



**INFORMATION AND  
COMMUNICATIONS  
TECHNOLOGY**

**CYBER SECURITY**

CP BUS 6.02 – PUBLIC  
2026–31 REGULATORY PROPOSAL

# Table of contents

<b>1. Overview</b>	<b>2</b>
<b>2. Background</b>	<b>3</b>
2.1 Compliance obligations	3
2.2 Our performance over the current regulatory period	3
2.3 Cyber threats and motivations	4
2.4 Shared IT systems	5
<b>3. Identified need</b>	<b>6</b>
3.1 Growing cyber security obligations	6
3.2 Increasing and more sophisticated security threats and need to focus on 'cyber-resilience'	7
3.3 Digitalisation and decentralisation changing the nature of risks to electricity systems	8
3.4 Unprecedented need for reliability and security due to a growing dependence on electricity	8
<b>4. Options analysis</b>	<b>10</b>
4.1 Risk monetisation framework	10
4.2 Option one: maintain existing cyber security maturity	12
4.3 Option two: enhance cyber security resilience capability	14
4.4 Option three: achieve market leading cyber security maturity	19
<b>5. Recommendation</b>	<b>23</b>
5.1 Implementation plan	23

# 1. Overview

In the rapidly evolving landscape of energy distribution, cyber security has become a critical priority for electricity distribution networks. With the increasing integration of smart grid technologies, cloud solution adoption, internet-of-things (IoT) devices, and advanced communication systems, we face a growing risk of cyber threats that could disrupt operations, compromise sensitive data, and endanger public safety.

This business case outlines the need for a robust cyber security strategy tailored to the unique challenges of our network. By enhancing our cyber security measures, threat detection and response capabilities and staff training, we can better mitigate cyber risks, ensure regulatory compliance, and safeguard our infrastructure and customers.

The cyber security landscape is constantly changing and evolving with ever more sophisticated threats targeting critical infrastructure providers. Within the next regulatory period, key drivers of change related to cyber security will include:

- growing cyber security compliance obligations
- increasing and more sophisticated security threats and the need to focus on 'cyber-resilience'
- digitalisation and decentralisation changing the nature of risks to electricity systems
- an unprecedented need for reliability and security due to a growing dependence on electricity related to the energy transition.

All of these factors and their ability to increase risks relating to cyber security need to be balanced against investment options that can deliver value to customers.

In response to the challenges outlined above, the following three options were assessed to identify the recommended approach for the 2026–31 regulatory period:

1. **Maintain existing cyber security maturity**– this option represents a 'do-nothing different' approach by maintaining existing capabilities with currency-related enhancements only
2. **Enhance cyber security resilience capability**– this is a risk-based approach targeting additional practices that provide the greatest risk reductions
3. **Achieve market leading cyber security maturity**– as the operator of critical infrastructure, we explored maximum possible measures under the AESCSF framework to ensure ongoing safety and reliability of the network.

Option two is our recommendation option. As a risk-based approach, this ensures that only the highest value practices are undertaken in the next regulatory period.

**TABLE 1**      **OPTIONS ANALYSIS SUMMARY (\$M, 2026)**

OPTION	CAPEX	OPEX	NPV
1      Maintain existing cyber security maturity	9.0	-	-
2      Enhance cyber security resilience capability	17.4	17.7	89.3
3      Achieve market leading cyber security maturity	20.3	20.3	88.8

Note: This includes costs and benefits for both CitiPower and Powercor

## 2. Background

As a critical infrastructure provider, any disruption to supply of electricity can have serious implications for our customers, business, the government and communities.

### 2.1 Compliance obligations

[REDACTED]

We also have obligations under the Australian Privacy Act 1988 (Cth) (Privacy Act), which require us to store and process personal information of customers and are subject to data and privacy protection regulations. The Privacy Act further defines the Australian Privacy Principles (APP) that outline requirements for how 'APP entities' must handle, use, and manage personal information.

Due to our organisational ownership structure, we are also subject to the Australian Government's Foreign Investment Review Board (FIRB) restrictions. This includes a variety of requirements, including restrictions relating to data sovereignty, which is an important consideration when deploying and uplifting cyber security capabilities.

All of these obligations require us to ensure that our systems and the data that we hold on behalf of customers and the industry is protected.

### 2.2 Our performance over the current regulatory period

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

## 2.3 Cyber threats and motivations







The cyber security threat landscape is constantly changing and evolving, and threat actors are becoming increasingly sophisticated at carrying out attacks.

Figure 1 sets out the common threat actor motivations, while figure 2 outlines the most relevant and prevalent cyber security threat outcomes. The threats present potential entry points for threat actors into our IT and operating technology (OT) systems.

**FIGURE 1 THREAT ACTOR MOTIVATIONS**



**FIGURE 2 CYBER SECURITY THREATS**

Cyber Security Threats	Description	Threat Actor Motivations	Common Means of Attack
<b>Ransomware or other Malware</b> 	This is a malware-based attack that prevents us from using our systems and data unless a ransom is paid.	<ul style="list-style-type: none"> <li>•Financial gain</li> <li>•Sabotage</li> <li>•Insider: malicious</li> </ul>	<ul style="list-style-type: none"> <li>•Phishing</li> <li>•USB-based Malware</li> <li>•Downloaded Malware</li> <li>•Compromised BYOD</li> <li>•Third party as a vector to our network</li> </ul>
<b>Extortion (Business operations or Data)</b> 	This is when a threat actor has access to or has copied sensitive information or data from our systems and threatens to publish this on public forums or the dark web unless a sum of money is paid to them. Often combined with a ransomware attack.	<ul style="list-style-type: none"> <li>•Financial gain</li> <li>•Sabotage</li> <li>•Insider: malicious</li> </ul>	<ul style="list-style-type: none"> <li>•Phishing</li> <li>•Business Email Compromise (BEC)</li> <li>•Data exfiltration</li> <li>•Third party as a vector to our network</li> <li>•Denial of Service</li> </ul>
<b>Credential Compromise</b> 	This is an attack that can gain access to username and password and second factors of authentication by a variety of methods. Alternatively, this can occur due to credentials being reused which are compromised elsewhere. If privileged credentials are accessed this can be particularly harmful. This attack is difficult to detect as it appears to be a legitimate user.	<ul style="list-style-type: none"> <li>•Financial gain</li> <li>•Insider: malicious</li> <li>•Insider: accidental</li> <li>•Sabotage</li> <li>•Hacktivism</li> </ul>	<ul style="list-style-type: none"> <li>•Brute-force attacks</li> <li>•Phishing</li> <li>•Credential Purchase</li> <li>•Interception attacks (Man in the middle)</li> <li>•Reuse attacks (Credential stuffing)</li> <li>•Third party as a vector to our network</li> </ul>
<b>Vulnerability Exploitation</b> 	A weakness in our systems is identified and exploited enabling a threat actor to gain unauthorised access.	<ul style="list-style-type: none"> <li>•Espionage</li> <li>•Financial gain</li> <li>•Insider: malicious</li> <li>•Insider: accidental</li> <li>•Hacktivism</li> <li>•Sabotage</li> </ul>	<ul style="list-style-type: none"> <li>•Zero-day exploit</li> <li>•SQL Injection</li> <li>•Remote Code Execution (RCE)</li> </ul>
<b>Sensitive Data Disclosure</b> 	Sensitive information is disclosed to an unauthorised recipient due to either user error or malicious intent. This may be as simple as entering the wrong email address when sending a file.	<ul style="list-style-type: none"> <li>•Financial gain</li> <li>•Insider: malicious</li> <li>•Insider: accidental</li> </ul>	<ul style="list-style-type: none"> <li>•Emails and phishing</li> <li>•Insecure physical storage</li> <li>•Unsanctioned cloud file storage use</li> <li>•USB and removable media access</li> </ul>
<b>Third Party Compromise</b> 	A trusted third party suffers a cyber attack with unauthorised systems access. Due to the third party having access to our systems and data, the attackers then are also able to access our systems and data.	<ul style="list-style-type: none"> <li>•Espionage</li> <li>•Financial gain</li> <li>•Insider: malicious</li> <li>•Insider: accidental</li> <li>•Hacktivism</li> <li>•Sabotage</li> </ul>	<ul style="list-style-type: none"> <li>•Exploiting Insufficient information security controls and practices</li> <li>•Supply chain compromise</li> </ul>

## 2.4 Shared IT systems

This business case covers IT expenditure related to both CitiPower and Powercor. Due to long term common ownership of these distribution businesses over time we have brought together CitiPower’s and Powercor’s IT systems to enable the lowest cost delivery of our IT requirements. For example, when we are required to make changes to our business processes we are only required to make these changes once, rather than having to make similar changes across two separate IT systems.

## 3. Identified need

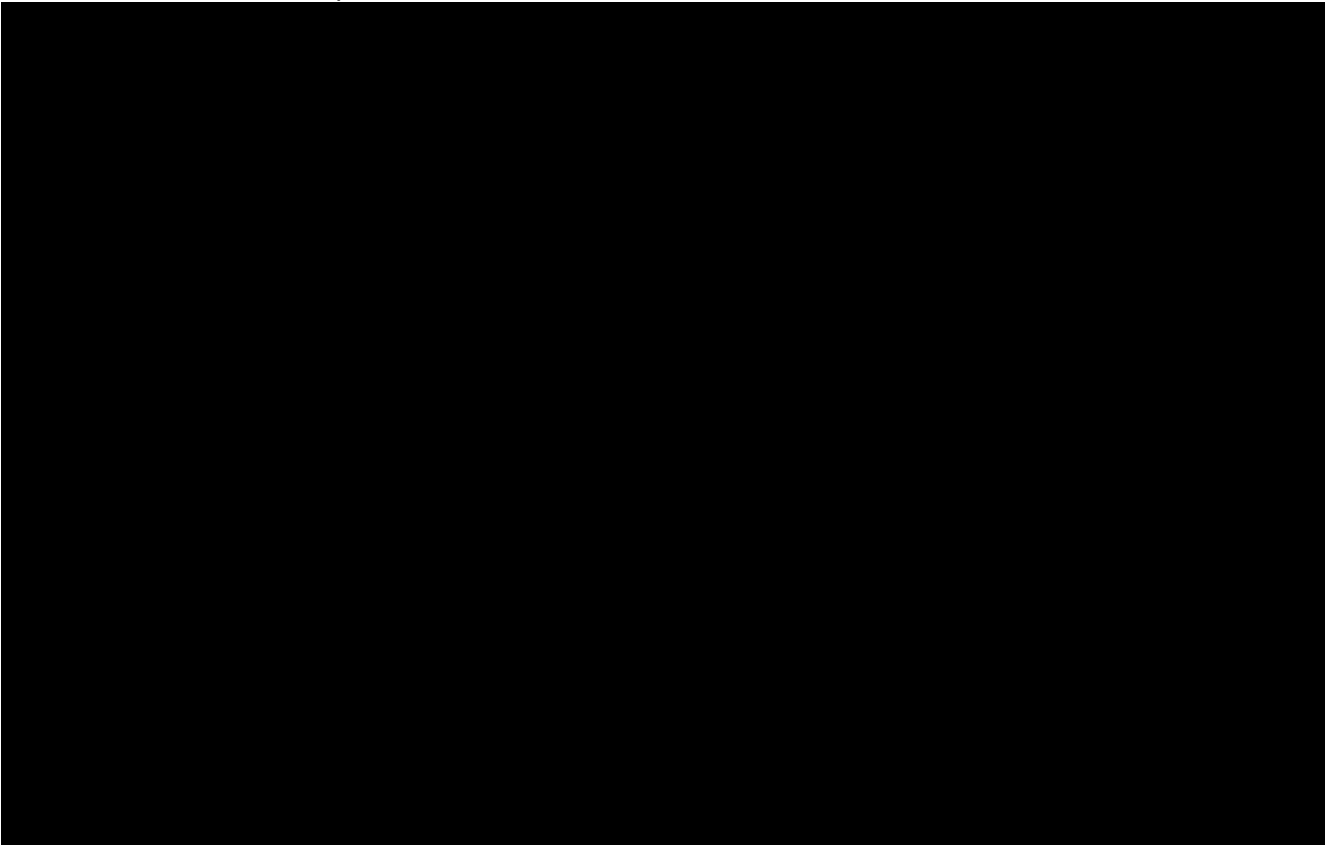
Throughout the 2021–26 regulatory period there have been a number of changes in the cyber security landscape that require us to enhance our cyber security practices. For the 2026–31 regulatory period, the identified need is to continue to meet our cyber security obligations and evolve our practices as the threat landscape continues to grow.

### 3.1 Growing cyber security obligations

Discussions on cyber security have come to the forefront in recent years, particularly with the Federal Government’s recent legislative amendments under the Security Legislation Amendment Act 2022. In addition, with the recent high profile security incidents (e.g. Optus, Medicare), cyber security is now again at front of mind for both our stakeholders as well as our everyday customers.

In November 2023, the Federal Government released the 2023–2030 Australian National Cyber Security Strategy, outlining a roadmap to make Australia a global leader in cyber security by 2030.<sup>1</sup>

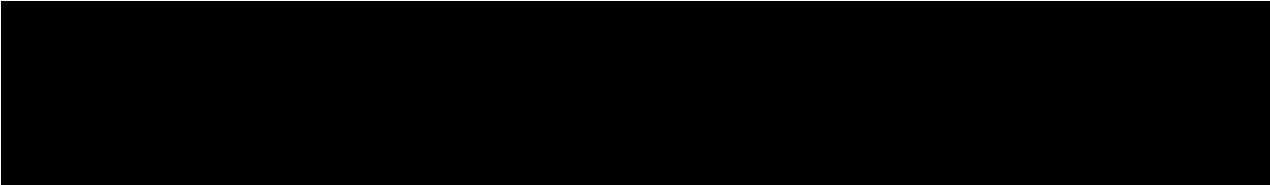
Following this in October 2024, a Cyber Security Legislative Package 2024 consisting of three bills was passed through federal parliament. It intends to implement seven initiatives under the 2023–2030 Australian Cyber Security Strategy, which aims to address legislative gaps to bring Australia in line with international best practice.



---

<sup>1</sup> Department of Home Affairs, [2023-2030 Australian Cyber Security Strategy](#), November 2023





The Government has, for some time, expressed concern about the risks associated with the proliferation of internet-of-things or IoT devices in Australian households. This is due to the manner in which they collect data (including sensitive data), and the cyber risk attached to this data being stolen. The legislation provides the Government the flexibility to address these concerns through specific standards.

For electricity distribution networks this could mean a potential impact on CER types of devices, and flow on impacts to energy management solutions like distributed energy resources management systems (DERMS).

We expect ongoing policy and compliance-driven requirements over the 2026–31 regulatory period to continue to lift minimum standards for how we must manage our network operations, in addition to broader 'best practice' methods to mitigate cyber threats.

### **3.2 Increasing and more sophisticated security threats and need to focus on 'cyber-resilience'**

Threat actors are becoming increasingly sophisticated at carrying out attacks. We must manage not only the increased risk of the number of attacks, but also the new sources and targets for such attacks. As highlighted in the box below, electricity providers are now one of the most frequently reported sources of critical infrastructure cyber attacks. Complete prevention is no longer possible, however we must continue to focus on developing resilience so that our systems can withstand, respond and recover without major disruptions to the grid and critical infrastructure operations.

In FY2023–24, the Australian Signals Directorate received over 36,700 calls to its Australian Cyber Security Hotline, an increase of 12% from the previous financial year. ASD also responded to over 1,100 cyber security incidents, highlighting the continued exploitation of Australian systems and ongoing threat to our critical networks.

The most frequently reported critical infrastructure sectors were electricity, gas, water and waste services (30%), education and training (17%) and transport, postal and warehousing (15%)<sup>2</sup>

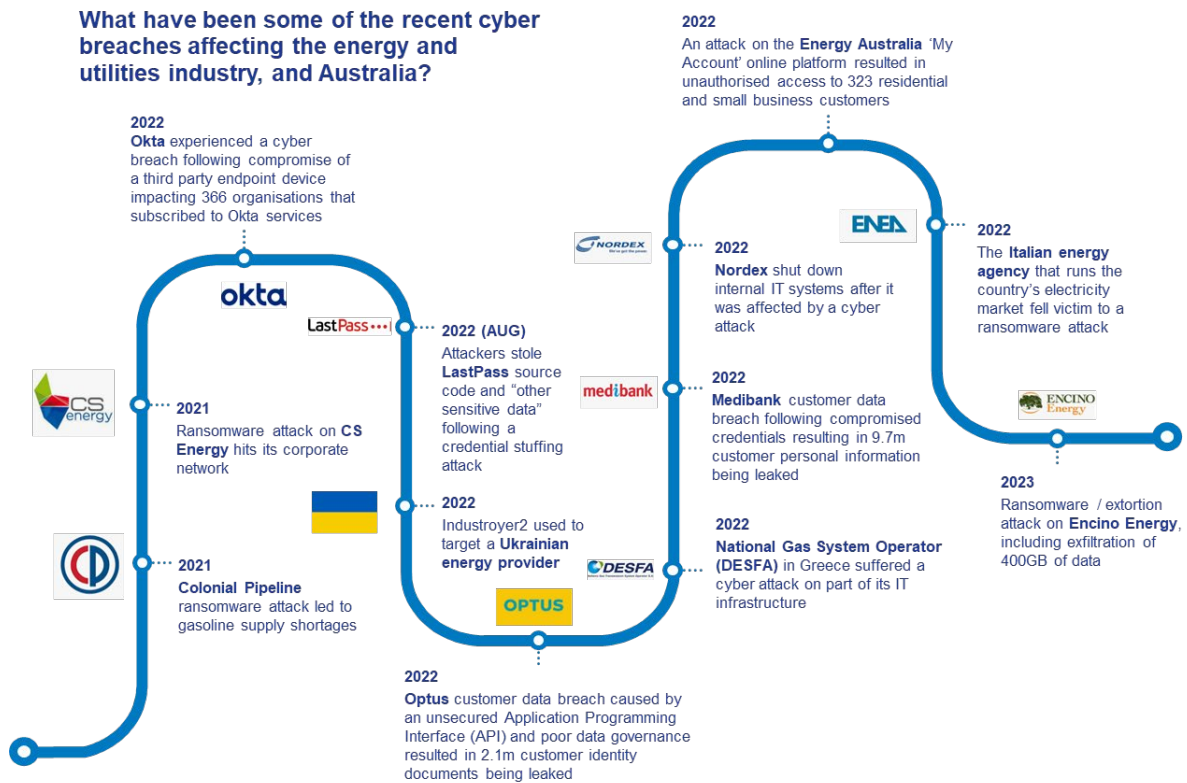
Figure 3 further highlights some of the major cyber breaches over the 2021–26 regulatory period across Australia and the broader energy industry. Cyber threat actors are now consistently targeting the energy and utilities industry.

---

<sup>2</sup> Annual Cyber Threat Report 2023-2024 | Cyber.gov.au



**FIGURE 3 CYBER SECURITY BREACHES TIMELINE**



### 3.3 Digitalisation and decentralisation changing the nature of risks to electricity systems

The electricity network is reliant on IT and operating technology (OT) systems and data. Hence it is critical these systems have robust cyber security controls to ensure the safe and reliable operation of the electricity network. Distribution businesses such as ours are targets for malicious cyber security threat actors in a constantly evolving threat environment. Threats in our sector include not just unauthorised access of IT systems or phishing of sensitive information. Malicious actors are increasingly targeting OT systems, such as supervisory control and data acquisition (SCADA) systems.

Our networks and their make up is increasingly shifting. Our consumers are no longer only energy consumers, but producers too. The distributed energy resources spread across our network, the new inter-connected devices digitalising our grids, and the IT-OT convergence all increase our exposure points and the complexities of how we manage the breadth of threat entries. We must assess and deploy safeguards and preventions across areas we previously did not focus our investment in, such as DERMs and a growing number of potential threat entry points.

### 3.4 Unprecedented need for reliability and security due to a growing dependence on electricity

While minimising cyber security threat has always been an objective, it is now more crucial than ever given the generational transformation of the Australian grid and the fast-paced energy transition. Australia is increasingly struggling to keep pace with grid transition timelines. All energy value chain players including distribution networks play a very important role in ensuring our networks are still providing customers with uninterrupted, reliable and affordable power, while the grid is replaced,

renewed and transitioning. Any recurring or major threats to our network can significantly impede the transition itself.

## 4. Options analysis

As set out in the previous section, external drivers such as government-led mandates on security and legislation such as SOCI require us to bolster our capabilities. At the same time, the AER and our stakeholders expect value from what we invest in.

Our approach to prioritising and investing in security capabilities needs to balance risk and value, ensuring we deliver high security, with minimal impact on customer affordability. To deliver this value, we considered three options to meet our cyber security requirements:

1. **Maintain existing cyber security maturity**– this option represents a ‘do-nothing different’ approach by maintaining existing capabilities with currency-related enhancements only
2. **Enhance cyber security resilience capability**– this is a risk-based approach targeting additional practices that provide the greatest risk reductions
3. **Achieve market leading cyber security maturity**– as the operator of critical infrastructure, we explored maximum possible measures under the AESCSF framework to ensure ongoing safety and reliability of the network.

The costs and associated net present value of each of the options is presented in table 2, and set out in further detail in our attached cyber security cost and risk models.<sup>3</sup>

**TABLE 2      OPTIONS ANALYSIS SUMMARY (\$M, 2026)**

OPTION	CAPEX	OPEX	NPV
1      Maintain existing cyber security maturity	9.0	-	-
2      Enhance cyber security resilience capability	17.4	17.7	89.3
3      Achieve market leading cyber security maturity	20.3	20.3	88.8

Note: This includes costs and benefits for both CitiPower and Powercor

### 4.1 Risk monetisation framework

To assess our investment options, we worked with EY to develop an ICT risk monetisation framework. This provides a standardised approach for identifying, classifying, and quantifying risks associated with potential IT investments.

The framework aims to support value-based decision making by translating risks into monetised values, facilitating consistent evaluation of cost-benefit analyses across potential investment scenarios.<sup>4</sup>

Figure 4 sets out the steps we have taken to quantify risks associated with this business case. Further information on each of these steps is included in the risk monetisation framework attachment.

<sup>3</sup> CP MOD 6.03 - Cyber security cost - Jan2025 – Public; CP MOD 6.04 - Cyber security risk - Jan2025 - Public  
<sup>4</sup> CP ATT 6.02 – EY - IT risk monetisation framework – Aug2024 – Public

**FIGURE 4 RISK MONETISATION STEPS**

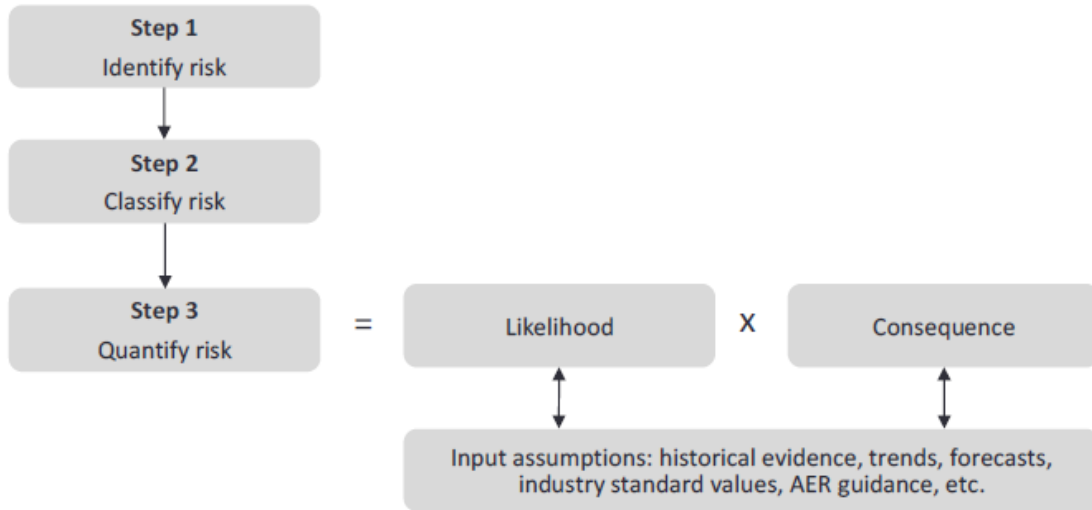


Table 3 provides a summary of each risk category included in our risk monetisation framework.

**TABLE 3 RISK FRAMEWORK SUMMARY**

CATEGORY	DESCRIPTION
Reliability	Risks related to events or failures that cause unforeseen impacts to electricity supply or export capability. For example, customer supply or solar export outages
Compliance	Risks of regulatory, legal, or financial penalties due to failure in meeting compliance obligations, such as delays in publishing key market data or unauthorised access to sensitive data
Bushfire	Risks that outages of critical operational systems may increase bushfire likelihood by impairing visibility of the network and timely decision-making
Safety	Risks affecting public and staff safety, such as loss of supply impacting life-support customers or disruptions to protective systems
Customer experience	Risks where customer interactions are impacted, such as outages of customer-facing IT systems
IT outage	Risks of systems becoming unavailable due to poor infrastructure maintenance, resource constraints, or cyber attacks. Examples include prolonged downtimes or outages caused by a cyber incident
IT suitability and sustainability	Risks arising from legacy systems that are prone to failures, inefficiencies, and incompatibilities. These systems may lead to increased maintenance costs, failures, and cyber vulnerabilities if not updated

## 4.2 Option one: maintain existing cyber security maturity

Option one is a do-nothing different approach to maintain the status quo. It focuses on sustaining our current level of cyber maturity through continued levels of operational expenditure.

This option will maintain the capabilities that have been deployed over the 2021–26 regulatory period without further investment in enhancing, expanding or developing new capabilities. However, this option does include investments in capabilities that must be undertaken to meet our known and anticipated legal and regulatory obligations, including conservative actions supporting compliance with the SOCI Act.



The table below summarises an assessment of option one against our key risk criteria.

A large solid black rectangular redaction box covering the entire content area of the table.

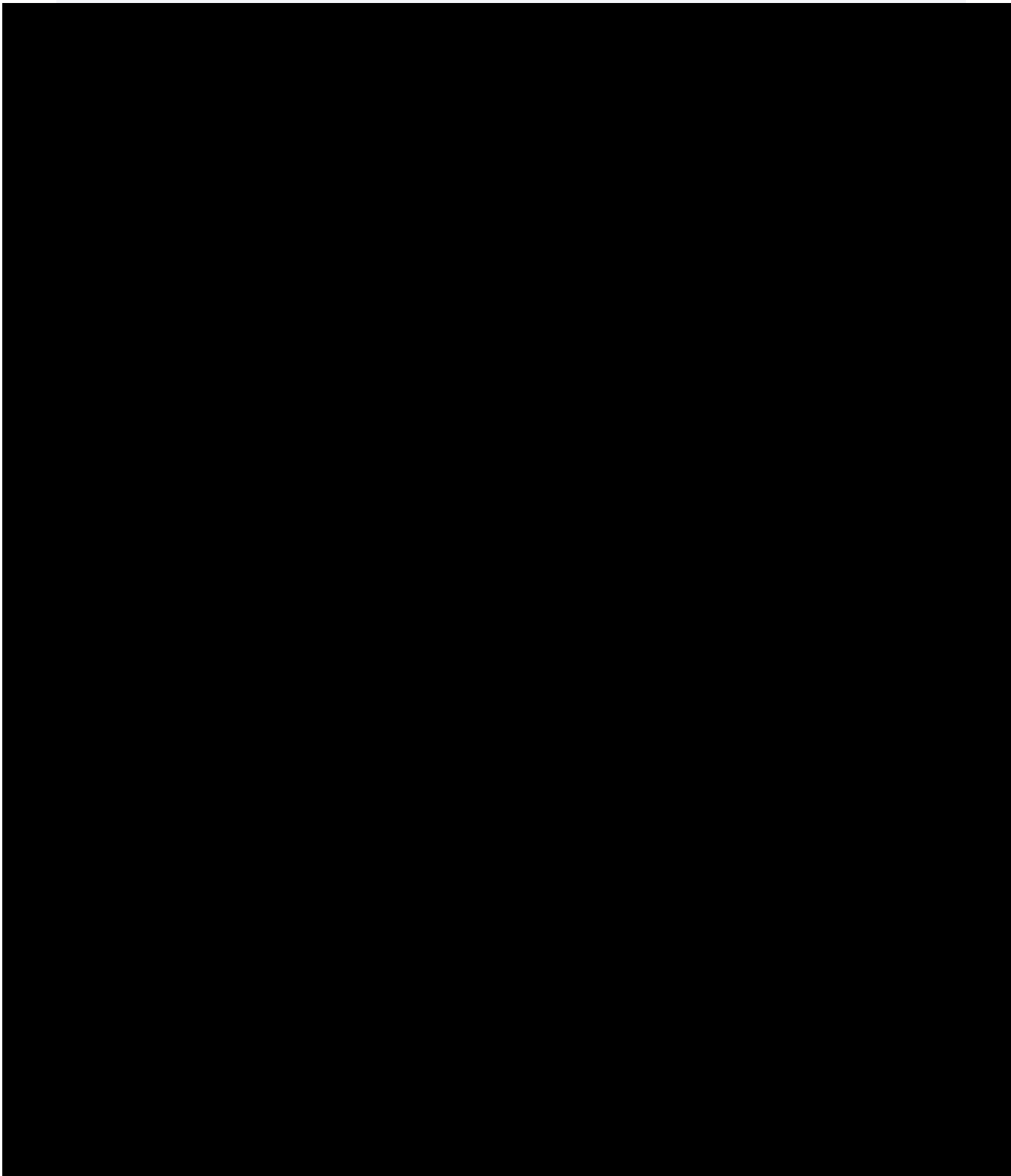


Table 5 sets out the capital and operating expenditure associated with option one.

**TABLE 5      OPTION ONE: EXPENDITURE PROFILE (\$M, 2026)**

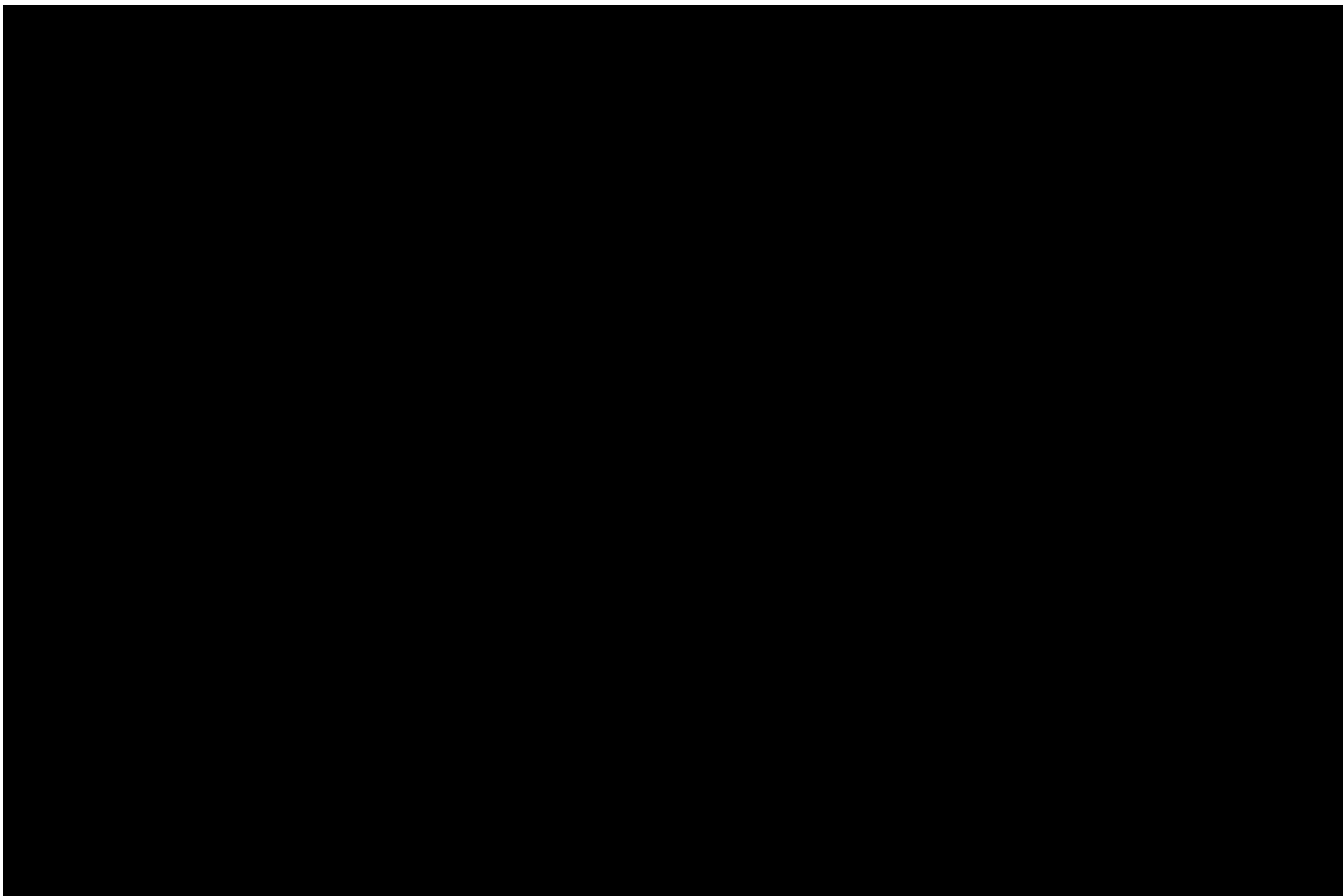
OPTION ONE		FY27	FY28	FY29	FY30	FY31	TOTAL
CitiPower	Capex	0.5	0.5	0.5	0.5	0.5	2.7
	Opex	-	-	-	-	-	-
Powercor	Capex	1.3	1.3	1.3	1.3	1.3	6.3
	Opex	-	-	-	-	-	-
<b>Total</b>		<b>1.8</b>	<b>1.8</b>	<b>1.8</b>	<b>1.8</b>	<b>1.8</b>	<b>9.0</b>

\*Rounding may lead to discrepancies between individual network costs and total costs

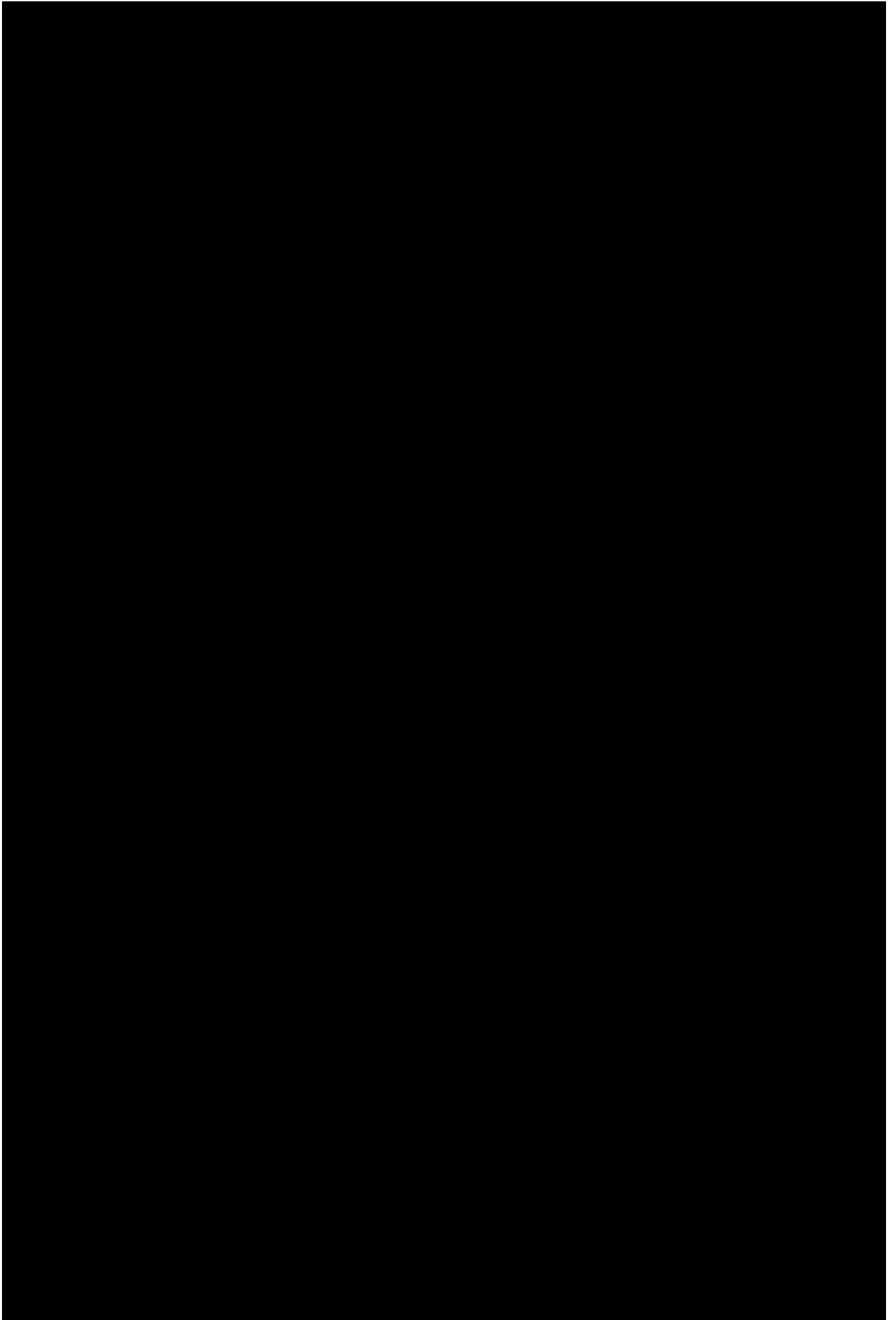
### 4.3 Option two: enhance cyber security resilience capability

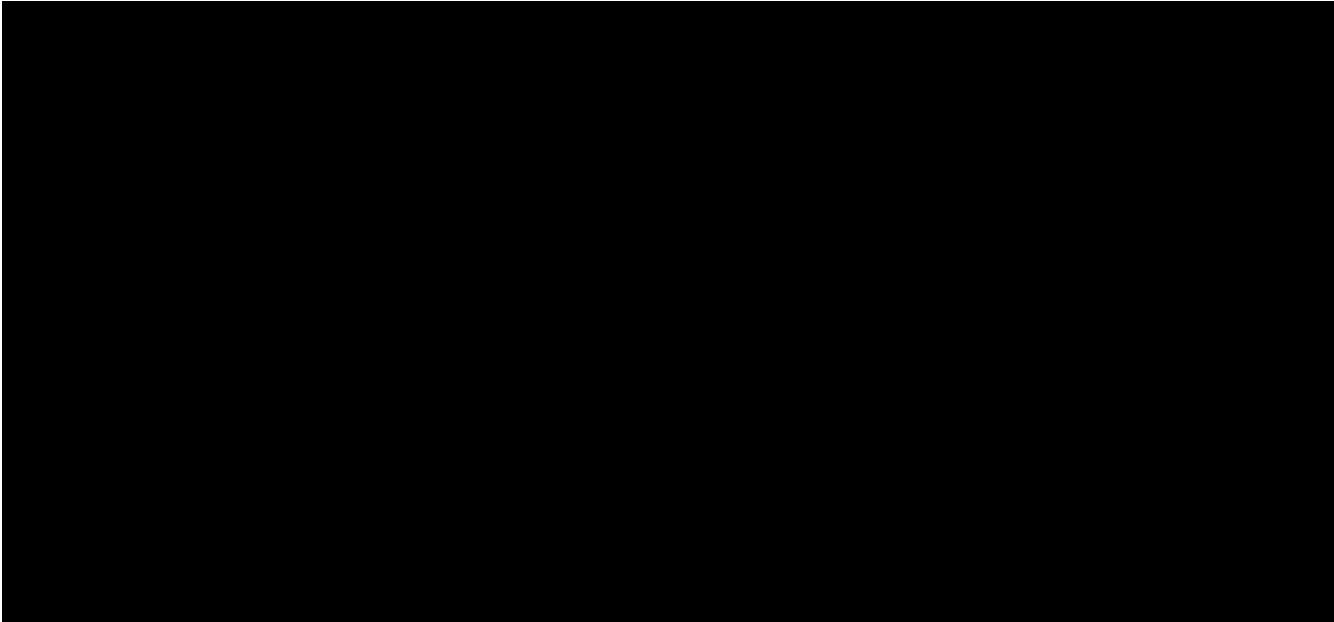
Option two will implement all SP2 practices and high value SP3 practices, continuing to enhance our enterprise cyber security capabilities but place greater emphasis on people, process and monitoring to improve company-wide cyber awareness and controls. This option has taken a risk-based approach to selecting the practices that we consider will provide the most value to customers.

The focus areas described in table 6 represent areas where we propose enhancements to existing cyber security capabilities, aimed at strengthening foundations, improving resilience, and addressing evolving risks. These refinements build on what is already in place and focus on delivering greater reliability, compliance, and operational effectiveness.



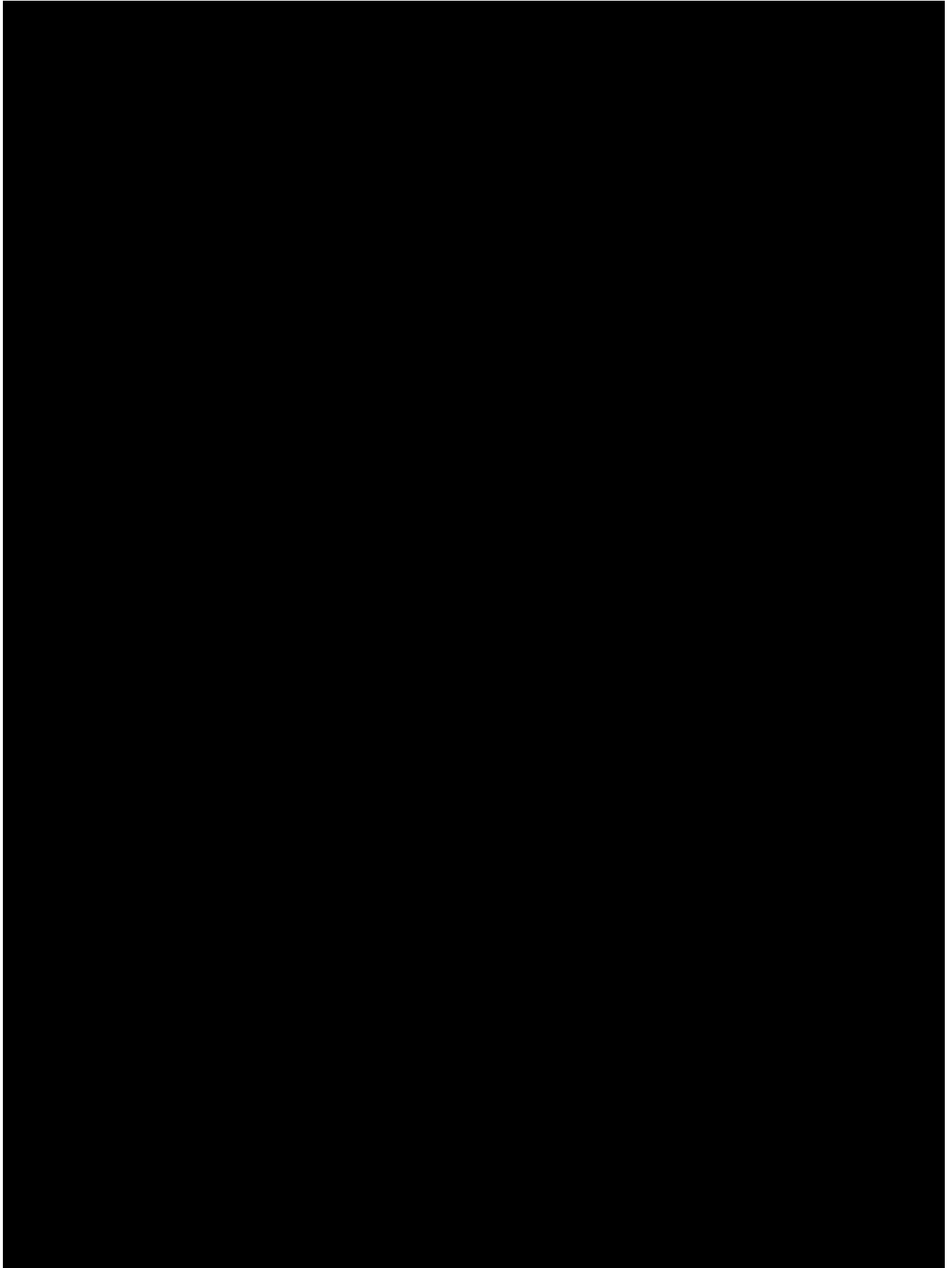






Additionally, several initiatives focus specifically on protecting against new risks associated with Customer Energy Resource (CER) devices. We need to implement new measures to identify specific CER assets, segment the CER environments in a secure manner, allow detection of cyber anomalies in the CER network, establish stricter design and test processes for anything that integrates with CER technologies, and develop detailed plans for what a cyber response will look like in the event of a CER-impacted cyber incident. This will be a new frontier where the response is a combination of a cyber and an electricity network response.

The table below summarises an assessment of option two against our key risk criteria.



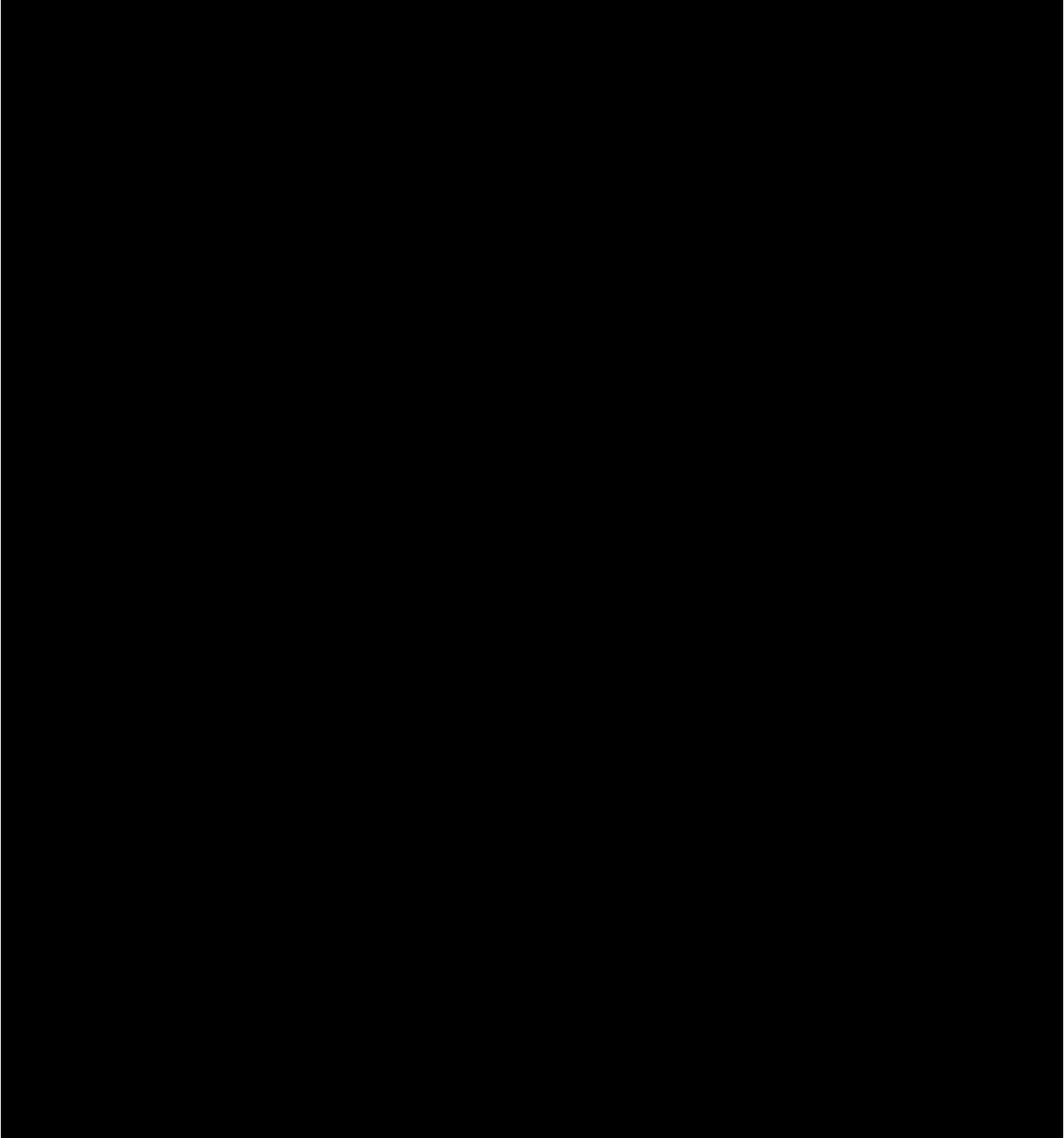


Table 8 sets out the proposed capital and operating expenditure associated with option two.

**TABLE 8      OPTION TWO: EXPENDITURE PROFILE (\$M, 2026)**

OPTION TWO		FY27	FY28	FY29	FY30	FY31	TOTAL
CitiPower	Capex	1.0	1.3	1.2	1.0	0.7	5.2
	Opex	0.4	0.8	1.1	1.5	1.6	5.3
Powercor	Capex	2.4	3.1	2.8	2.2	1.7	12.2
	Opex	0.8	1.8	2.5	3.5	3.7	12.4
<b>Total</b>		<b>4.6</b>	<b>7.0</b>	<b>7.5</b>	<b>8.3</b>	<b>7.7</b>	<b>35.0</b>

\*Rounding may lead to discrepancies between individual network costs and total costs

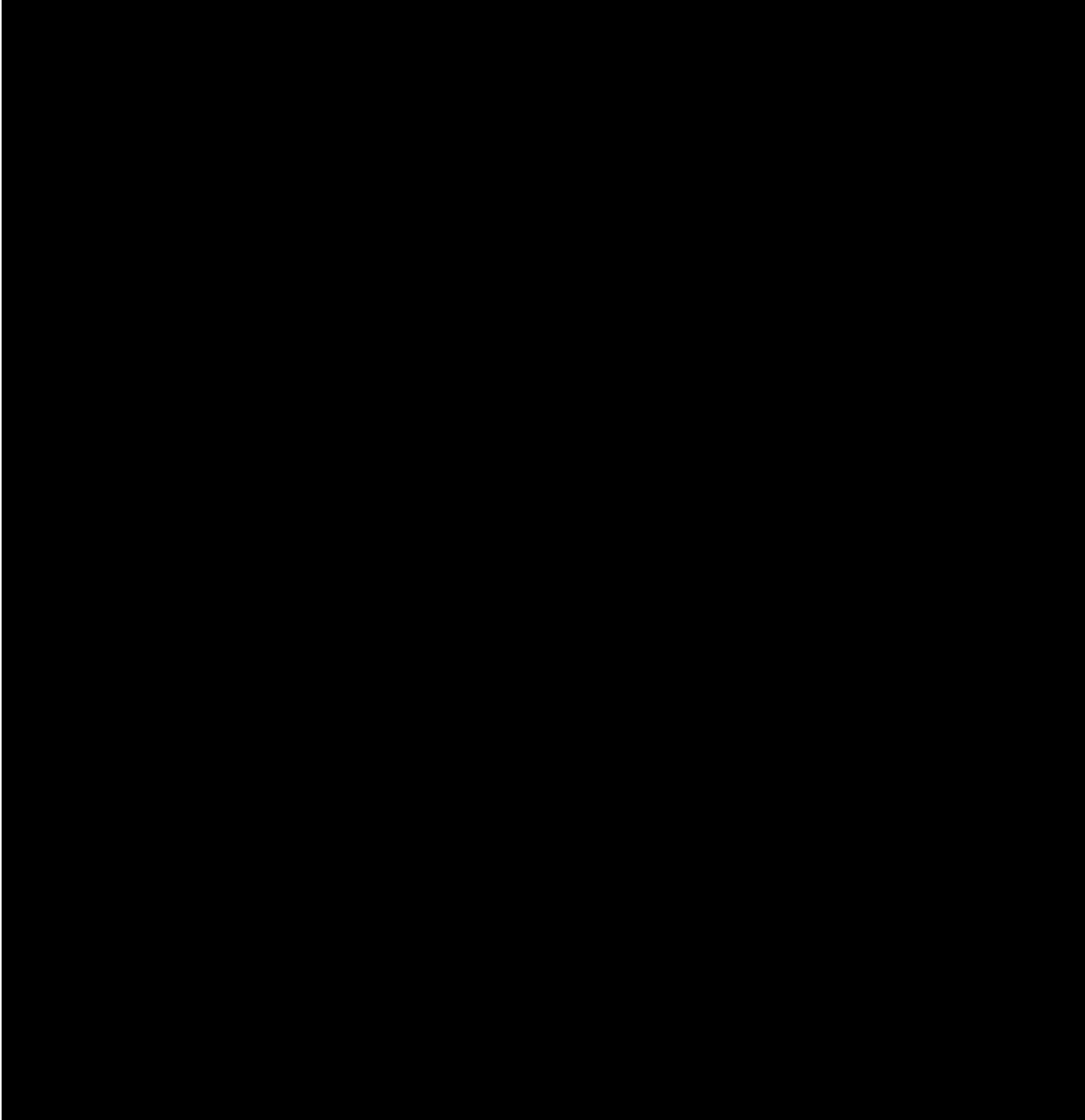
#### 4.4 Option three: achieve market leading cyber security maturity

This option would complete 100 per cent of SP3 practices currently outlined in AESCSF version 2.0, allowing us to achieve maximum compliance level. This option prioritises framework completion.

The main uplift capabilities compared to option two are in strengthened automation and monitoring for real-time visibility of all platforms across our IT and OT environments.

The implementation of these practices requires investment and effort beyond option two to achieve the AESCSF's 'largely implemented' rating.

In addition to option two implementations, we would implement the further measures set out in table 9 to achieve 100 per cent of AESCSF SP3.



The table below summarises an assessment of option three against our key risk criteria.

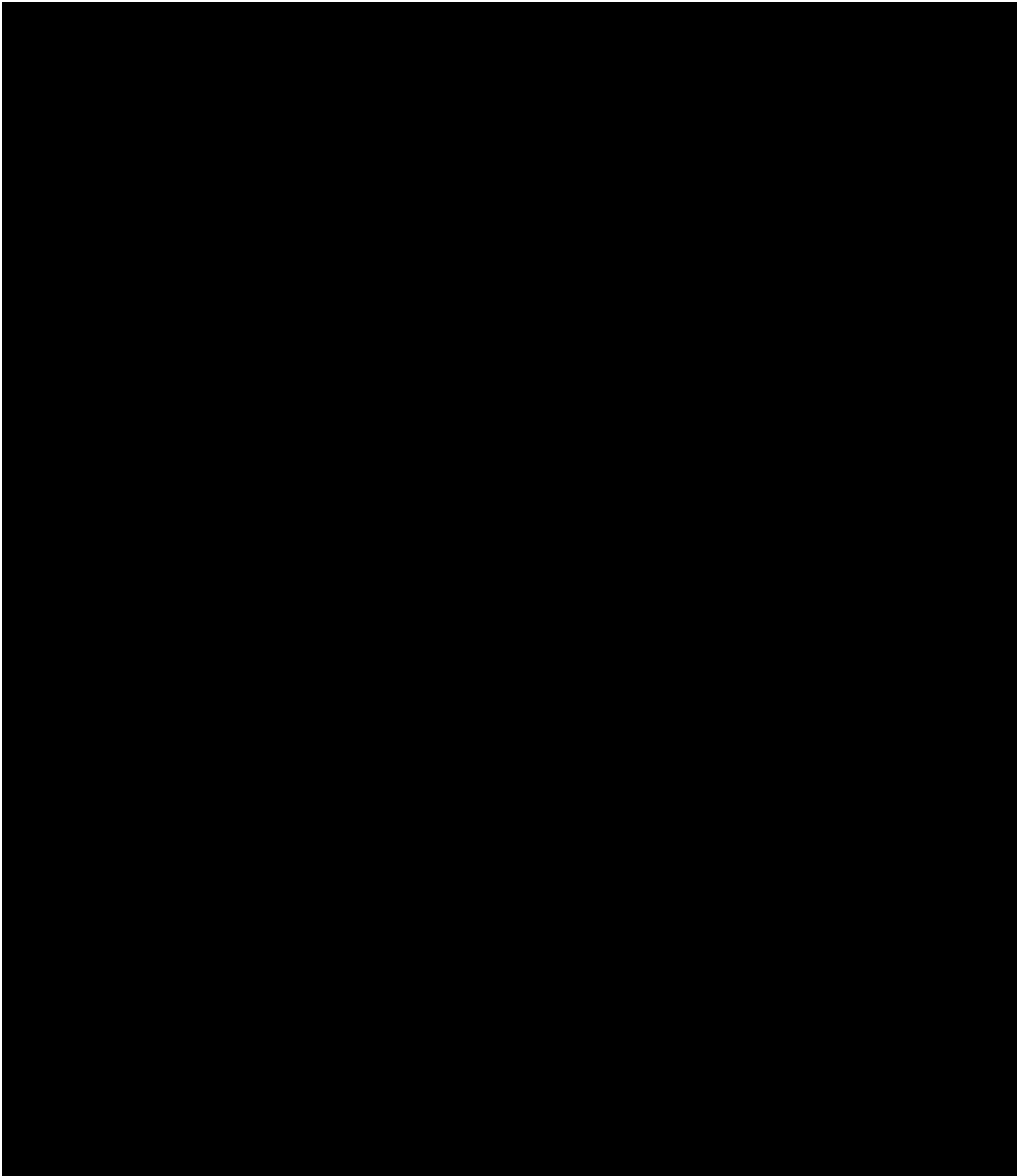




Table 11 sets out the capital and operating expenditure associated with option three. This option incurs further costs to meet the remaining SP3 practices not covered under option two.

**TABLE 11      OPTION THREE: EXPENDITURE PROFILE (\$M, 2026)**

<b>OPTION THREE</b>		<b>FY27</b>	<b>FY28</b>	<b>FY29</b>	<b>FY30</b>	<b>FY31</b>	<b>TOTAL</b>
CitiPower	Capex	1.1	1.6	1.3	1.1	0.9	6.1
	Opex	0.4	0.8	1.2	1.8	2.0	6.1
Powercor	Capex	2.7	3.8	3.0	2.6	2.2	14.2
	Opex	0.8	1.8	2.8	4.1	4.6	14.2
<b>Total</b>		<b>5.0</b>	<b>8.0</b>	<b>8.3</b>	<b>9.6</b>	<b>9.8</b>	<b>40.6</b>

\*Rounding may lead to discrepancies between individual network costs and total costs

## 5. Recommendation

As our network becomes increasingly reliant on technology-enabled solutions, such as DERMS, and increasing number of endpoints are connected to our network, there is an increasing number of units to protect. We aspire to continue improving our cyber security capabilities within our locus of control, and ongoing people and process improvements are as important as technical protections such as identity access management (IDAM) and firewalls.

Our preferred option is option two as it considers specific cyber practices that are highest value for investment in our network and for our customers. This option considers the AESCSF framework, but is not limited by a specific target state level. [REDACTED]

Our proposed program of work will enable us to identify, protect, detect, respond and recover from cyber threats, and is based on people, processes and technology. All industries continue to experience the ongoing and increasing threat of a cyber security attack. As a critical infrastructure provider we have heightened responsibilities to proactively mitigate against potential risks. While the AESCSF version 2.0 is useful to help benchmark maturity and minimum mandated compliance, a risk-managed approach specific to our own network's risks and priorities is the key approach considered for our 2026–31 program. Our proposed expenditure profile is provided in table 12.

**TABLE 12 RECOMMENDED OPTION: EXPENDITURE FORECAST (\$M, 2026)**

OPTION TWO		FY27	FY28	FY29	FY30	FY31	TOTAL
CitiPower	Capex	1.0	1.3	1.2	1.0	0.7	5.2
	Opex	0.4	0.8	1.1	1.5	1.6	5.3
Powercor	Capex	2.4	3.1	2.8	2.2	1.7	12.2
	Opex	0.8	1.8	2.5	3.5	3.7	12.4
<b>Total</b>		<b>4.6</b>	<b>7.0</b>	<b>7.5</b>	<b>8.3</b>	<b>7.7</b>	<b>35.0</b>

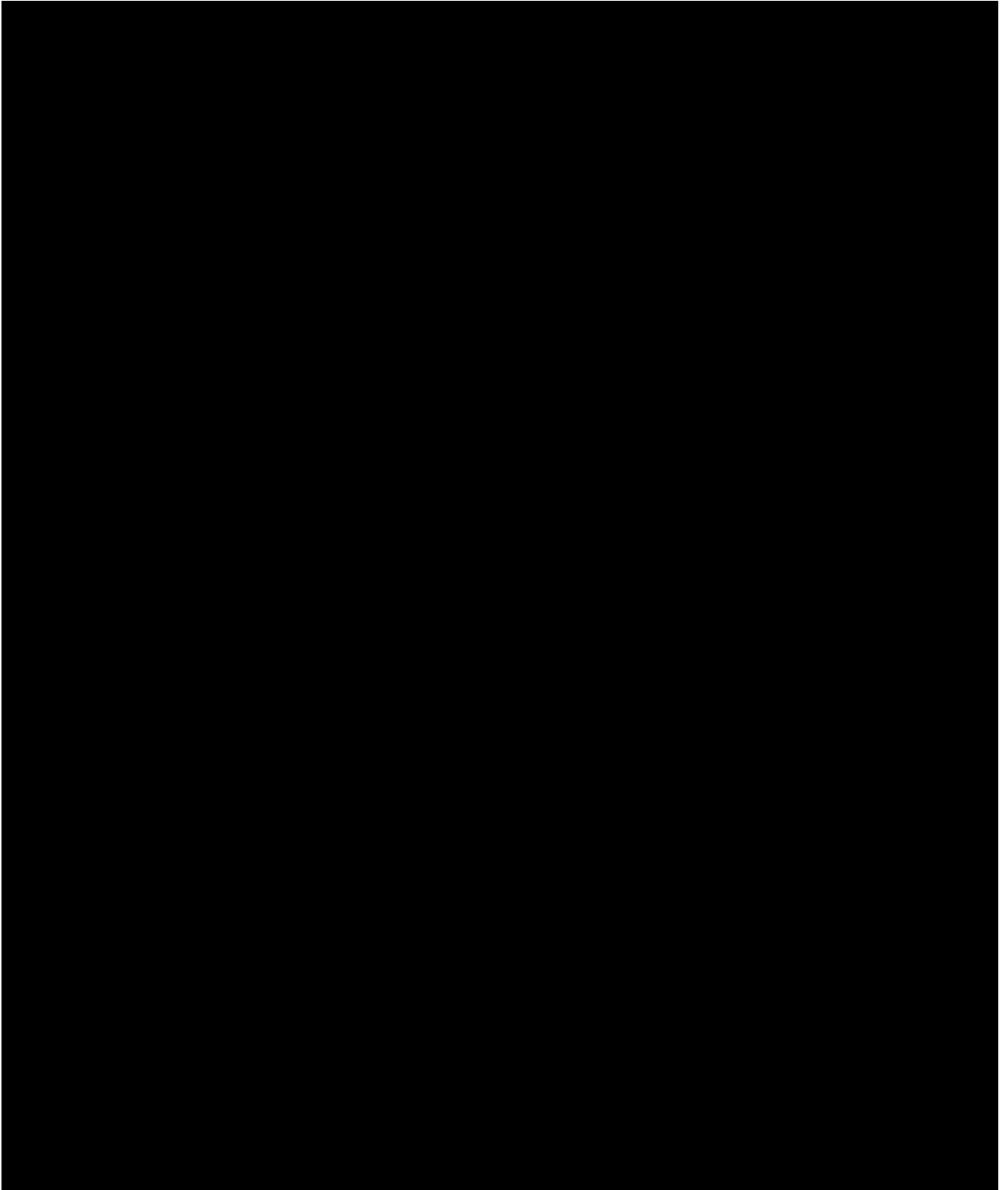
\*Rounding may lead to discrepancies between individual network costs and total costs

### 5.1 Implementation plan

[REDACTED]

[REDACTED]

[REDACTED]





For further information visit:

 [CitiPower.com.au](http://CitiPower.com.au)

 CitiPower and Powercor Australia

 CitiPower and Powercor Australia

 CitiPower and Powercor Australia