4.0)
ICT capex	Non-recurrent	(43.7)
Network capex	Recurrent	(11.7)
Network capex	Non-recurrent	(24.5)
ICT opex	N/A	(46.5)
Network opex	N/A	(16.2)
Benefits	N/A	213.8
<b>Commercial NPV</b>		<b>67.3</b>

**Table 8: NPV Sensitivity (\$M, real December 2022)**

Net Present Value	Discount Rate		Benefits	
	+1%	-1%	125%	75%
Recommended option (Option 3)	62.0	72.9	120.7	13.8



## 6 APPENDICES

### 6.1 Applicable Compliance Requirements

Energy Queensland is required to meet regulatory and compliance obligations within its Cyber Security capabilities in relation to its corporate non-network ICT systems as set out below.

**Table 3 Applicable Compliance Requirements Overview**

Obligation	Description of Requirement
<b>Security of Critical Infrastructure Act 2018 (SoCI Act)</b>	<p>The SoCI Act places a number of obligations on critical infrastructure entities. The most notable is a requirement for Energex and Ergon Energy Network to develop and maintain a Critical Infrastructure Risk Management Program (CIRMP) to prevent Cyber Security risks from occurring and to minimise or eliminate, so far as reasonably practicable, the occurrence and impacts of Cyber Security incidents. SoCI also requires entities to comply with a security management framework and specific maturity targets of a selected framework. It is expected that over the course of the 2025-30 regulatory control period, obligations under the SoCI Act will become more onerous.</p> <p>The SoCI Act seeks to manage the complex and evolving national security risks of sabotage, espionage and coercion posed by foreign involvement in Australia's critical infrastructure.</p> <p>The Act applies to 22 asset classes across 11 sectors including the energy sector and requires us to comply with certain obligations set out in the Act.</p>
<b>Privacy Act 1988, Information Privacy Act 2014</b>	<p>As specified in the <i>Privacy Act 1988</i> (Privacy Act), Energy Queensland is required to maintain strong controls and security on the accessibility of customer data as well as ensuring appropriate availability of data. Keeping Energy Queensland's critical systems up to date, supported and secured is a key enabler of maintaining these controls. Having appropriate controls and Cyber Security systems in place is a key enabler to appropriately securing information and reducing the risk of a data breach.</p>
<b>National Electricity Law and National Electricity Rules</b>	<p>The National Electricity Law (NEL) requires Energex and Ergon Energy Network to promote efficient investment in, and efficient operation and use of electricity services for the long-term interests of consumers of electricity with respect to price, quality, safety, reliability, and security of supply of electricity as per the National Electricity Objective (NEO).</p> <p>The operating and capital expenditure objectives set out in the National Electricity Rules (NER) require Energex and Ergon Energy Network to maintain both the quality, reliability, and security of supply of standard control services and the reliability and security of the distribution network.</p>
<b>The Australian Energy Cyber Security Framework (AESCSF)</b>	<p>Energex and Ergon Energy Network must ensure their critical non-network ICT systems are kept up to date, supported and secured to meet the AESCSF maturity targets established under SoCI rules. There is potential that this will become a licensing requirement in the future and therefore the assets must be maintained to enable licenses to be kept up to date.</p>
<b>Credit card payment regulations/ payment privacy</b>	<p>Energy Queensland must comply with a number of regulations to ensure the security of credit card payments and payment privacy. The merchant bank sets the terms of service that Energy Queensland must meet. Further, Energy Queensland must meet the obligations under the Australian Privacy Principles in the Privacy Act.</p>

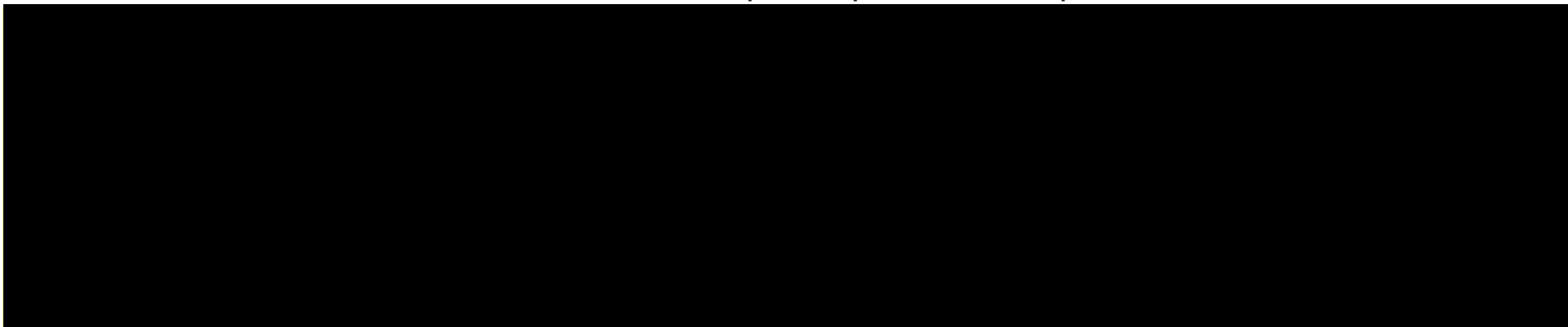
## 6.2 Options Analysis

This section summarises the options against the criteria analysed in defining the investment proposed in this business case.

### Compliance expectations addressed by option

This criterion assesses the ability to meet expected Cyber Security regulations and readiness for future regulatory changes. The table below outlines the assessment against the three options.

**Table 12: Addressment of compliance expectations across Options**

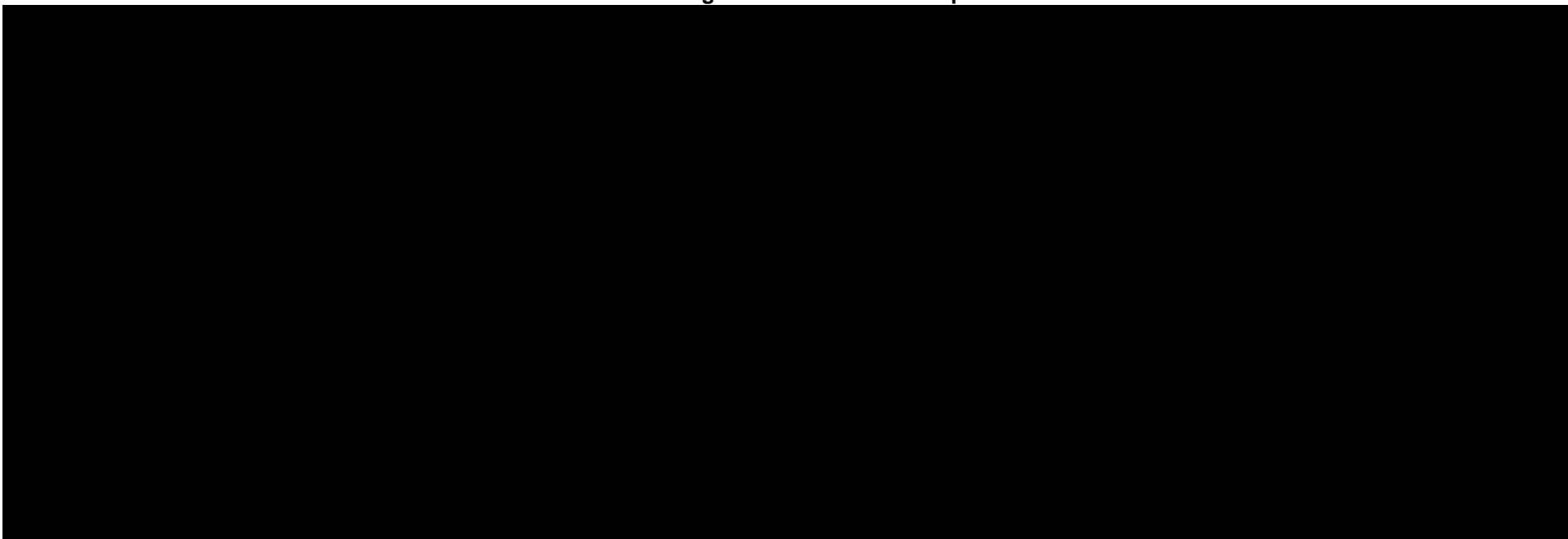


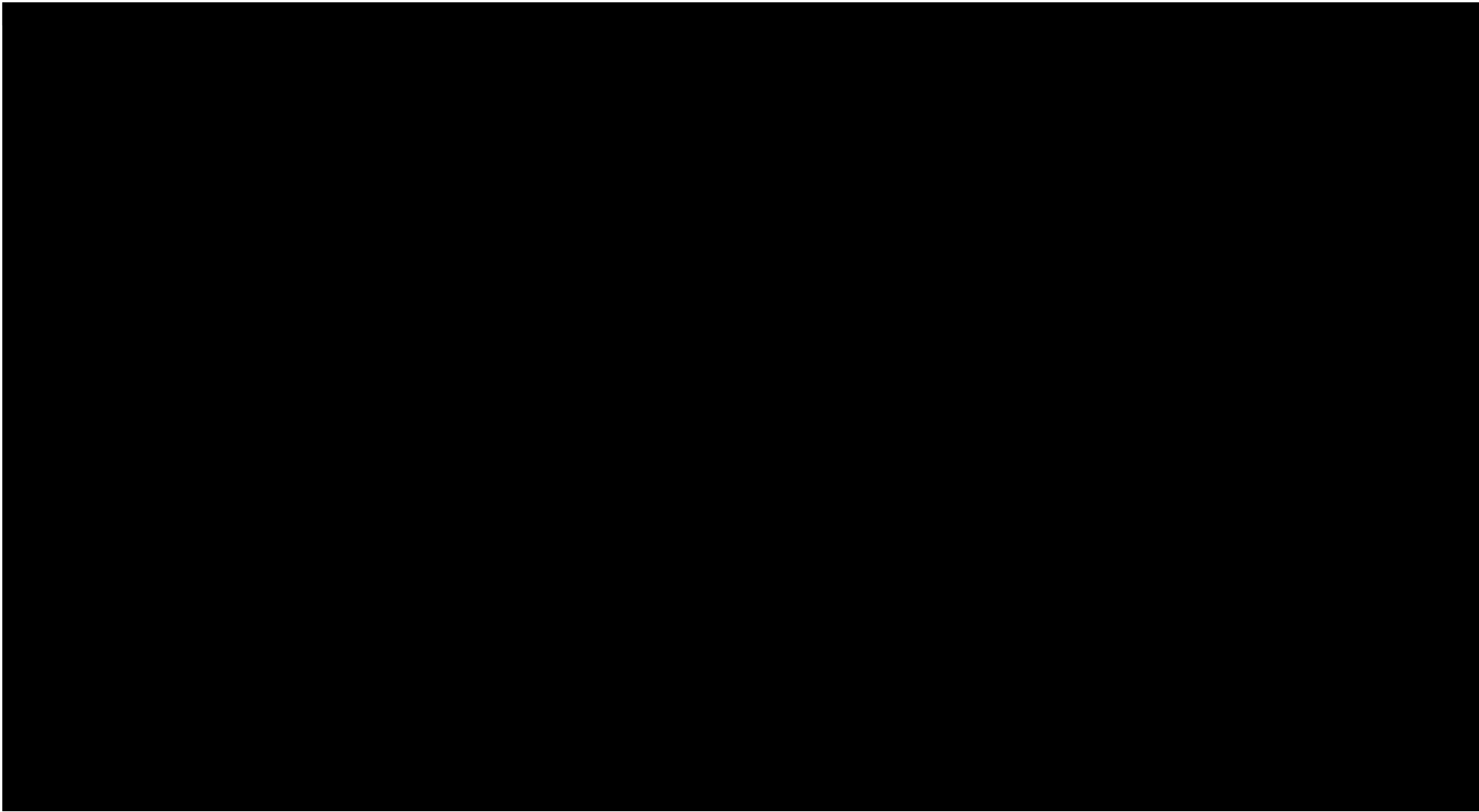
---

### Risk mitigation associated with option

This criterion assesses the qualitative likelihood of each option mitigating Energy Queensland corporate risks (i.e., probability of risk occurring). The table below outlines the assessment against the three options.

**Table 13: Mitigation of risks across Options**





## Financial benefits associated with option

This criterion assesses the financial benefits delivered to Energy Queensland, and the broader community from each option. The table below outlines the results of the analysis against the three options.

**Table 14: Financial benefits associated with Options (\$M)**

Benefit category	Option 1: Evolve Current Cyber Security Capabilities	Option 2: Evolve Current Cyber Security Capabilities and provide basic capability uplift to support grid evolution	Option 3: Strengthen all current, and build new, Cyber Security Capabilities
Cost Avoidance	212.8	244.5	262.8

For Net Present Value investment analysis three adverse event scenarios have been considered and modelled as cost avoidance benefits. These are:

[REDACTED]

[REDACTED]

[REDACTED]

The consequences of each of these scenarios were modelled using the following assumptions:

[REDACTED]

[REDACTED]

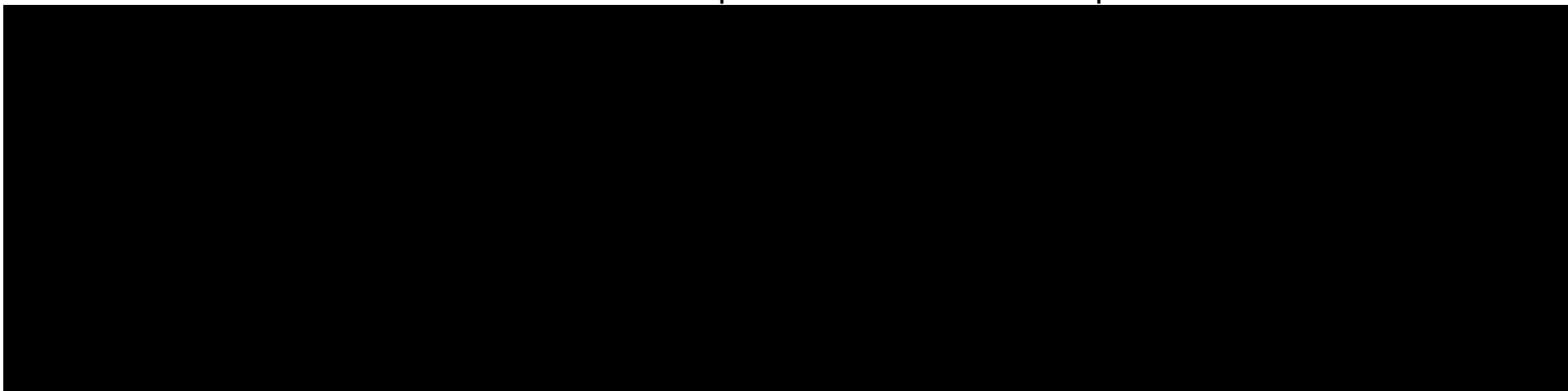
For each scenario an assessment of relative likelihood (using Energy Queensland's risk evaluation matrix) was then conducted and analysed to determine a final combined financial impact which was used as input into a cost avoidance calculation.

---

### Non-financial/not-quantified benefits associated with option

This criterion assesses the non-financial/not-quantified benefits delivered to Energy Queensland, and the broader community from each option. The table below outlines the assessment against the three options.

**Table 15: Non-financial/not-quantified benefits associated with Options**



## Costs associated with option

This criterion assesses the quantitative non-recurrent and recurrent (capital and operating) costs associated with each option. The table below outlines the assessment against the three options.

**Table 16: Costs associated with Options (\$M, real December 2022)**

Costs category	Option 1: Evolve Current Cyber Security Capabilities	Option 2: Evolve Current Cyber Security Capabilities and provide basic capability uplift to support grid evolution	Option 3: Strengthen all current, and build new, Cyber Security Capabilities
Recurrent capital expenditure	18.5	18.5	18.5
Non-recurrent capital expenditure	53.0	74.5	80.3
Operating expenses	67.3	72.8	75.1
<b>Total</b>	<b>138.8</b>	<b>165.7</b>	<b>173.8</b>

## 6.3 Alignment with the National Electricity Rules

**Table 17: Recommended Option's Alignment with National Electricity Rules**

NER capital expenditure objectives	Rationale
<p><b>A building block proposal must include the total forecast capital expenditure which the DNSP considers is required in order to achieve each of the following (the capital expenditure objectives):</b></p>	
<p><b>6.5.7 (a) (1)</b> <b>meet or manage the expected demand for standard control services over that period</b></p>	<p>The recommended Option results in the lowest residual Cyber Security risk to Energex and Ergon Energy Network's distribution network during the 2025-30 regulatory control period. Cyber security impacts all aspects of distribution network and service management and is critical to ensuring expected demand for standard control services can be met during this period cyber-attacks.</p>
<p><b>6.5.7 (a) (2)</b> <b>comply with all applicable regulatory obligations or requirements associated with the provision of standard control services;</b></p>	<p>The recommended Option will ensure Energex and Ergon Energy Network complies with all applicable regulatory obligations, including Energy Queensland license conditions, the SOCI Act and the Privacy Act.</p>
<p><b>6.5.7 (a) (3)</b> <b>to the extent that there is no applicable regulatory obligation or requirement in relation to:</b></p> <ul style="list-style-type: none"> <li><b>(i) the quality, reliability or security of supply of standard control services; or</b></li> <li><b>(ii) the reliability or security of the distribution system through the supply of standard control services,</b></li> </ul> <p><b>to the relevant extent:</b></p> <ul style="list-style-type: none"> <li><b>(iii) maintain the quality, reliability and security of supply of standard control services; and</b></li> <li><b>(iv) maintain the reliability and security of the distribution system through the supply of standard control services</b></li> </ul>	<p>The recommended Option implements the strongest cyber controls to ensure that standard control services are maintained, and Energex and Ergon Energy Network's distribution network is protected from potential cyber-attacks. These controls ensure that Energex and Ergon Energy Network can continue to maintain the quality, reliability and security of supply required for standard control services during 2025-30.</p>
<p><b>6.5.7 (a) (4)</b> <b>maintain the safety of the distribution system through the supply of standard control services.</b></p>	<p>The recommended Option provides the lowest risk pathway to ensuring continued and quality supply of standard control services, thereby ensuring safety of the distribution system is maintain during 2025-30.</p>
NER capital expenditure criteria	Rationale
<p><b>6.5.7 (c)</b> <b>the AER must be satisfied that the total forecast capital expenditure for the regulatory control period reflects each of the following capital expenditure criteria:</b></p>	



NER capital expenditure objectives	Rationale
<p>(1) the efficient costs of achieving the capital expenditure objectives;</p> <p>(2) the costs that a prudent operator would require to achieve the capital expenditure objectives; and</p> <p>(3) a realistic expectation of the demand forecast, and cost inputs required to achieve the capital expenditure objectives.</p>	<p>The recommended Option meets the regulatory capital expenditure objectives and maintains Energex and Ergon Energy Network’s Cyber Security risk profile within Energex and Ergon Energy Network’s risk appetite limit.</p> <p>A detailed cost-benefit analysis above provides sufficient evidence for Energex and Ergon Energy Network’s preference for the preferred Option. Costs were estimated using historical costs, knowledge of recent market procurement for equivalent services and products, as well as specialist advice from subject matter experts.</p> <p>Risks were similarly analysed with a critical methodology to ensure reasonable assumptions and forecasts were accounted for. The recommended Option results in the lowest residual Cyber Security risks for Energex and Ergon Energy Network’s distribution network and customers during the 2025-30.</p>

## 6.4 Assumptions

The enterprise assumptions on which the need for this business case has been assessed are documented in the ‘RDP 2025 Project – Shared Assumptions’ document. In addition, assumptions are being made for this business case.

Table 18 explores the assumptions that are applicable for the recommended option only.

**Table 18: Assumptions Overview**

Assumption Description	Impact if assumption proved invalid	How will the assumption be assessed?
<p><b>Growth / change rates in the 2025-30 regulatory control period, based on Enterprise Assumptions on growth / change rate in our grid (e.g., customer numbers, DER capacity, EVs, dynamic connections, number of Intelligent Devices etc.) and strategic direction (such as the rollout of distribution network support BESS which is already underway).</b></p>	<p>Altered expenditure profile to reflect actual change rates</p>	<p>Continued monitoring of business needs and change rates</p>
<p><b>Prudent ICT assessment based on a definition of N-1, patching which is a risk management strategy where a system is patched to the second most recent level that the vendor has released. This approach aims to limit the risk of hitting unidentified issues/bugs in new patches, as the earlier patch has likely had more field testing.</b></p>	<p>Altered expenditure profile to reflect actual cost</p>	<p>Continuous assessment through our Standard Cyber Risk and Compliance management processes.</p>
<p><b>The post-2025 market reform, the evolution of the Security of Critical Infrastructure act (SOCI) and ESB data strategy will result in significant new compliance and legal obligations in the 2025-30 regulatory control period impacting cyber-security requirements.</b></p>	<p>Whilst this is unlikely, it would impact Risk and compliance profile which will result in an altered expenditure profile</p>	<p>Continuous assessment through our Standard Cyber Risk and Compliance management processes.</p>

## 6.5 Dependencies

All non-network ICT and network investments that include components of digital nature (including intelligent devices connected to the power network) are dependent on the Cyber Security investments in this business case.

In addition, the following table lists investments that this Cyber Security business case depends on for its success.

**Table 20: Dependencies Overview**

Dependency Description	Dependent upon
<p>These business cases include ICT asset management activities (e.g., system upgrades and legacy system replacements) that are required to ensure that contemporary Cyber Security controls can continue to be applied effectively, to keep our customers, digital systems, our staff and our network safe.</p>	<p>Customer, Asset and Works Management, Digital Core, Integrated Grid Planning, Digital Foundations, Data &amp; Intelligence</p>
<p>In addition, Data &amp; Intelligence investments provide the data classification, governance, management and sharing capabilities that complement the Cyber Security controls to ensure that our information is safe and secure.</p>	<p>Data &amp; Intelligence</p>
<p>In addition, Digital Foundation provides:</p> <ul style="list-style-type: none"> <li>• The infrastructure, technologies, integration and service management platforms underpinning all other non-network ICT business cases.</li> <li>• Investments to improve data protection in hybrid clouds environments and for IoT device management, which will contribute to effective mitigation of cyber risks (e.g., Sensitive Information Loss or Malicious Critical Infrastructure Attack).</li> <li>• DevOps, monitoring, and service management capabilities that will be used by CUP and Cyber Security operations.</li> </ul>	<p>Digital Foundations</p>
<p>There are a range of proposed Network investments that include network asset management activities, such as the renewal of hardware, software and telecommunications assets for OT, or the renewal of intelligent OT devices connected to the power network). These asset renewals are required to ensure that contemporary Cyber Security controls, as defined in the AESCSF<sup>7</sup> and NIST<sup>8</sup> Frameworks, can continue to be applied effectively, and that our Network remains reliable, secure, and is safe from Cyber Security attacks.</p>	<p>Network Business Cases for OT asset management / renewal</p>

<sup>7</sup> Australian Government, URL: Australian Energy Sector Cyber Security Framework | [energy.gov.au](http://energy.gov.au)

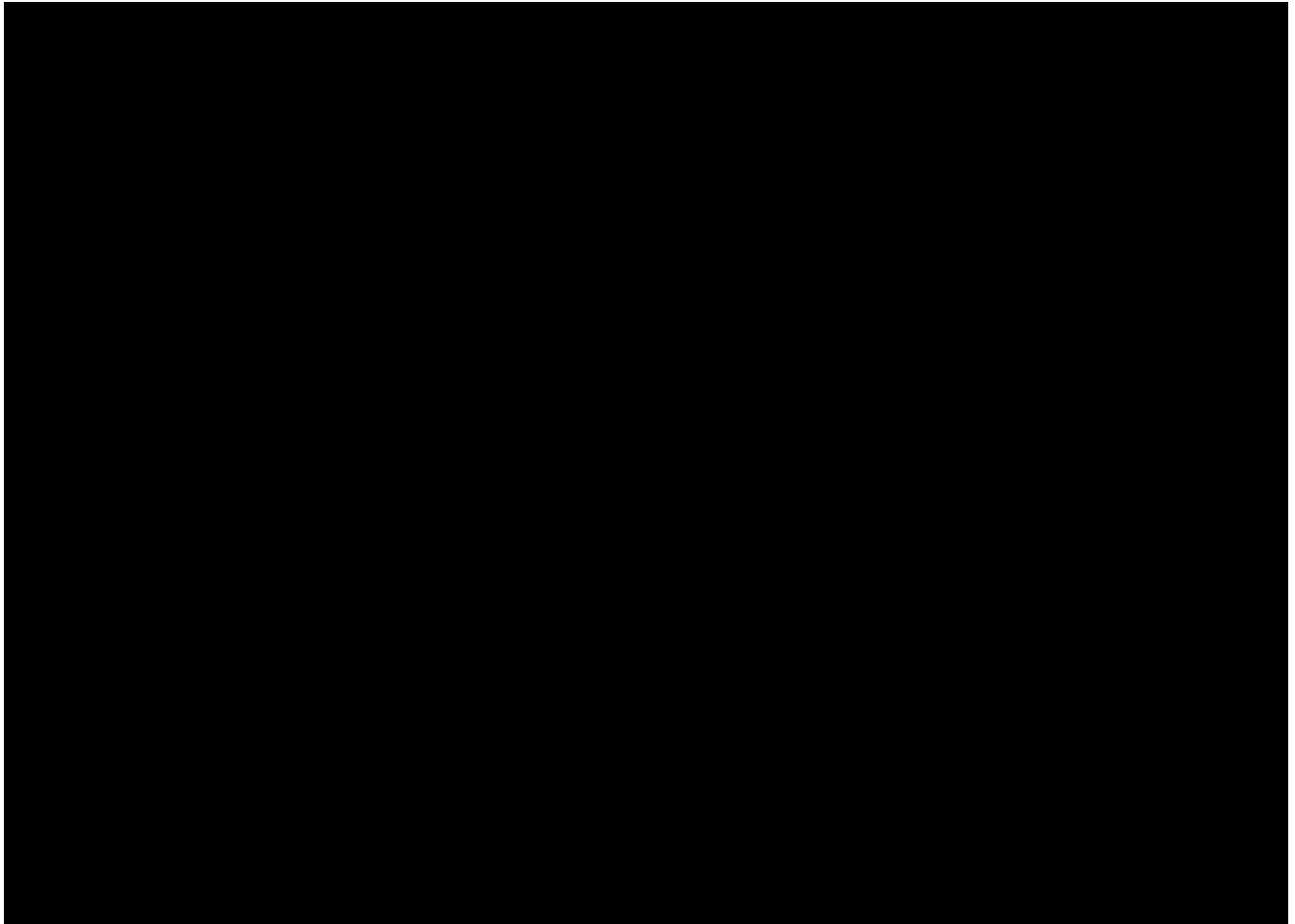
<sup>8</sup> NIST, URL: Cybersecurity Framework | NIST

---

## 6.6 Delivery Risks and Controls

The recommended option (Option 3) has a number of delivery risks and consequences attached. These are detailed below, including associated controls.

**Table 19: Delivery risks associated with recommended option**



## 6.7 Reconciliation Table

Table 20: Financial Reconciliation (\$M)

Capital Expenditure	Entity	FY26	FY27	FY28	FY29	FY30	Total 2025-30
Expenditure in business case \$M, real December 2022	Energy Queensland	■	■	■	■	■	56.3
<b>Allocation to entity (where applicable)</b>							
\$M, real December 2022	Energex	■	■	■	■	■	23.5
\$M, real December 2022	Ergon Energy Network	■	■	■	■	■	31.3
\$M, real December 2022	Other	■	■	■	■	■	1.5
<b>Allocation to SCS capex (DNSP only)</b>							
\$M, real December 2022	Energex	■	■	■	■	■	21.2
\$M, real December 2022	Ergon Energy Network	■	■	■	■	■	26.0
<b>Add escalation adjustments (DNSP only)</b>							
Escalation from \$M, real December 2022 to \$M, real June 2025	Energex	■	■	■	■	■	24.0
Escalation from \$M, real December 2022 to \$M, real June 2025	Ergon Energy Network	■	■	■	■	■	29.4
Expenditure in AER capex model/Reset RIN \$M, real June 2025	Energex	■	■	■	■	■	24.0
Expenditure in AER capex model/Reset RIN \$M, real June 2025	Ergon Energy Network	■	■	■	■	■	29.4