

9.02

Nominated cost pass through events

Content

1	OVERVIEW	3
1.1	Document outline	4
2	AUSGRID'S APPROACH TO RISK MANAGEMENT	5
2.1	Risk management framework	5
2.2	Assessing the appropriate regulatory treatment of risks	6
2.3	Consideration of cost impacts to consumers	7
3	NOMINATED PASS THROUGH EVENTS	9
3.1	Approach for the 2019-24 regulatory period	9
3.2	Proposed definitions	12
3.3	Justification for nominated cost pass through events	15
4	APPLICATION OF PASS THROUGH PROVISIONS TO ALTERNATIVE CONTROL SERVICES	18
	APPENDIX A: APPLICATION OF PASS THROUGH PROVISIONS TO ALTERNATIVE CONTROL SERVICES	20
A.1.	Alignment between insurance cover and hazardous events	23

1 OVERVIEW

This document sets out in detail Ausgrid's proposed nominated pass through events for the 2019-24 regulatory control period.

For the current (2015-19) regulatory period, we conducted a detailed assessment of our risk management framework. The assessment included engaging an external consultant to assess our risk management framework. As part of our assessment we considered which events should be nominated as pass through events and provided compelling evidence as to why our nominated events should be accepted by the Australian Energy Regulator (AER). The AER agreed with our proposals.

Ausgrid's risk management framework has not materially changed from the framework presented in our last regulatory proposal. Further, there has not been a material change in our operating environment that would give rise to a need to change our risk management framework.

For these reasons, we have simplified our approach towards nominating pass through events for this regulatory period. Our decision to manage certain risks via the cost pass through mechanism in the National Electricity Rules (NER) was based on an internal review to ascertain whether:

- The nominated pass through events approved by the AER for the current regulatory remained appropriate
- Any amendments were required to the definitions for the current approved pass through events
- Whether any new risks had arisen that may require an additional pass through event to be nominated.

In conducting this review we have considered a number of factors, including:

- Our ability to prevent or mitigate the risk
- The availability of insurance (external and self-insurance)
- The magnitude of the risk if it were to occur
- Relevant provisions in the NER and National Electricity Law (NEL).

Ausgrid has assessed the key risks it faces, as a network service provider operating in New South Wales (NSW), against the above criteria. Following our assessment we have concluded that the pass through events nominated and approved as part of the current 2014-19 regulatory period remain appropriate. However, we have proposed a number of minor changes to the definitions to ensure consistency with the definitions approved for other distribution network service providers (DNSP).

The events we are proposing be approved as nominated pass through events for our 2019-24 regulatory control period are the same as for the 2014-19 period. These are:

- An insurance cap event
- A natural disaster event
- A terrorism event
- An insurer's credit risk event.

Ausgrid considers that managing our exposure to those risks via the pass through provisions represents the most prudent and efficient means for addressing risks which are:

- Beyond our control to prevent/mitigate
- Cannot be effectively insured
- Have a low probability of occurrence
- Are likely to have significant cost impacts.

Ausgrid considers that these pass through events should apply to alternative control services (ACS), as well as standard control services (SCS). This is consistent with the NER, which refers to the provision of direct control services (i.e. both SCS and ACS) in relation to pass through events.¹

In applying pass throughs to ACS, Ausgrid considers that the AER should depart from the materiality threshold defined in the NER. This is because the NER definition of “materially” is linked to the concept of an annual revenue requirement, which is only relevant to SCS. For ACS, Ausgrid considers the AER should continue to apply a 1 per cent threshold, however the relevant measure is the revenue for the alternative control service that is impacted by the event that had occurred, not the annual revenue requirement.

1.1 Document outline

The remainder of this document discusses Ausgrid’s risk assessment framework and our proposed nominated pass through events in more detail. Specifically, this document sets out:

- Ausgrid’s approach to risk management
- Ausgrid’s nominated pass through events
- The application of pass through events to alternative control services

An appendix provides further details on our approach to risk management.

¹ NER clause 6.6.1(j)(2) and 6.6.1(j)(2A).

2 AUSGRID'S APPROACH TO RISK MANAGEMENT

2.1 Risk management framework

Ausgrid's approach to risk management is based on its Board Policy on Risk Management, which is aimed at sustaining a culture of risk management based on proactive and systematic identification and management of risk to support the delivery of safe, reliable and efficient energy services to Ausgrid's customers.

Ausgrid's Risk Management Policy is implemented through its Risk Management Framework and Risk Management Plan. Our Risk Management Framework sets out the foundation documents and organizational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the business.

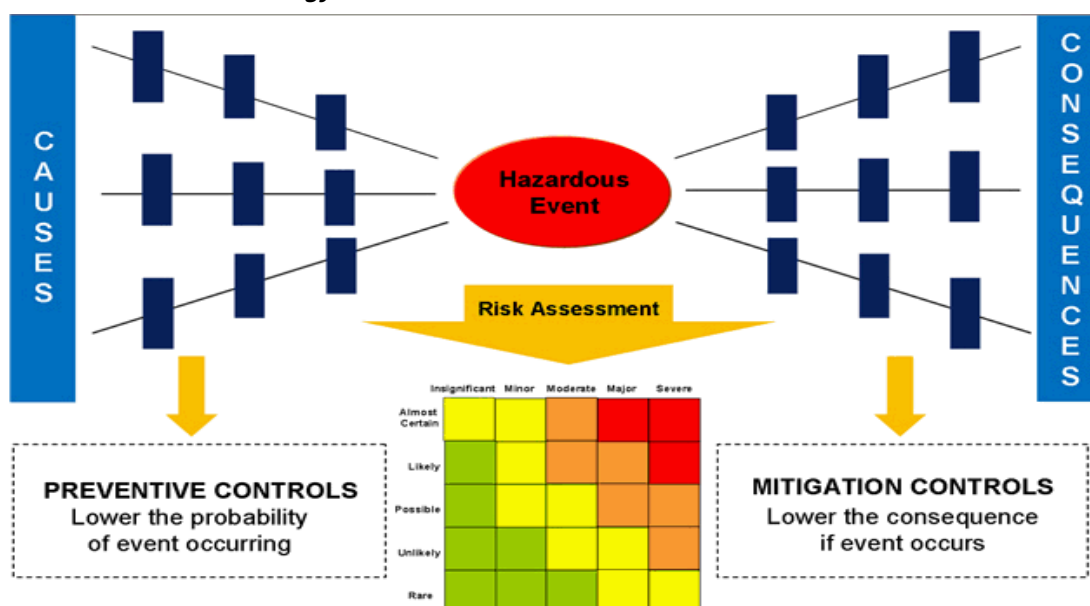
Ausgrid's Risk Management Framework utilises the bow-tie risk methodology to assess its key risks. The bow-tie methodology considers plausible worst case hazardous events and identifies both the preventative controls to reduce the likelihood of the risk occurring and mitigation controls to reduce the consequence of the event. Figure 1 illustrates the bow-tie risk methodology.

In addition, Ausgrid maintains comprehensive insurance arrangements which are regularly reviewed to align with the bow-tie methodology. Advice is also obtained from external risk and insurance brokers/consultants (currently Arthur J Gallagher (AJG)) and Ausgrid's internal insurance specialists to establish the appropriate levels of coverage, implement appropriate insurance market negotiation strategies and to efficiently and effectively manage claims.

Appendix A provides a summary of Ausgrid's key risks and control measures for preventing and mitigating the identified risk.

Ausgrid's Board Policy: Risk Management, Risk Management Plan and Ausgrid's Network Management Plan are available on request.

Figure 1. Bow-tie risk methodology



2.2 Assessing the appropriate regulatory treatment of risks

In considering how best to manage risks from a regulatory perspective, Ausgrid's approach is to ensure that all risks are appropriately provisioned for and allocated to the party best able to bear the risk.

All risks faced by a DNSP are covered by one of the following:

- Forecast operating expenditure— this includes external insurance
- Forecast capital expenditure
- Rate of return
- Self-insurance
- Pass-through
- Not covered/retained by the business (cost impact of the risks is not significant).

In determining which mechanism should be used for efficiently managing a risk, Ausgrid had regard to the nature of the risk and the risk can be managed through prudent risk controls and appropriate levels of commercial insurance. Where this is the case, the cost of managing the risk is covered through forecast opex, forecast capex or the rate of return. The majority of our risks are covered in this way.

However, there are some risks which are beyond our control to prevent and have a low probability of occurrence or are unpredictable. In managing these types of risks, Ausgrid can either self-insure or nominate a pass through event.

'Self-insurance' in the regulatory context refers to setting aside funds as compensation for potential losses in the future, and is distinct from other interpretations of the term which refer to the general practice of retaining potential financial risks and absorbing any potential future losses internally.

In determining whether it would be appropriate to self-insure for certain risks, Ausgrid has regard to whether it is able to 'effectively' self-insure for the risk. That is, whether Ausgrid would have the capacity to effectively pool enough funds to cover the severity of the likely impact should the risk occur.² Other considerations that we also have regard to include:

- Whether the risk is practically quantifiable and does not merely relate to the loss of value³
- Whether the risk is negatively asymmetric⁴
- AER information requirements⁵
- Administrative and reporting requirements.⁶

² For example, the risk of damages from a significant earthquake that is likely to occur less than 1 in 1,000 years. In theory, this risk can be self-insured by saving an annual premium to pay for the earthquake when it occurs. However, if the event occurred prior to 1,000 years (i.e. in year 20) the business would have an insufficient pool of funds to cover the costs of the event.

³ The probability of the event occurring is relevant for quantifying the likely impact of the event (i.e. loss times probability) as it will determine the self-insurance allowance that the AER will likely approve. The AER has stated that the financial impact of the event must be able to be recorded in the building block revenue components (i.e. opex or capex) hence the mere loss of value from the event occurring would not be allowed as self-insurance allowance.

⁴ According to the AER, events could have upside and downside risks. Expressed in a different way this refers to whether an event is characterised by symmetrical or asymmetrical risks. Asymmetric risks can be distinguished from symmetric risks, in the sense that if an asymmetric risk occurred it would only increase a DNSPs' costs whereas symmetrical risks are not always characterised by an increase in costs.

⁵ The AER requested the very detailed information on 'self-insurance' in the regulatory information notice (RIN) it issued to the Victorian DNSPs to substantiate their self-insurance claims. Information required by the AER included details of all amounts and values used to calculate the proposed insurance; an explanation of the methodology; Board resolutions to self-insure; actuary reports verifying the self-insurance premiums; annual accounts recording the cost of self-insurance as an operating expense.

Where Ausgrid determines that it is appropriate to self-insure, we include a forecast allowance as part of our base year opex.

Any residual risks which are not addressed by opex, capex, or the rate of return - are either likely to be catastrophic or insignificant. Where the cost impacts are deemed to be small, such as below insurance deductibles, Ausgrid is likely to be the most appropriate party to bear the costs associated with this event, and as a result will absorb the cost impacts associated with the risk materialising. However, where the likely cost impact from a risk is determined to potentially have a significant cost impact, the risk is further assessed against the PTE considerations contained in Chapter 10 of the NER.

Consequently, in reaching a decision to manage our exposure to certain risks via the nominated pass through provisions, Ausgrid has exhausted all other practicable means for addressing the risk under the regulatory framework. The events that we propose to nominate as pass through events are risks that:

- Are uncontrollable, in the sense that they cannot reasonably or practicably be mitigated or prevented
- Have a low probability of occurrence and are unpredictable
- Cannot be effectively insured, in the sense that external insurance is unavailable on commercial terms or Ausgrid would not have sufficient capacity to pool enough risk to cover the severity of the likely impact should the event occur
- Are not already accounted for in Ausgrid's regulatory proposal
- Are likely to have a significant cost impact
- Falls outside of the defined pass through events in the NER.

Given the nature of these residual risks, we consider cost pass throughs to be the most appropriate and cost efficient means for managing them. We do not consider that self-insurance would be an appropriate means for managing risks of this nature as quantifying a self-insurance allowance would be either subjective (due to the nature of the risk and a wide range of possible values), or could potentially expose the network service provider to catastrophic financial consequences if the risks were to eventuate.

We consider that our approach to cost pass throughs is consistent with the AER's position in relation to these types of events and with the revenue pricing principles in the NEL, and preserves incentives under the Rules framework.⁷

2.3 Consideration of cost impacts to consumers

In determining whether to nominate cost pass through events as part of our regulatory proposal, Ausgrid has regard to the likely cost impacts to customers from adopting this approach. We note that there are no immediate costs to customers from an event being approved by the AER as a nominated cost pass through. In addition, there are no cost impacts to customers if the event does not occur during the regulatory control period.

Costs associated with nominated pass through events (and more broadly cost pass throughs) are only recovered from customers if the event occurs. Even then, it is not automatic that the DNSP will be allowed to pass through the costs associated with the event, as the AER must approve the any application to pass through the cost of the event to customers.

⁶ Electing to self-insure for a risk means that the business must establish formal measures for pooling and managing the risk, and will also need to report the ongoing management of its self-insurance via the RIN, which as noted above is onerous.

⁷ AER, Final Decision: ElectraNet Transmission Determination 2013-14 to 2017-18, 30 April 2013, pp 190-191; AER, Victorian electricity distribution network service providers Distribution determination 2011-2015, Draft Decision June 2010, pp 711-713. See also section 7A(2)(a) and (b) of the NEL.

Cost pass through events (whether prescribed in the Rules or nominated) simply operate as a gateway for network service providers to access the pass through approval process under clause 6.6.1 of the Rules. There are a number of requirements that a DNSP must first satisfy in order for the costs associated from a pass through event to be recovered.

Specifically, a DNSP must first make an application to the AER demonstrating that an event has occurred that:

1. Falls within a prescribed or nominated pass through category
2. Materially increases (decreases) the costs of providing standard control services
3. Sets out the amount that the network service provider proposes should be recovered.⁸

If the DNSP is unable to demonstrate requirements 1 and 2, then the pass through event will not be established and cannot be approved by the AER. Costs are not recovered from customers and the network service provider must absorb the costs from the event.

In addition, just because an event is accepted as an approved pass through does not mean that the AER will approve the amount the DNSP is proposing. In determining the amount, if any, to be passed through, the AER must take into account a number of factors. In the case of a positive change event, the AER must apply an efficiency test to the proposed amount. In particular, it must consider the efficiency of the network service provider's decisions and actions in relation to the event, including whether the provider has failed to take any action that could reasonably be taken to reduce the magnitude of the eligible pass through amount and whether the provider had taken or omitted to take any actions which increased the magnitude of the amount.⁹

Consequently, there are no immediate impacts to customers from the AER approving Ausgrid's nominated pass through events. Approval of these events merely enables Ausgrid to access the pass through approval process under the Rules should the nominated event occur, which in turn provides a mechanism for further analysis and determination by the AER. The approval process provisions enable the AER to apply the same level of scrutiny and assessment to a pass through application as it would to a regulatory proposal, thus ensuring only the efficient costs from the event are recovered.

⁸ Materiality in this context is defined as 1% of the network service provider's annual revenue requirement. Refer to definition of materiality in Chapter 10 of the NER.

⁹ Clause 6.6.1(j), NER.

3 NOMINATED PASS THROUGH EVENTS

Ausgrid nominates the same pass through events that apply to the current period, with some amendments to align the definitions with those approved for other DNSPs. We also propose to explicitly include cyber-attacks in the definition of a terrorism event.

As discussed above, Ausgrid adopts prudent risk and asset management measures to ensure the safety, reliability and security of electricity supply to all of its customers. We are compensated for undertaking risk prevention/mitigation activities under the regulatory framework through allowances under forecast capex, forecast opex (including external insurance and self-insurance), and the rate of return on assets. However, these mechanisms do not provide a return for all the risks that we face as a network service provider and in some instances it may be appropriate to nominate a pass through event.

3.1 Approach for the 2019-24 regulatory period

Ausgrid's operating environment in relation to risk has not significantly changed since we submitted our last regulatory proposal and our risk management framework has remained broadly similar. Consequently, we have decided to conduct a more streamlined assessment approach for determining whether risks should be managed via the cost pass through mechanism for our 2019-24 regulatory proposal.

Our approach was to conduct an internal review to ascertain whether:

- The nominated pass through events that were approved by the AER for the current regulatory period remain appropriate
- Any amendments are required to the definitions for the current approved pass through events
- Any new risks have arisen that may require a pass through event to be nominated.

As a result of this process, we are proposing the same nominated cost pass through events which apply during the current regulatory period, which are set out in Box 1 below. We note that the AER has consistently approved these nominated cost pass through events for almost all DNSPs and TNSPs that have proposed these events as part of their regulatory determinations.¹⁰

Box 1: 2019-24 Nominated cost pass through events

- Insurance cap event
- Insurer's credit risk event
- Natural disaster event
- Terrorism event.

¹⁰ The one exception is Directlink, who applied for but was denied a pass through for Insurer's credit risk event.

Our proposed definitions for each of these events, is outlined in Section 3.2 with any proposed changes from the definition approved by the AER for the current regulatory period marked up. Our explanation for why each of the proposed pass through events meets the PTE considerations is discussed in section 3.3.

The only substantive change to the definitions is to explicitly include cyber terrorism in the definition of terrorism event, which is discussed in further detail below.

3.1.1 Amending the definition of terrorism event to include cyber terrorism

Ausgrid considers that the definition of terrorism should be amended to explicitly consider the impacts of cyber terrorism, as the current definition focuses on physical acts – that is, the use of force or violence. While the definition is not limiting, we consider that the current drafting creates uncertainty as to whether cyber related terrorism such as espionage, sabotage, and coercion fall within the scope of the terrorism event.

We note that in its 2016-20 revenue proposal, Citipower proposed to amend the definition of terrorism event to explicitly include reference to a cyber-attack.¹¹ However as part of its proposed amendments to the definition, Citipower proposed to remove the third limb of factors the AER would have regard in assessing a terrorism event pass through application. That is, the proposed definition removed the requirement that the AER would have regard to, amongst other things, “whether a declaration has been made by a relevant government authority that a terrorism event has occurred”.

The AER’s preliminary decision was to reject Citipower’s proposal to add cyber-attacks to examples of what might constitute an act of terrorism.¹² This was partly due to the AER’s view that such attacks, including the introduction of harmful code or viruses, should be managed through prudent and efficient IT protection.

In response, Citipower argued that a cyber-related attack could occur despite it having taken prudent and efficient actions in accordance with good industry practice.¹³ The AER ultimately accepted that a cyber-related attack could occur despite prudent protection measures.¹⁴ However, the AER did not accept that it was necessary to include a description of cyber-terrorism in the definition. The AER noted that if a cyber-attack has the characteristics of an act of terrorism, then Citipower could apply to have those costs passed through.

Therefore, while it is implicit from the AER’s decision of Citipower’s nominated pass through events that cyber related attacks could fall within the scope of the “terrorism event”, we consider that further amendments are required to provide greater certainty on the regulatory treatment of such events, and also to align the definition with recent market and legislative developments aimed at addressing cyber security concerns.

Cyber security and cyber terrorism are becoming an increasing focus in today’s digital age, with the Commonwealth Attorney General’s Department (Attorney General’s Department) assessing the risk to the Australian economy from computer intrusion and the spread of malicious code by organised crime as high.¹⁵ The Attorney General’s Department further

¹¹ Citipower, Regulatory Proposal 2016-2020, April 2015, p.261

¹² AER, CitiPower Preliminary decision 2016-20, Attachment 15 – Pass through events, October 2015, p.19.

¹³ Citipower, Revised Regulatory Proposal 2016-20, January 2016, 426-428.

¹⁴ AER, CitiPower Final decision 2016-20, Attachment 15 – Pass through events, October 2015, pp.19-20.

¹⁵ <https://www.ag.gov.au/RightsAndProtections/CyberSecurity/Pages/default.aspx>

noted the scale, sophistication and perpetration of cyber-crime was increasing and becoming more difficult to identify and mitigate against, with the distinction between traditional threat actors—hackers, terrorists, organised criminal networks, industrial spies and foreign intelligence services—becoming increasingly blurred.

The increased threat and cascading effect on the Australian economy from cyber related attacks on critical infrastructure is evident by the recent establishment of a Critical Infrastructure Centre in January 2017, and the Security of Critical Infrastructure Act 2018 aimed at managing the national security risks posed to critical infrastructure from espionage, sabotage and coercion.¹⁶

Electricity distribution assets are deemed to be a critical infrastructure by the Critical Infrastructure Centre and the Security of Critical Infrastructure Act 2018. This is because in addition to the significant impact on communities and business from a prolonged disruptions, electricity providers hold large data sets about customers and their electricity usage, which need to be appropriately protected.¹⁷

Cyber security has also been raised as an important issue in the Independent Review into the Future Security of the National Electricity Market ('Finkel review'). The Finkel review recommended that that a stronger risk management framework be implemented, as set out in the Box 2.

Box 2: Stronger cyber security arrangements

The Finkel review raised concerns about the potential vulnerability of the power system to a number of emerging threats, including cyber-attacks. The report recommended a stronger risk management framework be implemented. Specifically, the report recommended:¹⁸

An annual report into the cyber security preparedness of the National Electricity Market should be developed by the Energy Security Board, in consultation with the Australian Cyber Security Centre and the Secretary of the Commonwealth Department of the Environment and Energy.

The annual report should include:

- *An assessment of the cyber maturity of all energy market participants to understand where there are vulnerabilities.*
- *A stocktake of current regulatory procedures to ensure they are sufficient to deal with any potential cyber incidents in the National Electricity Market.*
- *An assessment of the Australian Energy Market Operator's cyber security capabilities and third party testing.*
- *An update from all energy market participants on how they undertake routine testing and assessment of cyber security awareness and detection, including requirements for employee training before accessing key systems.*

While Ausgrid has in place measures to limit the likelihood of a cyber-terrorism event impacting our network, and will work closely with the relevant parties to implement the Finkel review recommendations, we consider that despite these measures a cyber-attack is

¹⁶ Australian Government, Critical Infrastructure Centre, Security of Critical Infrastructure Bill 2017 – Explanatory Document, October 2017, p 7.

¹⁷ Ibid.

¹⁸ Independent Review into the Future Security of the National Electricity Market: Blueprint for the Future, Commonwealth of Australia June 2017, p22.

plausible. In the past five years Ausgrid has had a number of cyber-security incidents, including:

- The CryptoLocker ransomware attack
- A telephone toll fraud
- The Wannacry ransomware attack
- The Petya ransomware attack.

The Australian Cyber Security Centre has also noted that the number, type and sophistication of cyber security threats are increasing.¹⁹ Consequently, Ausgrid is concerned that the increased sophistication and frequency of cyber-attacks may expose Ausgrid to an increased risk of a targeted attack that could affect our ability to comply with regulatory requirements (such as the daily submission of market data), and adversely impact on our business operations for a period of time.

We consider amending the definition of “terrorism event” to explicitly recognise cyber terrorism is appropriate given the changing nature of terrorism. Adopting such an approach is also consistent with the Australian Government’s national security priorities regarding cyber security and recommendations under the Finkel review.

Our proposed amendments to the definition are set out in the Table 1 below. Our suggested drafting changes to the definition are minor in nature, and do not change or remove any of the assessment factors that the AER should have regard to in determining whether a “terrorism event” has occurred. Rather the changes are aimed at providing greater clarity on the scope of “terrorism event,” so that it is more explicit that the event is intended to encompass activities which a non-physical in nature.

3.2 Proposed definitions

Ausgrid’s proposed nominated pass through event definitions are outlined below in a Table 1. As illustrated in Table 1, we have proposed very minor amendments to our previous nominated pass through event definitions. Most of our proposed amendments are aimed at removing the term “materially” from the definition of our nominated pass through events to avoid confusion with the definition of “materiality” in the NER.

The most notable change to our proposed nominated pass through events definitions is to the “terrorism event.” As noted in section 3.1.1 these amendments are considered minor in nature and are primarily aimed at clarifying the scope and nature of activities that would be captured by this event.

¹⁹ Australian Cyber Security Centre, 2015 Threat Report, p.4.

Table 1. Proposed definitions

Pass through event	Proposed definition	Explanation for proposed amendment
Insurer's credit risk event	<p>An insurer's credit risk event occurs if</p> <ul style="list-style-type: none"> A nominated insurer of Ausgrid becomes insolvent, and as a result, in respect of an existing or potential insurance claim for a risk that was insured by the insolvent insurer, Ausgrid: <ul style="list-style-type: none"> is subject to a higher or lower claim limit or a higher or lower deductible than would have otherwise applied under the insolvent insurer's policy; or incurs additional costs associated with funding an insurance claim, which would otherwise have been covered by the insolvent insurer. <p>Note: In assessing an insurer's credit risk event pass through application, the AER will have regard to, amongst other things,</p> <ul style="list-style-type: none"> Ausgrid's attempts to mitigate and prevent the event from occurring by reviewing and considering the insurer's track record, size, credit rating and reputation. In the event that a claim would have been made after the insurance provider became insolvent, whether Ausgrid had reasonable opportunity to insure the risk with a different provider. 	No change from current definition.
Insurance cap	<p>An insurance cap event occurs if:</p> <ul style="list-style-type: none"> Ausgrid makes a claim or claims and receives the benefit of a payment or payments under a relevant insurance policy, Ausgrid incurs costs beyond the relevant policy limit, and the costs beyond the relevant policy limit materially increase the costs to Ausgrid in providing direct control services. <p>For this insurance cap event:</p> <ul style="list-style-type: none"> the relevant policy limit is the greater of: <ul style="list-style-type: none"> Ausgrid's actual policy limit at the time of the event that gives, or would have given rise to a claim, and the policy limit that is explicitly or implicitly commensurate with the allowance for insurance premiums that is included in the forecast operating expenditure allowance approved in the AER's final decision for the regulatory control period in which the insurance policy is issued. A relevant insurance policy is an insurance policy held during the 2019-24 regulatory control period or a previous regulatory control period in which Ausgrid was regulated. <p>Note for the avoidance of doubt, in assessing an insurance cap event cost pass through application under rule 6.6.1(j), the AER will have regard to:</p> <ul style="list-style-type: none"> the relevant insurance policy for the event, and the level of insurance that an efficient and prudent NSP would obtain in respect of the event. 	Removed the reference to materiality so as to avoid confusion with the definition of materiality set out in the NER. This is the approach adopted by the AER in recent determinations for DNSPs. ²⁰

²⁰ See, for example, AER, CitiPower distribution determination final decision 2016-20, Attachment 15, p18.

Pass through event	Proposed definition	Explanation for proposed amendment
Natural disaster event	<p>A natural disaster event occurs if:</p> <ul style="list-style-type: none"> Any major fire, flood, earthquake or other natural disaster occurs during the 2019-24 regulatory control period and materially increases the costs to Ausgrid in providing direct control services, provided the fire, flood or other event was not a consequence of the acts or omissions of the service provider. The term 'major' in the above paragraph means an event that is serious and significant. It does not mean material as that term is defined in the Rules (that is 1 per cent of the DNSP's annual revenue requirement for that regulatory year). <p>Note: In assessing a natural disaster event pass through application, the AER will have regard to, amongst other things:</p> <ul style="list-style-type: none"> whether Ausgrid has insurance against the event, the level of insurance that an efficient and prudent NSP would obtain in respect of the event, whether a relevant government authority has made a declaration that a natural disaster has occurred. 	<p>Removed the reference to materiality so as to avoid confusion with the definition of materiality set out in the NER. This is the approach adopted by the AER in recent determinations for DNSPs.</p>
Terrorism event	<p>A terrorism event occurs if:</p> <p>An act (including, but not limited to, the use of force or violence or the threat of force or violence), <u>attacks or other disruptive activities against critical infrastructure or underlying technology, or the threat of such attacks or disruptive activities, or of the deliberate introduction of malware</u> of any person or group of persons (whether acting alone or on behalf of or in connection with any organisation or government), which from its nature or context is done for, or in connection with, political, religious, ideological, ethnic or similar purposes or reasons (including the intention to influence or intimidate any government and/or put the public, or any section of the public, in fear) and which materially increases the costs to Ausgrid in providing direct control services.</p> <p>Note: In assessing a terrorism event pass through application, the AER will have regard to, amongst other things:</p> <ul style="list-style-type: none"> whether Ausgrid has insurance against the event, the level of insurance that an efficient and prudent NSP would obtain in respect of the event, and whether a declaration has been made by a relevant government authority that a terrorism event has occurred. 	<p>Removed the reference to materiality so as to avoid confusion with the definition of materiality set out in the NER. This is the approach adopted by the AER in recent determinations for DNSPs</p> <p>Included suggested addition to current definition to provide clarity that cyber-terrorism is included.</p>

3.3 Justification for nominated cost pass through events

Table 2 below, sets out our rationale for why our proposed nominated pass through events are required to mitigate our expose to certain low probability high cost impact events.

Table 2. Justification for nominated cost pass through events

Pass through event	Rationale	Application of PTE considerations
Natural disaster event	<p>A 'natural disaster event' cost pass through captures a key category of uncertain, potential high cost impact events outside our reasonable control. Natural disasters typically result in DNSPs incurring substantial costs, including those arising from property damage to network assets. We consider that a pass through represents the most efficient means for managing risks of this nature and, in addition, is consistent with the PTE considerations and pricing principles in the NEL.</p> <p>Whilst there may be some overlap between a 'natural disaster event' and an 'insurance cap event' it is anticipated that both events will be necessary, as the costs associated from third party claims are unlikely to be captured by a 'natural disaster event.' The AER has previously accepted both events.²¹</p>	<p>The proposed 'natural disaster event' is not covered by a category of pass through event specified in clause 6.6.1(a1)(1) to (4) of the Rules.</p> <p>The nature and the type of event can be clearly identified at the time of this determination, as recognised by the AER in its previous determinations.²²</p> <p>Whilst Ausgrid cannot prevent a natural disaster from occurring it does have in place a number of preventative measures in place in relation to potential natural disasters. These include a Bush Fire Mitigation Strategy and locating its assets in geotechnical stable areas. In the event of a natural disaster event, Ausgrid has in place a Emergency Management Plan and Incident Management Process, Incident Management System and Risk Escalation Process which are designed to ensure that impacts from such events are minimised and managed in a coordinated and timely manner</p>

²¹ The AER has made the following observation in relation to the natural disaster event: "The AER recognises that there is some potential overlap with other allowances or events such as liability above the insurance cap. However, it will consider any specific cost claim under the most appropriate event and ensure it is not double counted." See AER, *Draft Distribution Determination, Aurora Energy Pty Ltd 2012-13 to 2016-17*, November 2011, p 39.

²² For example, AER, *Victorian electricity distribution network service providers distribution determination 2011-2015, Draft Decision*, June 2010; AER, *Final Distribution Determination, Aurora Energy Pty Ltd 2012-13 to 2016-17*, 30 April 2012; AER, *Final Decision – ElectraNet Transmission Determination 2013-14 to 2017-18*, 30 April 2013.

Pass through event	Rationale	Application of PTE considerations
Insurance cap	The probability of incurring liabilities above our insurance limit is extremely low, commercial and self-insurance are not available on reasonable grounds and the cost impacts from such an event would be catastrophic.	<p>The event is not covered by a category of pass through event specified in clause 6.6.1(a1)(1) to (4) of the Rules; The nature and type of the event can be clearly identified at the time the AER makes its determination for Ausgrid, as evidenced by the proposed definition and the fact that the AER has previously accepted this event for other DNSPs and Ausgrid.</p> <p>The extent to which Ausgrid can reasonably prevent a claim occurring which exceeds its insurance cap, or can mitigate the cost impact of such an event, is limited. We note that the AER has previously concluded that an insurance cap event satisfies this consideration in its most recent determinations for all other DNSPs.</p> <p>Ausgrid has obtained efficient levels of insurance cover commensurate with our assessment of our business risk. However, the coverage of such insurance is typically capped, with levels of cover above the cap typically requiring higher premiums. Ausgrid has not sought to take out higher levels of insurance to mitigate our exposure to such an event, as we believe that such a response would be inefficient and also disproportionate given the low probability of us incurring liabilities above our insurance cap. Including an insurance cap event as a pass through event represents a more appropriate means for managing Ausgrid's risk exposure to such an event given the:</p> <ul style="list-style-type: none"> • Complexity associated with developing credible self-insured risk quantifications for very low probability events, such as those that are above existing liability limits/caps; and • Catastrophic nature of such an event – given Ausgrid's existing policy limits.²³
Insurer's credit risk event	Ausgrid has in place a number of mitigation strategies to avoid being in a situation where one of its insurer's becomes insolvent. However, whilst the likelihood of this risk materializing is very low it is not improbable. Consequently, to manage our exposure to any of our insurer's becoming insolvent, Ausgrid proposes an 'insurer's credit risk event' to apply during its 2019-24 regulatory control period.	<p>The event is not covered by a category of pass through event specified in clause 6.6.1(a1)(1) to (4) of the Rules. The nature and the type of event can be clearly identified at the time of this determination, as recognised by the AER in previous determinations.</p> <p>Ausgrid seeks to mitigate the risk of any of insurers becoming non-viable by regular monitoring and reporting by the broker of insurer Standard & Poor (S&P) rating movements. Our minimum acceptable insurer S&P rating is A-. Also multiple insurers are used on the Ausgrid's liability and Industrial Special Risks (ISR) insurance policies, therefore spreading the risks amongst several insurers and minimises our reliance on any one insurer. We also endeavour to keep liability insurance exposure to A-insurers to less than 10% and our brokers AJG monitor insurer ratings to ensure that any changes are flagged as soon as possible. Our brokers cannot and do not guarantee the security of our insurers.</p> <p>It is not economically viable for Ausgrid to insure (commercial and self-insurance) against this event as the probability of this occurring is extremely low. Further, given the risk mitigation strategies outlined above, it is not viable to commercially insure this risk with another insurer.</p>

²³ Refer to Appendix A for further details on policy limits.

Pass through event	Rationale	Application of PTE considerations
Terrorism event	<p>Ausgrid proposes that a 'terrorism event' be included as a pass through event, as part of its regulatory determination for the 2019-24 regulatory control period, as this represents the most prudent and efficient means for managing a risk of this nature in its forthcoming regulatory control period.</p> <p>Whilst Ausgrid does have some commercial insurance that would likely be triggered if a terrorism event occurred, this is likely to be insufficient in mitigating the cost impacts from such an event.</p> <p>Where a terrorism event occurred which enabled an existing commercial policy to be called upon, this would reduce the costs incurred directly by Ausgrid and therefore reduce the amount claimed under any cost pass through.</p>	<p>The proposed 'terrorism event' is not covered by a category of pass through event specified in clause 6.6.1(a1)(1) to (4) of the Rules;</p> <p>The nature and type of the event can be clearly identified at the time the AER makes its determination for Ausgrid, as evidenced by the proposed definition, use in previous AER determinations and the fact that the event was previously prescribed in the Rules.</p> <p>Ausgrid's ability to reasonably prevent a terrorism event from occurring and/or substantially mitigate the cost impact from the event is limited. Whilst the occurrence of a terrorism event is largely beyond our control to prevent, we in have place a number of prudent measures to reduce the likelihood of such an event from occurring. These include:</p> <ul style="list-style-type: none"> • Ausgrid has an ongoing program to meet its obligations in relation to infrastructure security. • Participation in joint security risk assessments of Ausgrid assets with the NSW Counter Terrorism Branch, Ministry of Policy and Emergency Services, which has resulted in 62 Ausgrid sites being classified as 'critical infrastructure.' • For each of its critical infrastructure sites Ausgrid undertakes a combination of staff site visits and contracted security service provider visits once every 24 hours, to identify any breaches in the perimeter barrier of a site. • Ausgrid personnel also undertake monthly inspections of all of our major substations to detect any breaches of the perimeter and/or any attempted intrusions. • Ausgrid inspects and risk assesses all physical perimeter security measures annually. <p>Ausgrid has commercial insurance cover which would likely be triggered by an act of terrorism. However, Ausgrid does not have specific cover for cyber security. The market for cyber insurance is developing and Ausgrid is reviewing its cyber risks and insurance cover prior to effecting insurance cyber insurance.</p> <p>The potential magnitude of the cost impact of a terrorism event means that it is a risk that Ausgrid believes cannot be credibly self-insured.</p>

4 APPLICATION OF PASS THROUGH PROVISIONS TO ALTERNATIVE CONTROL SERVICES

Ausgrid considers the AER should clarify that the pass through framework applies to ACS. Ausgrid also considers the definition of 'materially' in the context of ACS should be clarified, as well as the appropriate mechanism to recover pass through amounts.

Ausgrid proposes that the pass through provisions for defined and nominated pass through events apply to alternative control services on the basis that the pass through provisions in the Rules apply to direct control services, which applies to both standard control services and alternative control services.²⁴

We note that the AER agreed with CitiPower's proposal (as well as the four other Victorian Distribution Network Service Providers (DNSPs) that nominated pass through events include alternative control services (ACS).²⁵ This means that DNSPs may apply to pass through an increase (or decrease) in costs incurred in providing both standard control services (SCS) or ACS. This is consistent with the prescribed pass through event definitions set out in the NER, which also reference direct control services. Ausgrid agrees and supports the AER's decision on this point.

We note that the AER's final decision for the NSW DNSPs 2014-19 determination was silent on whether it accepted Ausgrid's proposal to apply the pass through framework to ACS.²⁶ For the avoidance of any doubt and for consistency with more recent determinations, Ausgrid considers that the AER should make it clear that the pass through framework applies to ACS. This is important as the risks faced by DNSPs in relation to these services are the same as those faced in providing SCS, and the availability of cost pass through provisions is consistent with the basis of the control mechanisms which have been developed in relation to those services.

In addition, to specifying that the pass through framework applies to ACS that the AER should clarify whether the:

- **Definition of 'materially' to be applied in assessing an ACS pass through application.** While the NER defines 'materially' as 1 per cent of the revenue requirement, the concept of an annual revenue requirement is only applicable to SCS. The characteristic and nature of ACS differs to that of SCS, which are more broad and general in nature, whereas ACS services are more bespoke and customer specific. Given these differences, it may be more appropriate to assess the materiality of an ACS pass through application as 1 per cent of the revenue for the impacted alternative control service rather than 1 per cent of the annual revenue requirement.
- **The appropriate mechanism to recover the approved pass through amount.** We note that the AER indicated in its determination of CitiPower, that any approved ACS pass through amount would be recovered via an adjustment to SCS. Ausgrid notes that an alternative option would be to recover an approved pass through amount via an

²⁴ Refer to Chapter 10 of the NER – definitions of 'negative change event', 'positive change event', 'regulatory change event', 'tax change event', 'service standard event', and 'retailer insolvency event.' See also Ausgrid proposed definition for its proposed nominated pass through events for 'an insurance cap event,' 'natural disaster event', 'terrorism event' and 'insurer's credit risk event.'

²⁵ AER, CitiPower distribution determination final decision 2016-20, Attachment 15 – Pass through events, p9.

²⁶ See Ausgrid's regulatory proposal, 1 July 2014 to 30 June 2019, 30 May 2014, page 29 and Attachment 4.13 to that proposal.

adjustment to ACS prices, as this would provide a more cost reflective basis for recovery.

APPENDIX A: APPLICATION OF PASS THROUGH PROVISIONS TO ALTERNATIVE CONTROL SERVICES

This Appendix sets out additional details on how Ausgrid manages its key risks.

Table A.1 – Summary of key risks and how they are managed

Risk	Description	Risk management approach	Treatment of residual risk
Asbestos	Liability for claims related to the impact of asbestos (both retrospectively and prospectively) on employees and third parties	<p>There are two components to the risk: (1) the risk of exposure to customers and the community; and (2) the risk of exposure to workers and contractors</p> <p>Insurance</p> <ul style="list-style-type: none"> (1) is dealt with via Ausgrid's Liability Insurance policy for limited cover up to [REDACTED] and Ausgrid's asbestos removal cover up to [REDACTED] (2) is dealt with through Ausgrid's self insurance for workers compensation <p>Risk controls</p> <ul style="list-style-type: none"> Asbestos awareness training Asbestos safety management plan Risk management policy and framework 	Residual risks above insurance cap amounts to be managed via the 'insurance cap event'
Gradual pollution	Unintentional pollution of the surrounding environment from underground fuel tank leakage, transformer oil, contamination from treated poles etc	<p>Risk controls</p> <ul style="list-style-type: none"> Environmental policy Risk management policy and plan 	Risk is retained by the business
Electric and magnetic fields (EMF)	Adverse health impacts caused by EMF and regulatory changes impacting the undertaking of "live line" work	<p>Insurance</p> <ul style="list-style-type: none"> Liability policy subject to \$100k deductible <p>Risk controls:</p> <ul style="list-style-type: none"> Environmental policy Monitoring of global research and developments 	Residual risks for above insurance cap amounts to be managed via the 'insurance cap event'

Risk	Description	Risk management approach	Treatment of residual risk
Business continuity	Future incidents/events that could significantly impact on the business' ability to continue business as usual	Insurance <ul style="list-style-type: none"> Limited cover through Ausgrid's Industrial Special Risks(ISR)/ property insurance Risk controls <ul style="list-style-type: none"> Emergency evacuations plans Incident management plans Facility incident response plan Business continuity plan 	Residual risk is retained by the business
Theft of assets	Risk of theft from employees and external parties	Insurance - covered by Ausgrid's ISR/property policy subject to a \$200k deductible Risk controls: <ul style="list-style-type: none"> CCTV Secure premises and security patrols 	Residual risks above insurance cap amounts to be managed via the 'insurance cap event'
Fraud	Theft, false accounting, bribery and corruption, deception and collusion	Insurance <ul style="list-style-type: none"> Covered by Ausgrid's crime policy with Risk controls: <ul style="list-style-type: none"> Inventory, bank and computer controls Limited cash on premises Audits and information security policy Fraud management policy 	Residual risks above insurance cap amounts to be managed via the 'insurance cap event'
Bomb threat/hoax, terrorism, Earthquakes, bushfire, non-terrorist impact of planes and helicopters and substations		Insurance <ul style="list-style-type: none"> Broadly covered by Ausgrid's liability policy insurance Terrorism, earthquakes, and property also being covered under Ausgrid's ISR/property policy Risk controls: <ul style="list-style-type: none"> Emergency evacuation plans Incident management plans Business continuity plans Security arrangements Bushfire risk management plan Strategic asset management plan 	<p>Risk for non-terrorist planes to be managed via an 'insurance cap event'</p> <p>Residual risks from bushfires, earthquakes and other natural disasters are to be managed via a 'natural disaster event' and 'insurance cap event' (depending on what is deemed to be appropriate by the AER.</p> <p>Residual risk from bomb threats and hoaxes are to be retained by the business</p> <p>Exposure to terrorism events are to be managed via a 'terrorism' event.</p>

Risk	Description	Risk management approach	Treatment of residual risk
Insurer's credit risk	Potential for insurer to default on promise to pay claims as well as the loss of premium paid upfront	Insurance – none Risk controls: <ul style="list-style-type: none"> • Use of multiple insurers where possible • Only accept insurers with S&P rating of A- or higher (or agencies with a similar rating) • Regular reporting on credit worthiness from brokers 	Exposure to be managed via an 'insurer's credit risks event' Residual risk of insurer's default without becoming insolvent is to be retained by the business
Counter party credit risk	Probability of retailer defaulting on payment obligations	Insurance – None Risk controls: <ul style="list-style-type: none"> • Existence of a credit manager role • Risk management policy • Counter party credit reviews • Security deposit if deemed appropriate 	Exposure managed via retailer insolvency pass through event
General public liability	Injuries or losses suffered by the general public as a result of Ausgrid's negligence	Insurance – covered by Ausgrid's liability policy subject to \$100k deductible except for bushfire property damage which is \$10m deductible Risk controls: <ul style="list-style-type: none"> • Network management framework • Public electrical safety awareness plan 	Residual risks for above insurance cap amounts to be managed via the 'insurance cap event'
Poles and lines	Exogenous incident causes damage to distribution network	Insurance – None Risk controls: <ul style="list-style-type: none"> • Recovery actions against third parties • Vegetation controls • Regular inspections • Asset management plan (Strategic Asset Management Plan) 	Residual risk absorbed by the Ausgrid
Power quality	Electricity supplied falls outside of statutory limits or perceived "good electricity practice"	Insurance – Ausgrid's liability insurance policy defective supply and failure to supply subject to \$100k deductible. Risk controls: <ul style="list-style-type: none"> • Maintenance of network • NECF/contractual arrangements 	Residual risks above insurance cap amounts to be managed via the 'insurance cap event'
Workers compensation	Substantial increase in workers compensation claims as a result of a cause outside of the control of the business	Insurance – self insure Risk controls: <ul style="list-style-type: none"> • Safety strategic plan • Excess of loss for Ausgrid 	Premiums covered via a regulatory allowance for self-insurance

A.1. Alignment between insurance cover and hazardous events

The maintenance of comprehensive insurance policies is an effective treatment action that transfers the financial risk associated with a hazardous event to the insurer. Ausgrid holds insurances that, in full or in part, limit the financial impact of each of our 34 operational hazardous events. Details of Ausgrid's insurance cover held to minimise the financial impact of the operational risks are provided in the Table A.1.1 below. Note the table includes any self-insured retention (SIR) amount and the limit/sum insured of the insurance policy concerned. That is, SIR in this context refers to the cost impact that Ausgrid absorbs or retains in the event of a risk materializing. The insurance policy limits have been arrived at by appropriate procedures including in conjunction with Ausgrid's insurance brokers.

In addition, Directors & Officers (D & O) insurance, which could apply to most areas and so has not been specifically drawn out in the table, covers the following:

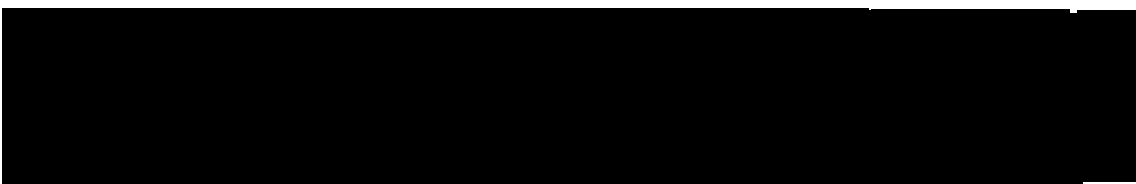


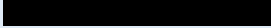





























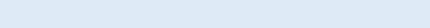

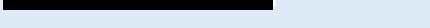






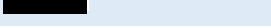


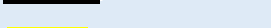














Table A.1.1 - Key risks and how they are managed

BR No.	Hazardous Event	Residual Risk Rating	SIR Limit	Insured Limit	Mitigating Insurance
1.1	Uncontrolled discharge or contact with electricity	High	<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div>
1.2	Exposure to hazardous materials	Medium	<div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div> <div></div>	<div></div> <div></div> <div></div> <div></div> <div></div>
1.3	Fall from height	High	<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div>	<div></div> <div></div> <div></div>

BR No.	Hazardous Event	Residual Risk Rating	SIR Limit	Insured Limit	Mitigating Insurance
1.11	Exposure to hazardous manual tasks	High	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
1.12	Uncontrolled release of a pressurised substance	Medium	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
1.13	Slips, Trips and Falls (excluding fall from height)	Medium	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
1.14	Exposure to environmental elements (heat & cold)	Medium	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
1.15	Exposure to non-ionising radiation	Medium	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
1.16	Incident while working at depth or in a confined space	High	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
1.17	Striking object with part of the body	Medium	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
1.18	Exposure to sound or sound pressure	Medium	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
1.19	Exposure to a biological hazard including flora/fauna	Medium	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
2.1	Performance of the Network is inadequate to meet customers' supply expectations	High	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>
2.2	The Network has insufficient capacity/capability to meet the demands placed on it	Medium	<div><div></div></div>	<div><div></div></div>	<div><div></div></div>

BR No.	Hazardous Event	Residual Risk Rating	SIR Limit	Insured Limit	Mitigating Insurance
2.3	A major fire caused by the Network or Network activity	Medium			
2.4	Loss of Upstream supply	Medium			
3.1	Loss of, or damage to, a physical organisational asset	High			
3.2	Claim for loss of, or damage to, a Third Party (excluding bushfire)	Medium			
3.3	Unbudgeted shortfall in finance due to unfavourable changes in revenue and/or costs	Medium			
3.4	Financial loss due to Retailer non-payment	Low			
3.5	Material adverse movement relating to significant foreign exchange exposure	Low			
3.6	Untimely TSA delivery and transition	Low			
4.1	Disputes leading to litigation and/or arbitration	Medium			
4.2	Non-compliance with legislation or license conditions	Medium			
4.3	Corrupt conduct by an employee, consultant or contractor	Medium			
5.1	Misalignment between Community expectations and management decisions	Medium			

BR No.	Hazardous Event	Residual Risk Rating	SIR Limit	Insured Limit	Mitigating Insurance
5.2	Ineffective management response to an incident/crisis	Medium			
5.3	Failure to embed National Energy Customer Framework requirements	Medium			
6.1	Polluting the environment	Medium	  	 	   
6.2	Unauthorised development or damage to flora, fauna or heritage	Medium			
6.3	Inappropriate management of waste and contaminated materials	Medium	  	 	   
6.4	Emissions causing nuisance to the community	Medium	  	 	   
7.1	Poor cultural alignment following new Operating Model implementation	Medium			
7.2	Loss of key knowledge and/or experience	Medium			
8.1	Failure to develop a robust Strategy	Medium			
8.2	Failure to deliver Strategy	Medium			
9.1	Loss of ICT & OT service	High	  	  	  
9.2	Breach of data integrity and/or security	Medium	 	 	