CitiPower, Powercor and United Energy:

ICT Risk Monetisation Framework

1 August 2024

Building a better working world

RELEASE NOTICE

Ernst & Young ("EY") was engaged on the instructions of CitiPower, Powercor and United Energy ("Client") to develop an ICT Risk Monetisation Framework (“Project”), in accordance with the engagement agreement dated 13 June 2024 including the General Terms and Conditions (“the Engagement Agreement”).

The results of EY’s work, including the assumptions and qualifications made in preparing the report, are set out in EY's report dated 1 August 2024 ("Report"). You should read the Report in its entirety including any disclaimers and attachments. A reference to the Report includes any part of the Report. No further work has been undertaken by EY since the date of the Report to update it.

Unless otherwise agreed in writing with EY, access to the Report by any party other than the Client (the Recipient) is made only on the following basis and in either accessing the Report or obtaining a copy of the Report the Recipient agrees to the following terms.

1. Subject to the provisions of this notice, the Report has been prepared for the Client and may not be disclosed to any other party or used by any other party or relied upon by any other party without the prior written consent of EY.

2. EY disclaims all liability in relation to any other party who seeks to rely upon the Report or any of its contents.

3. EY has acted in accordance with the instructions of the Client in conducting its work and preparing the Report, and, in doing so, has prepared the Report for the benefit of the Client, and has considered only the interests of the Client. EY has not been engaged to act, and has not acted, as advisor to any other party. Accordingly, EY makes no representations as to the appropriateness, accuracy or completeness of the Report for any other party's purposes.

4. No reliance may be placed upon the Report or any of its contents by any party other than the Client. Any party receiving a copy of the Report must make and rely on their own enquiries in relation to the issues to which the Report relates, the contents of the Report and all matters arising from or relating to or in any way connected with the Report or its contents. No duty of care is owed by EY to any Recipient of the Report in respect of any use that the Recipient may make of the Report. EY disclaims all liability, and takes no responsibility, for any document issued by any other party in connection with the Project.

5. The Report is confidential and must be maintained in the strictest confidence and must not be disclosed to any party for any purpose without the prior written consent of EY.

6. The Recipient must not name EY in any document prepared by the Recipient that is to be lodged or filed by you with any regulator or is to be made publicly available (“Public Document”) without EY’s prior written consent, which may be granted at EY’s absolute discretion. If the Recipient is required by applicable laws or regulations to name EY in any Public Document, the Recipient may do so provided it has given EY prior written notice, if such prior written notice is permitted by applicable laws or regulations.

7. The Recipient of the Report:

   (a) may not make any claim or demand or bring any action or proceedings against EY or any of its partners, principals, directors, officers or employees or any other Ernst & Young firm which is a member of the global network of Ernst Young firms or any of their partners, principals, directors, officers or employees ("EY Parties") arising from or connected with the contents of the Report or the provision of the Report to the Recipient; and
   (b) must release and forever discharge the EY Parties from any such claim, demand, action or proceedings.

8. In the event that the Recipient discloses the Report to a third-party in breach of the terms of this notice ("Breach Event"), the Recipient will be liable for all claims, demands, actions, proceedings, costs, expenses, loss, damage and liability made or brought against or incurred by EY or EY Parties, arising from or connected with the Breach Event.

Table of contents

1. Introduction

1.1 Purpose

CitiPower, Powercor and United Energy (CP/PAL/UE) engaged EY to prepare an ICT Risk Monetisation Framework. This document sets out that framework.

The ICT Risk Monetisation Framework describes the approach used by CP/PAL/UE to identify, classify and quantify risks associated with information and communication technology (ICT) projects.

The purpose is to help inform an optimal set of ICT investments by providing a consistent framework for assessing the annual value, in dollar terms, of relevant business and ICT risks under different investment options.

Where a proposed ICT project has a number of options with different risk profiles, having a consistent framework to assign a monetised value to the residual risk in each option enables the net economic benefit of different investment options to be compared, so that the option that delivers the best net economic value can be selected.

A well-defined and consistent framework for valuing risk reduction, alongside other ICT project benefits, promotes a consistent and rigorous approach to Value Based Decision Making (VBDM) during ICT investment planning.

1.2 Scope

The ICT Risk Monetisation Framework comprises:

- A standard set of risks that may be relevant to ICT projects
- For each risk, the method to be used to estimate the likelihood of the negative outcome contemplated by the risk eventuating and the monetised consequence should the negative outcome occur
- A standard set of input metrics that are relevant to the estimation of likelihood or consequence for the risks, and the source to be used for these inputs
- A bottom-up methodology for quantifying risks.

This framework is intended to be used only for ICT projects. Non-ICT projects may consider similar risks, but the methods and inputs used to calculate changes in risk likelihood and consequence under different investment scenarios will be different for different kinds of investment.

The standard set of risks included in this framework document is not intended to be exhaustive. EY does not offer an opinion regarding the extent to which the risks included herein may or may not eventuate, or may or may not be mitigated through ICT investments; that will be assessed by CP/PAL/UE on a case-by-case basis during the preparation of ICT investment cases.

1.3 Alignment

The ICT risk monetisation approach adapted by CP/PAL/UE in the businesses' 2021-26 regulatory proposals to the Australian Energy Regulator (AER) has been used as the basis for this ICT Risk Monetisation Framework. It aligns with CP/PAL/UE's corporate Enterprise Risk Management Framework[1], Framework Value[2] and Investment planning value framework[3], as part of the broader

[1] See 13-10-CPPCUE0005 Enterprise Risk Management Framework
[2] See STR-0006 Framework Value
[3] Investment planning value framework (Copperleaf) – need citation, current copy appears to be in draft

Enterprise Risk Management Framework[4] that governs risk management across CP/PAL/UE's network assets.

The framework also aligns with the National Electricity Rules (NER) and the guidance provided by the AER in its Better Resets Handbook[5].

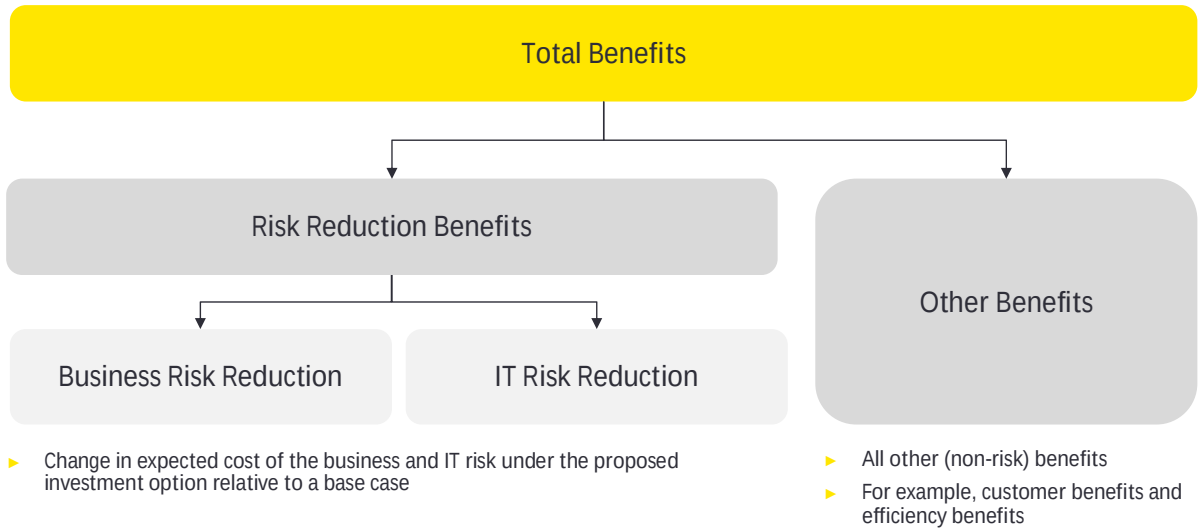
[4] See CPPCUE005 Enterprise Risk Management Framework
[5] AER, *Better Resets Handbook – Towards Consumer Centric Network Proposals*, December 2021

2. ICT Risk Monetisation Framework

2.1 Risk monetisation as part of a cost-benefit analysis

The purpose of risk monetisation is to translate an identified risk – for example, the risk that customers' smart meters cannot be read due to a failure of CP/PAL/UE's ICT systems – into an annualised dollar figure. Where certain investments reduce risk and hence reduce the cost of risk, this reduction is a benefit that sits alongside other benefits in an investment case.

Figure 1 - Risk monetisation as part of cost-benefit analysis



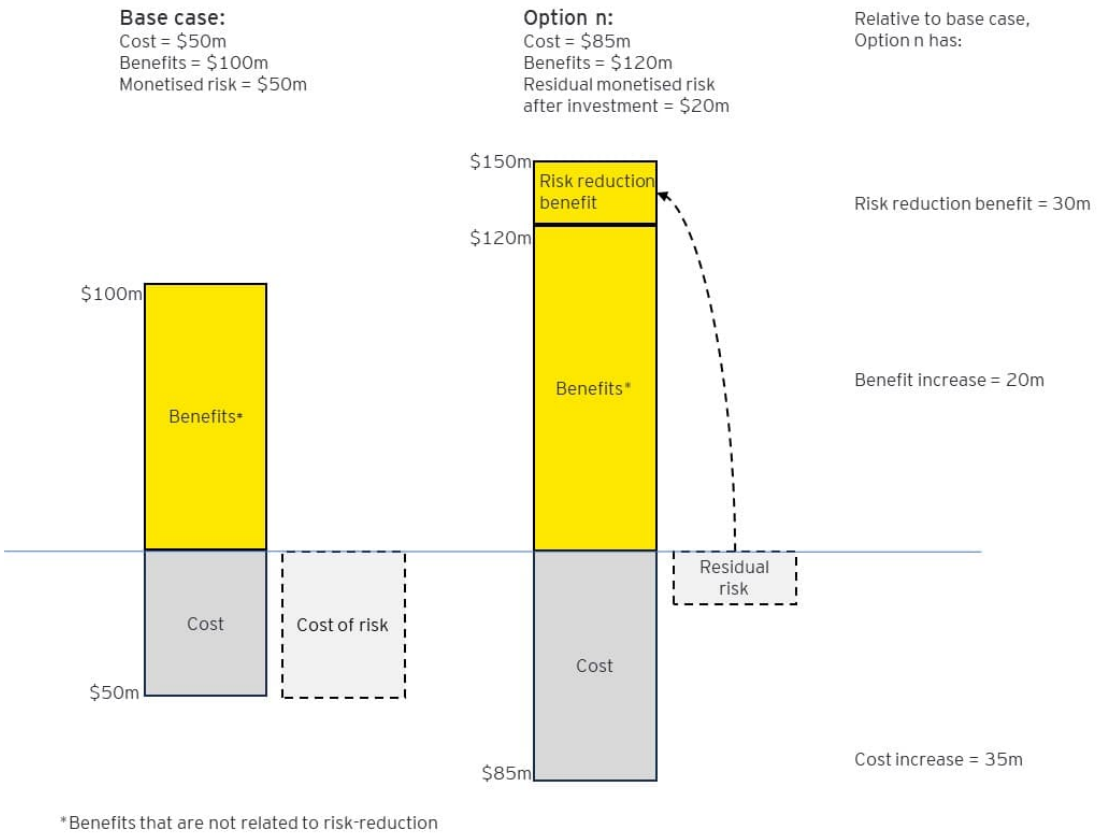
The annual risk cost is calculated based on the likelihood of the risk eventuating in any given year multiplied by the expected dollar cost incurred if the risk eventuates. Likelihood could be informed by historical records of similar faults occurring, and the cost of consequence could be based on customers' lost value or the cost of penalties for non-compliance with regulatory obligations.

To the extent that an ICT investment is expected to reduce a given risk, the risk monetisation framework enables that reduction in risk to be incorporated as part of a cost-benefit analysis as follows:

- Calculate the annual cost of the risk in the base case, i.e. without the proposed investment.
- Re-calculate the annual cost of the risk post-investment, taking into account the impact of the investment on reducing likelihood and/or consequence.
- The difference in annualised cost of risk between the base case and the investment case is a financial benefit stream that can be used, along with any other quantified benefits expected from the investment, to determine whether the proposed investment is likely to be economic.

Figure 2 illustrates this process.

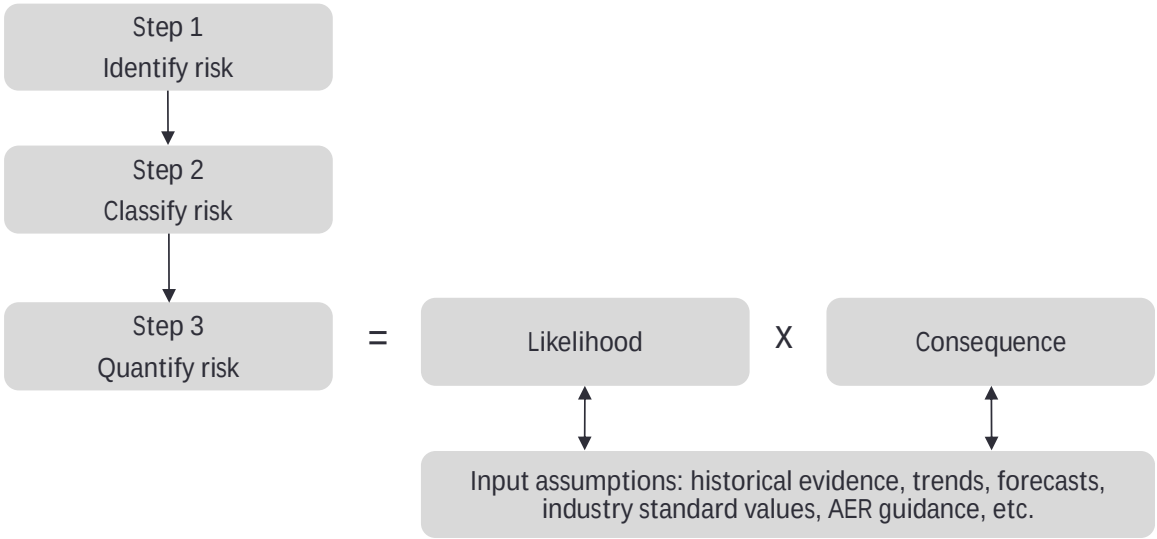
Figure 2 - Comparing investment options including monetised risk



2.2 Risk monetisation process

The risk monetisation process is illustrated in Figure 3 and described further below.

Figure 3 - Risk monetisation process



2.3 Step 1: Identify risk

The first step is to identify a specific risk, that is, a negative consequence, that could arise. For the purpose of applying this framework, a risk should be:

- Able to be described clearly and unambiguously
- Clearly related to ICT investment, i.e. a risk that can reasonably be modified in either likelihood or consequence by investment in, or failure to invest in, ICT systems
- Credible, i.e. with a credible likelihood of occurring within the forward horizon used for investment planning
- Material, i.e. expected to give rise to an annual risk cost that is non-trivial and likely to be relevant in the comparison of ICT investment options
- Quantifiable, i.e. having a reasonable basis to estimate both likelihood and consequence, ideally based in evidence
- Unique, i.e. a risk should stand alone and not overlap with any other risk, to avoid the possibility of double-counting.

This framework document sets out a standard list of risks that could be considered for ICT investment decisions. Only certain risks will be applicable to any given ICT cost-benefit analysis, and the extent to which each risk herein meets the above criteria will depend on the nature of the investment being proposed.

2.4 Step 2: Classify risk

Each risk is assigned to a risk category, which guides the method and inputs to be used to quantify the risk.

The framework comprises six Business Risk categories and two ICT Risk categories, as summarised in the tables below. The categories and their descriptions are drawn from CP/PAL/UE's existing risk framework documentation with one exception: the two previous ICT risk categories of Suitability and System Sustainability have been combined into one. This is because CP/PAL/UE's experience quantifying these risks separately in previous business cases found that these categories were often hard to separate in practice.

Table 1: CP/PAL/UE risk categories – business risks

Business Risks	
Category	Description
Reliability impact	Capture the impact of an event or a failure which would cause the organisation to incur any unforeseen impacts to supply or export capability.
Compliance risk	Risk of legal or regulatory sanction, financial or reputational loss arising from failure to abide by the commercial compliance obligations required (i.e. Australian Energy Market Operator (AEMO), AER and Essential Services Commission (ESC))
Bushfire risk	Outages of the operational technology interfaces that provide visibility of the network may increase bushfire risk by preventing operators from making accurate and timely decisions.
Safety risk	Considers safety risk to the public and staff including network electrical safety, works practices and workplace risk (not including bushfire risk) For example: • Re-energising a section of the network that is expected to be de-energised for planned maintenance works • Disruption of power to customers who rely on life support equipment
Customer experience risk	Outages, data breaches involving customer information that will adversely impact customer interactions.
Financial loss	Direct financial consequence not otherwise taken into account in any of the above areas of consequence.

Table 2: CP/PAL/UE risk categories – ICT risks

ICT Risks	
Category	Description
Outage	Outages may be caused due to poor infrastructure currency and insufficient infrastructure resource capacity (e.g. server memory). Outage resolution may be prolonged due to unavailability of appropriate technical resources (e.g. vendor support) or available replacement hardware through not refreshing software after it reaches end of life.
Suitability and sustainability	Legacy, unmaintained systems are more prone to failures, data loss and security breaches. This can affect CP/PAL/ UE's ability to meet regulatory and compliance requirements such as customer management, financial and market reporting obligations. E.g. data loss occurring due to not having enough data storage. Unplanned maintenance more likely to lead to failures. Increased spend on workarounds. If systems are not refreshed, they will not be compatible with associated market products when reaching End of Life, such as security patches. Ensuring continued access to patches through refreshes would reduce vulnerabilities to cyber security attacks. In addition, refreshing would ensure additional costs from maintaining inefficient, unconsolidated systems are not incurred.

2.5 Step 3: Quantify risk

Risk is quantified as:

Monetised risk = likelihood x consequence

2.5.1 Likelihood

Likelihood is defined as the probability of the negative outcome occurring in any given year. A risk that is expected to eventuate once in every five years has likelihood value of 0.2, a one-in-ten-year event has a likelihood value of 0.1, and so on.

For many risks, the likelihood may be estimated directly as an annual probability, e.g. using historical evidence of the frequency of some event occurring. For certain kinds of risk, it may be appropriate to break down the estimation process further and calculate likelihood based on the intrinsic probability that some trigger condition may arise, which may be due to external factors outside of CP/PAL/UE's control, and the probability that the trigger condition would lead to the negative consequence, which may be something that could be changed by ICT investments designed to mitigate the risk. CP/PAL/UE's framework for assessing cyber security risks takes this latter approach, as summarised in section 3.3 below.

The framework is not intended to be prescriptive in this regard: likelihood should be estimated in the manner that is most appropriate for the risk in question based on the relevant evidence at hand.

2.5.2 Consequence

Consequence is defined as the dollar cost incurred when the risk eventuates. This may be an internal cost, e.g. lost productivity calculated based on the hourly rate for staff affected, a customer cost, e.g. the cost of a loss of electrical supply calculated using the AER's Value of Customer Reliability (VCR), or some other external cost, e.g. the cost of increased carbon emissions.

To calculate consequence values, the risk monetisation framework uses one of two methods, depending on whether the risk in question is a business risk or an ICT risk.

2.5.2.1 Consequence for business risks

For business risks, consequence is estimated using the Johnson modification of the Pearson–Tukey formula[6]. The formula uses a triangular (three-point) probability distribution to convert individual estimates of best case, worst case and most likely cost outcomes into a single figure, as shown below:

$$consequence\ value\ = \frac{3\ \times\ best\ case\ +\ 10\ \times\ most\ likely\ +\ 3\ \times\ worst\ case}{16}$$

The individual inputs of best case, most likely and worst case are estimated individually for each risk.

For consequences that apply at a whole-of-business level rather than a project level, a single value of consequence based on the standard values from CP/PAL/UE's Investment Planning Value Framework (Copperleaf) may be used instead of the above formula.

2.5.2.2 Consequence for ICT risks

For ICT risks, consequence is estimated as the sum of two components:

1. The lost productivity of workers who rely on the system in question, if the system is unavailable. This is estimated based on the number of affected users, the system downtime and the expected impact on productivity, which can vary depending on the level of dependence the users have on the systems to perform their work and the extent to which alternatives or workarounds such as manual processes are available.

2. The cost to rectify the issue. This can be estimated based on the expected number of staff hours required to fix the issue, plus any fixed costs (e.g. vendor costs or replacement equipment).

2.5.3 Disproportionality factors

Disproportionality factors are additional multipliers applied to the value of consequence for risks involving harm to people, harm to property, fire danger or harm to the environment. They are intended to capture the fact that the business has an extremely low tolerance to certain risks and hence assigns a higher value to investments intended to mitigate them than the value given by standard metrics such as the Value of Statistical Life (VSL)[7].

CP/PAL/UE's Framework Value defines the following disproportionality factors:

Table 3- Disproportionality factors

Category	Value
Harm to property from network	1
Harm to property from bushfire	1
Harm to environment	1
Safety – Public trespass	1
Safety – Single fatality of serious injury (public or worker)	3
Safety from Bushfire in Hazardous Bushfire Risk Area	3
Safety – Multiple fatality of serious injury (public or worker)	6

[6] Johnson, D., *Triangular Approximations for Continuous Random Variables in Risk Analysis*, Journal of the Operational Research Society, vol. 53, no. 4, pp. 457-467, 2002

[7] Australian Government, Department of the Prime Minister and Cabinet, Office of Impact Analysis, *Guidance note: value of statistical life*, October 2023

Category	Value
Safety from Bushfire in REFCL declared area	6
Safety from Bushfire in Electric Line Construction areas	10

3. Guidance on application of the ICT Risk Monetisation Framework

3.1 Overview of ICT risks

Building on the risk identification and classification process outlined in section 2, Table 4 summarises a standard set of ICT risks that could be considered in each ICT investment case, and form the basis of this ICT Risk Monetisation Framework. This list is not intended to be exhaustive and does not preclude consideration of other risks within an ICT cost-benefit analysis where appropriate to do so, so long as these are assessed in a manner consistent with the approach set out in this Risk Monetisation Framework. Similarly, not all risks in the table will be relevant to every ICT investment case.

Table 4 – Common risks

Business Risks		
Category	ID	Description
Reliability impact	BR1	Customer loss of supply due to cyber attack
	BR2	Customer loss of supply due to system failure
	BR3	Customer loss of export capability due to system failure
	BR4	Customer loss of export capability due to cyber attack
	BR5	Supply restoration time impacted by system failure
	BR6	Supply restoration time impacted by cyber attack
Compliance risk	BC1	Delays in publishing key data to the market due to system failure
	BC2	Delays in publishing key data to the market due to cyber attack
	BC3	Unauthorised access to employee personal data due to reasons other than a cyber attack
	BC4	Unauthorised access to employee personal data due to cyber attack
	BC5	Unauthorised access to customer data due to reasons other than a cyber attack
	BC6	Unauthorised access to customer data due to cyber attack
	BC7	System fault causes failure to notify life-support customers of an outage
	BC8	Cyber attack causes failure to notify life-support customers of an outage
Bushfire risk	BF1	Systems outage impacts bushfire preparation / mitigation program
	BF2	Cyber attack causes systems outage impacting bushfire preparation / mitigation program
Safety risk	BS1	Systems outage causes loss of supply to life-support customers
	BS2	Cyber attack causes systems outage impacting life-support customers
	BS3	Cyber attack prevents correct operation of network protection systems
Customer experience risk	BCX1	Customers impacted by failure of customer-facing system due to software or hardware fault
	BCX2	Customers impacted by failure of customer-facing system due to cyber attack
Financial loss		As required - no standard risks defined for this category
ICT Risks		
Category	ID	Description
Outage	ITO1	System failure
	ITO2	System down due to cyber attack
	ITO3	System failure – impact on field services delivery
	IT04	System down due to cyber attack – impact on field services delivery

Suitability and sustainability	ITS1	Increased change management costs
	ITS2	Data storage exceeded
	ITS3	Performance degradation
	ITS4	Increased maintenance costs

The remainder of this section provides further guidance on the approach to assign a likelihood and consequence for each risk to enable risk monetisation.

3.2 General guidance

The proposed measures of likelihood and consequence are intended as guides only; the most appropriate measures will depend on the nature and scope of the ICT investment under consideration (e.g. which specific operational and business systems it impacts upon) and on the practical availability of relevant evidence or other input data.

For ICT risks it is often the case that the same outcome can arise from different causes. For example, a system outage could arise due to:

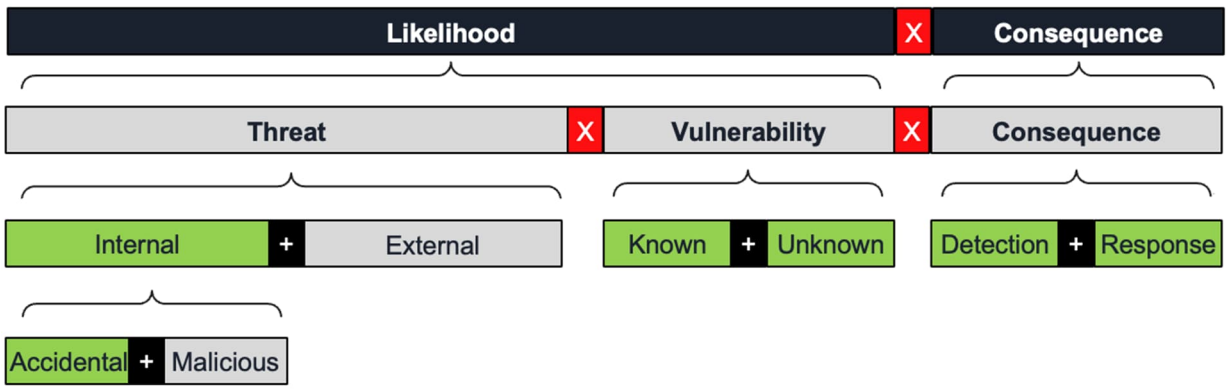
- A software failure
- A hardware or infrastructure fault
- Human error (e.g. accidental shutdown of a production system)
- A cyber attack.

For the purpose of this document, common risks are considered as either non-cyber, which would include failures of software, hardware, infrastructure or process, or cyber-related. This reflects that the factors influencing likelihood and consequence for cyber-related risks tend to be quite different to those for other risks. In the tables below, many risks have both a non-cyber and a cyber-related version.

3.3 Guidance on cyber security risks

CP/PAL/UE's 2020 Cyber Security Strategy identifies that likelihood and consequence for cyber security risks may be broken down into several contributing factors, as shown in Figure 4. The factors shown in green in the figure are those that can potentially be influenced through ICT investments.

Figure 4 - Factors influencing likelihood and consequence for cyber security risks



The Cyber Security Strategy identifies six cyber security threats of concern, shown below.

Table 5 - Cyber security threats

Cyber Security Threats	Description	Threat Actor Motivations	Common Means of Attack
Ransomware or other Malware	This is a malware based attack that prevents use of systems and data unless a ransom is paid.	• Financial gain • Sabotage • Insider: malicious	• Phishing • USB-based Malware • Downloaded Malware • Compromised BYOD • Third party as a vector the network
Extortion (Business operations or Data)	This is when a threat actor has access to or has copied sensitive information or data from 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.	• Financial gain • Sabotage • Insider: malicious	• Phishing • Business Email Compromise (BEC) • Data exfiltration • Third party as a vector the network • Denial of Service
Credential Compromise	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.	• Financial gain • Insider: malicious • Insider: accidental • Sabotage • Hacktivism	• Brute-force attacks • Phishing • Credential Purchase • Interception attacks (Man in the middle) • Reuse attacks (Credential stuffing) • Third party as a vector the network
Vulnerability Exploitation	A weakness in systems is identified and exploited enabling a threat actor to gain unauthorised access.	• Espionage • Financial gain • Insider: malicious • Insider: accidental • Hacktivism • Sabotage	• Zero-day exploit • SQL Injection • Remote Code Execution (RCE)
Sensitive Data Disclosure	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.	• Financial gain • Insider: malicious • Insider: accidental	• Emails and phishing • Insecure physical storage • Unsanctioned cloud file storage use • USB and removable media access
Third Party Compromise	A trusted third party suffers a cyber attack with unauthorised systems access. Due to the third party having access to CP/PAL/UE systems and data, the attackers are then also able to access CP/PAL/UE systems and data.	• Espionage • Financial gain • Insider: malicious • Insider: accidental • Hacktivism • Sabotage	• Exploiting Insufficient information security controls and practices • Supply chain compromise

These six threats provide a useful framework when considering likelihood of cyber security risks and how to quantify the two input factors of threat and vulnerability. For example:

- How many phishing emails are received each year by CP/PAL or UE staff with access to critical systems? (threat, external, may be evidence-based)?
- What is the probability that one of these will result in a successful security breach by the attacker? (vulnerability, estimated and able to be influenced).

The ICT Risk Monetisation Framework does not require that likelihood factors like threat and vulnerability should be individually estimated for each of the above six threats to calculate the overall likelihood for a cyber security risk. Rather, these threats should be used as a guide as to the kind of factors that may be taken into consideration when estimating likelihood for a cyber security risk. In sections 3.4 and 3.5 below, for each risk that is a cyber security risk, the relevant cyber security threats are identified.

3.4 Business risks

3.4.1 Reliability impact risks

These risks capture the impact of an event or a failure which would cause CP/PAL/UE to incur any unforeseen impacts to supply or export capability because of an event such as equipment damage or failure.

Table 6 - Reliability impact risks

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
BR1	Customer loss of supply due to cyber attack	Certain OT systems, e.g. ADMS, SCADA and AMI have the capability for an operator to remotely disconnect customers from supply, e.g. disconnect smart meters, open substation breakers or mid-line load switches, activate load shedding, etc. If a cyber attacker gains control of one of these systems then they can cause a customer outage. Customers impacted will lose supply and, if they have solar, will lose the ability to generate. Outages caused by deliberate cyber attacks are likely to impact large numbers of customers and involve measures to disrupt efforts at recovery, e.g. locking out access to systems or wiping disks, as happened in the 2015 cyber attack in Ukraine where attackers gained control of SCADA systems at three distribution companies and disconnected feeders at 30 substations, leaving 225,000	Forecast frequency of attacks to OT systems of the kind that could give attacker the capability to disconnect customers: *Credential compromise* *Vulnerability exploitation*	Probability of a cyber attack being successful, taking into consideration any heightened security measures associated with critical OT systems compared to other systems.	VCR Number of customers impacted Expected time to restore supply (hours) Average energy consumed per customer per hour Number of solar customers impacted Average export energy per solar customer per hour (24 hour average to account for probability of outage in daylight hours) CECV (24 hour average) Note: when estimating number of customers impacted: 1. Number of solar customers may be estimated pro-rata as a percentage of number of customers, based on estimated average solar penetration 2. For larger incidents it may be appropriate to apply a discount factor, e.g. 30%, to reduce the consequence value, reflecting the fact that, in practice, some customers	Single zone substation / load group impacted	Multiple zone substations / load groups impacted	All customers impacted (e.g. mass AMI disconnection)

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
		customers off supply for 3-6 hours[8].			would be restored early through manual efforts as part of the incident response.			
	Example consequence value = (Expected duration of outage x Number of customers affected x Average energy per customer per hour x VCR) + (Expected duration of outage x Number of solar customers impacted x Average solar customer export kWh per hour x CECV)							
BR2	Customer loss of supply due to system failure	This risk would apply in the case where a failure of an IT or OT system or supporting infrastructure could cause customers to lose supply or could increase the risk of customers losing supply. A failure, even of critical OT systems like ADMS or SCADA, would not normally result in a customer outage. In future, however, it is possible that a failure of a system like DERMs that is actively managing voltage or power flows could lead to localised outages.	Forecast frequency of software or hardware failure of a kind that could cause a loss of supply or could increase the risk of a loss of supply.		VCR Number of customers impacted Expected time to restore supply (hours) Average energy consumed per customer per hour Number of solar customers impacted Average export energy per solar customer per hour (24 hour average to account for probability of outage in daylight hours) CECV (24 hour average)	Single LV transformer area impacted	Multiple LV transformer areas or single zone substation impacted	Multiple zone substations impacted
	Example consequence value = (Expected duration of outage x Number of customers affected x Average energy per customer per hour x VCR) + (Expected duration of outage x Number of solar customers impacted x Average solar customer export kWh per hour x CECV)							
BR3	Customer loss of export capability due to system failure	Solar customers that are on 'dynamic operating envelope' (DOE) or emergency backstop connection schemes could lose the ability to export energy if the systems that enable these schemes (e.g. IEEE2030.5 utility server) fail, as these solar inverters are designed to fall back to a low or zero export limit if communication to the central server is lost.	Forecast frequency of software or hardware failure impacting a system that is directly involved in emergency backstop measures or DOEs (e.g. utility server) that causes export limiting (assuming customer equipment fails safe to zero- or low-export limit on loss of control)		Number of solar customers impacted Average export energy per solar customer per hour (24 hour average to account for probability of outage in daylight hours) Expected curtailment time (hours to fix) CECV (24 hour average)	All solar customers on DOE/backstop scheme impacted, short duration	All solar customers on DOE/backstop scheme impacted, medium duration	All solar customers on DOE/backstop scheme impacted, long duration

[8] D. E. Whitehead, K. Owens, D. Gammel and J. Smith, *Ukraine cyber-induced power outage: Analysis and practical mitigation strategies*, 2017 70th Annual Conference for Protective Relay Engineers (CPRE)

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
	Example consequence value = (Likely system downtime x number of solar customers on DERMS x average solar customer export kWh per hour x CECV)							
BR4	Customer loss of export capability due to cyber attack	A cyber attack that impacts on systems that enable DOEs or emergency backstop schemes could force all customers on such schemes to zero export.	Likelihood of cyber attack on export / backstop systems: *Ransomware* *Credential compromise* *Vulnerability exploitation* *Third party compromise*	Probability that attack will succeed	CECV (24 hour average) Number of solar customers impacted (number connected to backstop/DOE mechanisms) Expected curtailment time (hours to fix) Average export energy per solar customer per hour (24 hour average)	All solar customers on DOE/backstop scheme impacted, short duration	All solar customers on DOE/backstop scheme impacted, medium duration	All solar customers on DOE/backstop scheme impacted, long duration
	Example consequence value = (Likely system downtime x Number of solar customers on DERMS x Average solar customer export kWh per hour x CECV)							
BR5	Supply restoration time impacted by system failure	The dispatch of field crews, network switching and coordination of supply restoration activities rely on various IT and OT systems. If these systems fail, staff will have to revert to manual procedures. This will increase the average time taken to restore supply to customers for any supply outages that occur while the systems are down. If the Fault Detection Isolation and Restoration (FDIR) system is impacted, automatic switching and fault isolation will not function on the affected feeders, which will increase the number of customers off supply.	Forecast frequency of software or hardware failure impacting a system that is directly involved in supply restoration (e.g. click, etc)	Likelihood that system downtime will coincide with an outage event.	VCR Number of customers impacted Expected increase in time to repair the fault (hours) Number of FDIR customers impacted if FDIR is unavailable Expected time to perform FDIR switching manually and restore supply for those customers Average energy per customer per hour Number of solar customers impacted Average export energy per solar customer per hour (24 hour average to account for probability of outage in daylight hours) CECV	Few customers impacted (minor outage)	Average outage (typical number of customers)	Large outage (storm event etc)
	Example consequence value = (Increase in supply restoration time x Total number of customers impacted in outages occurring during system downtime x Average customer kWh per hour x VCR) + (Increase in supply restoration time x Total number of solar customers impacted in outages occurring during system downtime x Average solar customer export kWh per hour x CECV)							

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
BR6	Supply restoration time impacted by cyber attack	This risk involves the same systems as in BR5 above, but reflects the case where these systems are impacted by a cyber attack rather than a hardware or software fault.	Likelihood of cyber attack on a system that is directly involved in supply restoration (e.g. click, etc): *Ransomware* *Credential compromise* *Vulnerability exploitation*	Likelihood that attack will succeed Likelihood that system downtime will coincide with an outage event	VCR Number of customers impacted Expected increase in time to repair the fault (hours) Number of FDIR customers impacted if FDIR is unavailable Expected time to perform FDIR switching manually and restore supply for those customers Average energy per customer per hour Number of solar customers impacted Average export energy per solar customer per hour (24 hour average to account for probability of outage in daylight hours) CECV	Few customers impacted (minor outage)	Average outage (typical number of customers)	Large outage (storm event etc)
	Example consequence value = (Increase in supply restoration time x Total number of customers impacted in outages occurring during system downtime x Average customer kWh per hour x VCR) + (Increase in supply restoration time x Total number of solar customers impacted in outages occurring during system downtime x Average solar customer export kWh per hour x CECV)							

3.4.2 Compliance risks

These risks measure risk of legal or regulatory sanction, financial or reputational loss arising from CP/PAL/UE's failure to abide by the commercial compliance obligations as set by market bodies such as the AEMO, AER and ESC.

Table 7 - Compliance risks

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
BC1	Delays in publishing key data to the market due to system failure	Certain systems are involved in the transmission of data to AEMO, including metering data, MSATS standing data, etc. If these systems fail, CP/PAL/UE may fail to meet its obligations under AEMO market procedures and may incur financial penalties as a result.	Forecast frequency of software or hardware failure impacting market system		Number of days that market systems are impacted Applicable civil penalty rates as defined in the National Electricity Rules (NER) clause 3.13(c) and National Electricity Law clause 2AB, which include a fixed component and a daily rate for every day of non-compliance.	Fixed penalty only, system restored in less than one day	Fixed penalty plus daily rate, typical fault restoration time, non-compliance may exceed one day	Fixed penalty plus daily rate, complex issue, worst-case fault restoration time, multiple days of non-compliance
	Example consequence value = Base civil penalty + (Number of additional days breach continues x Daily civil penalty)							
BC2	Delays in publishing key data to the market due to cyber attack	This risk involves the same systems as in BC1 above, but reflects the case where these systems are impacted by a cyber attack rather than a hardware or software fault.	Forecast frequency of cyber attack targeting a market system *Ransomware* *Credential compromise* *Vulnerability exploitation*	Likelihood that attack will succeed	Number of days that market systems are impacted Applicable civil penalty rates as defined in the National Electricity Rules (NER) clause 3.13(c) and National Electricity Law clause 2AB, which include a fixed component and a daily rate for every day of non-compliance.	Fixed penalty only, system restored in less than one day	Fixed penalty plus daily rate, typical system restoration time for cyber incident, non-compliance may exceed one day	Fixed penalty plus daily rate, complex issue, worst-case system restoration time for cyber incident, multiple days of non-compliance
	Example consequence value = Base civil penalty + (Number of additional days breach continues x Daily civil penalty)							
BC3	Unauthorised access to employee personal data due to reasons other than a cyber attack	CP/PAL/UE IT systems store certain personal data on its employees that could be disclosed, e.g. due to poor disposal practices for storage media.	Forecast frequency of (non-cyber-related) employee personal data breach		Cost to investigate and remediate	Minor breach, limited data exposed, isolated incident	More significant breach, process changes required to prevent recurrence	Major breach, significant changes required to processes and/or systems to prevent recurrence
	Example consequence value = Cost of external vendor to investigate and remediate							

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
BC4	Unauthorised access to employee personal data due to cyber attack	CP/PAL/UE IT systems store certain personal data on its employees that could be accessed in a cyber attack.	Forecast frequency of cyber attack targeting employee data *Extortion* *Sensitive data disclosure*	Likelihood that attack will succeed	Cost to investigate and remediate, including engagement of specialist cyber consultant to undertake forensics. Note, this cost may be broadly similar regardless of the severity of the breach.	Minor breach, limited data exposed from small number of staff.	More significant breach	Major breach, many or all staff affected.
	Example consequence value = Cost of external vendor to investigate and remediate							
BC5	Unauthorised access to customer data due to reasons other than a cyber attack	CP/PAL/UE IT systems store certain personal data on its customers that could be disclosed, e.g. due to negligence, malpractice or poor disposal practices for storage media.	Forecast frequency of (non-cyber-related) customer data breach		Civil penalties sought by Australian Information Commissioner under the Privacy Act 1988	Minor breach, limited data exposed from small number of customers (10% of max penalty)	More significant breach (50% of max penalty)	Major breach, many or all customers affected, sensitive personal data exposed (100% of max penalty)
	Example consequence value = Civil penalty amount							
BC6	Unauthorised access to customer data due to cyber attack	CP/PAL/UE IT systems store certain personal data on its customers that could be accessed in a cyber attack.	Forecast frequency of cyber attack targeting customer data *Extortion* *Sensitive data disclosure*	Likelihood that attack will succeed	Civil penalties sought by Australian Information Commissioner under the Privacy Act 1988	Minor breach, limited data exposed from small number of customers (10% of max penalty)	More significant breach (50% of max penalty)	Major breach, many or all customers affected, sensitive personal data exposed (100% of max penalty)
	Example consequence value = Civil penalty amount							
BC7	System fault causes failure to notify life-support customers of an outage	CP/PAL/UE has obligations under the Electricity Distribution Code of Practice to notify registered life support customers of planned outages. If the systems that support this activity fail, notification requirements may not be met and civil penalties may	Forecast frequency of software or hardware failure impacting systems required to notify life support customers.	Likelihood of failure coinciding with a scheduled outage	Civil penalties due to non-compliance with Electricity Distribution Code of Practice	Single life support customer impacted	Several life support customers impacted	Many life support customers impacted

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
		ensue. This could occur if the failure is not detected in a timely manner, and/or if manual workarounds are not fully effective.						
	Example consequence value = Civil penalty amount							
BC8	Cyber attack causes failure to notify life-support customers of an outage	This risk involves the same systems as in BC7 above, but reflects the case where these systems are impacted by a cyber attack rather than a hardware or software fault	Forecast frequency of cyber attack targeting a system required to notify life support customers. *Ransomware* *Credential compromise* *Vulnerability exploitation*	Likelihood that attack will succeed Likelihood of failure caused by attack coinciding with a scheduled power outage	Civil penalties due to non-compliance with Electricity Distribution Code of Practice	Single life support customer impacted	Several life support customers impacted	Many life support customers impacted
	Example consequence value = Civil penalty amount							

3.4.3 Bushfire risks

These risks include outages of the operational technology interfaces that provide visibility of the network, which may increase bushfire risk by preventing operators from making accurate and timely decisions.

Table 8- Bushfire risks

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
BF1	Systems outage impacts bushfire preparation / mitigation program	CP/PAL/UE may undertake various activities to reduce fire-start risk, e.g. pre-bushfire season inspections, vegetation management or protection settings changes. These activities could be impacted by failure of the supporting IT and OT systems, necessitating the need for less efficient manual workarounds and, in the worst case, leading to an increased risk of fire start if the effectiveness of the programs is materially impaired.	Forecast likelihood of software or hardware failure impacting on systems that support bushfire preparedness / fire start mitigation activities	Likelihood that fault occurs at a time that impacts bushfire preparedness activities	Cost of workarounds / manual processes (additional staff effort) Corporate risk framework (Copperleaf) measures for harm / loss of life	Minor issue, workaround cost only	More significant issue, higher workaround cost	Severe issue, workaround not fully effective, fire start risk increased
	Example consequence value = (Additional time required to perform manual processes x Number of staff involved in manual processes x Average hourly rate for internal employees) + Copperleaf measures for harm / loss of life							
BF2	Cyber attack causes systems outage impacting bushfire preparation / mitigation program	This risk involves the same systems as in BF1 above, but reflects the case where these systems are impacted by a cyber attack rather than a hardware or software fault	Likelihood of cyber attack on a system that is directly involved in bushfire preparedness *Ransomware* *Credential compromise* *Vulnerability exploitation*	Likelihood that fault occurs at a time that impacts bushfire preparedness activities	Cost of workarounds / manual processes (additional staff effort) Corporate risk framework (Copperleaf) measures for harm / loss of life	Minor issue, workaround cost only	More significant issue, higher workaround cost	Severe issue, workaround not fully effective, fire start risk increased
	Example consequence value = (Additional time required to perform manual processes x Number of staff involved in manual processes x Average hourly rate for internal employees) + Copperleaf measures for harm / loss of life							

3.4.4 Safety risk

These risks consider safety risk to the public and staff including network electrical safety, works practices and workplace risk (not including bushfire risk).

Table 9 - Safety risks

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
BS1	Systems outage causes loss of supply to life-support customers	This risk is similar to BR2 above, but would capture the specific additional risk of harm to life support customers when they lose supply. In practice this is unlikely to be quantifiable today, noting that (a) a system fault would not normally cause a supply outage and (b) life support customers can and do lose supply in any event from time to time, so the marginal risk of harm due to supply outages associated with IT/OT system faults may not be quantifiable. As OT systems evolve in future this risk may become more relevant.	Forecast frequency of software or hardware failure of a kind that could cause a loss of supply		Number of customers impacted Percentage of customers who are life support customers Probability of harm arising from supply outage Corporate risk framework (Copperleaf) measures for harm / loss of life	Single life support customer impacted	Several life support customers impacted, short duration	Several life support customers impacted, long duration
	Example consequence value = (Number of customers impacted x Percentage of customers who are life support customers x probability of harm / loss of life x Copperleaf measures for harm / loss of life)							
BS2	Cyber attack causes systems outage impacting life-support customers	This risk is similar to BS1 above, but in the case where the outage in question arises from a cyber attack. As above, this may not be quantifiable in practice today.	Forecast frequency of attacks to OT systems (ADMS, SCADA, AMI, etc) of the kind that could give attacker the capability to disconnect customers (disconnect smart meters, open CBs / load switches, activate load shedding, etc): *Credential compromise* *Vulnerability exploitation*	Probability of a cyber attack being successful	Number of customers impacted Percentage of customers who are life support customers Corporate risk framework (Copperleaf) measures for harm / loss of life	Single zone substation / load group impacted	Multiple zone substations / load groups impacted	All customers impacted (e.g. mass AMI disconnection)
	Example consequence value = (Number of customers impacted x Percentage of customers who are life support customers x probability of harm / loss of life x Copperleaf measures for harm / loss of life)							

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
BS3	Cyber attack prevents correct operation of network protection systems	A cyber attacker that gains control of key OT systems could potentially change network protection settings, impairing the normal operation of network protection systems. This could cause an elevated safety risk, e.g. risk of failure to de-energise a downed line or re-energising a line that should be de-energised for maintenance	Forecast frequency of attacks to protection systems *Credential compromise* *Vulnerability exploitation*	Probability of a cyber attack being successful Likelihood of coincidence with network damage, e.g. line down or maintenance activity	Corporate risk framework (Copperleaf) measures for harm / loss of life	No harm	Harm to single member of the public or personnel	Harm to multiple members of the public or personnel or loss of life
	Example consequence value = Copperleaf measures for harm / loss of life							

3.4.5 Customer experience risks

These risks include outages and data breaches involving customer information that will adversely impact customer interactions.

Table 10 - Customer experience risks

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
BCX1	Customers impacted by failure of customer-facing system due to	Customers contact CP/PAL/UE and receive information on a daily basis via the call centre, web site, social media, text messaging, etc.	Forecast likelihood of software or hardware failure impacting on customer-facing systems		Customer value of lost time Number of customers impacted Average number of contacts (call centre, web site, social media etc) per customer per hour	Single system impacted, low customer traffic at the time	Multiple systems impacted, average levels of customer	All systems impacted at time of high customer traffic (e.g. storm or fire event),

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	Examples of consequence		
			Threat / likelihood of trigger	Vulnerability / likelihood of impact		Best case	Most Likely	Worst case
	software or hardware fault	If the supporting IT systems fail, customer service is impacted and customers who are enquiring about new connections, installing solar, seeking information on supply outages, etc, will incur lost time trying to resolve their issues via other channels.			Hours of system downtime		traffic at the time	extended restoration time
	Example consequence value = (Duration of downtime x Average number of customer contacts per hour x Additional customer time per contact when normal channels unavailable x Customer value of lost time)							
BCX2	Customers impacted by failure of customer-facing system due to cyber attack	This risk involves the same systems as in BCX1 above, but reflects the case where these systems are impacted by a cyber attack rather than a hardware or software fault	Forecast likelihood of cyber attack on customer-facing systems *Ransomware* *Credential compromise* *Vulnerability exploitation*	Likelihood that attack will succeed	Customer value of lost time Number of customers impacted Average number of contacts (web site, social media etc) per customer per hour Hours of system downtime	Single system impacted, low customer traffic at the time, extended restoration time	Multiple systems impacted, average levels of customer traffic at the time, extended restoration time	All systems impacted at time of high customer traffic (e.g. storm or fire event), extended restoration time
	Example consequence value = (Duration of downtime x Average number of customer contacts per hour x Additional customer time per contact when normal channels unavailable x Customer value of lost time)							

3.4.6 Financial loss

These risks represent a direct financial consequence not otherwise taken into account in any of the above areas of consequence. Financial loss will be considered on a case-by-case basis for each ICT investment case.

3.5 IT risks

3.5.1 Outage risks

Outages may be caused due to poor infrastructure currency and insufficient infrastructure resource capacity (e.g. server memory).

Outage resolution may be prolonged due to unavailability of appropriate technical resources (e.g. vendor support) or available replacement hardware through not refreshing software after it reaches end of life.

Table 11 - ICT outage risks

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	
			Threat / likelihood of trigger	Vulnerability / likelihood of consequence	Productivity loss	Restoration cost
ITO1	System failure	This risk relates to the impact on productivity within the business when an IT or OT system fails due to a hardware or software fault and the users of that system are unable to perform their work, or have to revert to manual processes to perform tasks.	Likelihood of system outage (informed by historical uptime of system in question / historical fault records)		Expected hours of downtime Total users impacted Average user hourly rate Productivity impact factor (for each hour of system downtime, how many hours of lost productivity ensues for the affected user group)	IT specialist / vendor hourly rate (24/7 average) Expected hours of downtime Estimated fixed cost of rectification (mobilisation)
	Example consequence value = (Likely system downtime x Number of users affected x Average hourly rate for internal employees) + (Number of IT specialists required to rectify x Hours to rectify x IT specialist/vendor hourly rate) + Rectification fixed costs					
ITO2	System down due to cyber attack	This risk is the same as ITO1 above, but reflects the case where systems are impacted by a cyber attack rather than a hardware or software fault	Likelihood of cyber attack that could render system unusable *Ransomware* *Credential compromise* *Vulnerability exploitation*	Likelihood that attack will succeed	Expected hours of downtime Total users impacted Average user hourly rate Productivity impact factor (for each hour of system downtime, how many hours of lost productivity ensues for the affected user group)	IT specialist / vendor hourly rate (24/7 average) Expected hours of downtime Estimated fixed cost of rectification (mobilisation)
	Example consequence value = (Likely system downtime x Number of users affected x Average hourly rate for internal employees) + (Number of IT specialists required to rectify x Hours to rectify x IT specialist/vendor hourly rate) + Rectification fixed costs					
ITO3	System failure - impact on field services delivery	Field staff rely on various IT and OT systems to perform their duties, including supply restoration work, scheduled maintenance, asset inspection, new customer connections and so on. If the supporting systems fail, field staff will have to revert to manual procedures, which increases the	Likelihood of system outage (informed by historical uptime of system in question / historical fault records)		Expected hours of downtime Additional staff cost of performing field work using manual procedures during this time	IT specialist / vendor hourly rate (24/7 average) Expected hours of downtime Estimated fixed cost of rectification (mobilisation)

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	
			Threat / likelihood of trigger	Vulnerability / likelihood of consequence	Productivity loss	Restoration cost
		staff effort required. This would be in addition to any impact on the office staff who use the same systems captured in ITO1 and, in the case of outage restoration, the customer impacts captured in BR2. Note that this risk will only apply to the extent that field staff are in-house and rely on in-house systems, as opposed to field services functions that are fully outsourced to Zinfra or others.				
	Example consequence value = (Incremental operational labour x Time to restore system (to fully operational) x User hourly rate) + (Number of IT specialists required x Hours taken to rectify per specialist x IT specialist hourly rate)					
ITO4	System down due to cyber attack – impact on field services delivery	This risk is the same as ITO3 above, but reflects the case where systems are impacted by a cyber attack rather than a hardware or software fault. Note that this risk will only apply to the extent that field staff are in-house and rely on in-house systems, as opposed to field services functions that are fully outsourced to Zinfra or others.	Likelihood of cyber attack that could render system unusable *Ransomware* *Credential compromise* *Vulnerability exploitation*	Likelihood that attack will succeed	Expected hours of downtime Additional staff cost of performing field work using manual procedures during this time	IT specialist / vendor hourly rate (24/7 average) Expected hours of downtime Estimated fixed cost of rectification (mobilisation)
	Example consequence value = (Incremental operational labour x Time to restore system (to fully operational) x User hourly rate) + (Number of IT specialists required x Hours taken to rectify per specialist x IT specialist hourly rate)					

3.5.2 Suitability and system sustainability risks

These risks reflect that legacy, unmaintained systems are more prone to failures, data loss and security breaches. This can affect CP/PAL/UE's ability to meet regulatory and compliance requirements such as customer management, financial and market reporting obligations. For example, data loss occurring due to not having enough data storage, or unplanned maintenance is more likely to lead to failures, or increased spend on workarounds.

If systems are not refreshed, they will not be compatible with associated market products when reaching End of Life, such as security patches. Ensuring continued access to patches through refreshes would reduce vulnerabilities to cyber security attacks. In addition, refreshing may avoid incurring additional costs from maintaining inefficient, unconsolidated systems.

Table 12 - ICT suitability and sustainability risks

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	
			Threat / likelihood of trigger	Vulnerability / likelihood of trigger	Productivity loss	Restoration cost
ITS1	Increased change management costs	Systems that are out of vendor support and no longer receiving updates may be more costly to modify if business needs change. Note that, depending on the business case, this factor could be included in the cost forecasts for different support or maintenance options, rather than as a monetised risk.	Estimated change requests / feature enhancements per system per annum		Percentage uplift on historical average cost per enhancement	N/A
	Example consequence value = Historical average cost per enhancement x Percentage uplift due to lack of vendor support					
ITS2	Data storage exceeded	If data storage capacity does not keep pace with growing data needs of the business, storage could run out, causing system downtime for all systems that rely on the affected storage element until the situation can be resolved (e.g. offloading or archiving some data and/or bringing more storage online). As the time to bring additional storage online could be significant, workarounds may	Likelihood that forecast growth in data exceeds available capacity at some point in the 5 year RCP		Expected hours of downtime Total users impacted Average user hourly rate Productivity impact factor (for each hour of system downtime, how many hours of lost productivity ensues for the affected user group)	IT specialist / vendor hourly rate (24/7 average) Fixed cost of rectification (mobilisation) Additional data storage capacity cost (may be capex or increase in opex depending on system)

ID	Specific IT risk	Description and guidance notes	Likelihood measures		Consequence measures	
			Threat / likelihood of trigger	Vulnerability / likelihood of trigger	Productivity loss	Restoration cost
		involve suspending less critical applications in order to restore the most critical ones, leading to extended outage time for some users.				
	Example consequence value = (Likely system downtime x Number of users affected x Average hourly rate for internal employees) + (IT specialist/ vendor hourly rate x Number of IT specialists required to rectify x Hours to rectify) + Additional data storage capacity cost					
ITS3	Performance degradation	Software systems, server hardware and network (LAN) infrastructure that is old and not maintained may progressively degrade in performance over time, leading to lost productivity for workers who depend on them.	Likelihood that forecast growth in data, system users, transactions or new applications leads to an overall degradation in performance and responsiveness of business systems		Total users impacted Average user hourly rate Productivity loss (estimated additional time taken to perform tasks, on average)	N/A
	Example consequence value = Number of users affected x Average hourly rate for internal employees x Estimated time increase per employee					
ITS4	Increased maintenance costs	Systems that are outside vendor maintenance contracts, or classified as end-of-life by vendors, have increased maintenance costs. Vendors that continue to offer maintenance for such systems may charge a premium, or maintenance contracts may need to be established with parties other than the original vendor. Note that, depending on the business case, this factor could be included in the cost forecasts for different support or maintenance options, rather than as a monetised risk.	Number of systems impacted by being out of vendor maintenance regime		Estimated uplift in historical maintenance costs (averaged across impacted systems)	N/A
	Example consequence value = Average historical maintenance costs x Percentage uplift in maintenance costs					

Appendix A Summary of standard inputs

The table below is a list of standard inputs for risk monetisation calculations and includes guidance on the source to be used for information.
Note:

- Most inputs, e.g. number of zone substations or number of customers, will have individual values for each of the three businesses CitiPower, Powercor and United Energy. For brevity, each has a single entry in the list below. The scope of the business case will dictate whether it is appropriate to use an individual value or to use an aggregate or sum across CP/PAL/UE.
- Many inputs, e.g. the number of solar customers, will change over time. For these, the value used to calculate risk should not be today's value but should be the value that reasonably reflects the expected value in the year that the risk or risk mitigation will occur. For example, it could be the average of the annual forecasts for each year in the upcoming regulatory period. For a number that is forecast to increase through the period like the number of solar customers this could be the forecast value in the middle or end of the period.
- In the table, inputs that are not based on primary sources but rather derived from other inputs are shown in grey.

Table 13 - Summary of standard inputs

Number	Input	Unit	Source / guidance	Relevant to risks
1	Number of customers	NMIs	Reset Regulatory Information Notice (RIN) Workbook 1 section 2.5	BR1, BR2, BR5, BR6
2	Number of solar or other export customers	NMIs	Reset Regulatory Information Notice (RIN) Workbook 1 section 7.8	BR1, BR2, BR5, BR6
3	Percentage of customers who are solar/export customers	Percentage	Derived from inputs 1 and 2 above, can be used to estimate the number of solar customers that would be represented in a given number of customers impacted by a loss of supply to the premises.	BR1, BR2, BR5, BR6
4	Number of solar customers connected to backstop / DOE mecha	NMIs	Reset Regulatory Information Notice (RIN) Workbook 1 section 7.8, forecast new export customers connected since backstop requirement mandated in July 2024	BR3, BR4
5	Number of zone substations	Number	Distribution Annual Planning Report (DAPR)	BR1, BR2
6	Average number of customers per zone substation	Number	May be derived from inputs 1 and 5	BR1, BR2
7	Expected average time to restore customer supply after an outage caused by a cyber attack	Hours	Estimate based on evidence from relevant historical events. At the present time the most relevant incident is the 2015 cyber attack on electricity networks in Ukraine which resulted in customers losing supply for between three and six hours or an average of 4.5 hours.	BR1, BR4, BS2
8	Value of Customer Reliability (VCR)	$/kWh	The VCR is the AER's measure to quantify the cost to customers of a loss of supply, based on customer research. For risk quantification, use a weighted average of the Victorian residential VCR and the VCR for distribution-connected commercial and industrial customers, as published annually by the AER, weighted according to the CP/PAL/UE customer mix relevant to the business case in question. At the present time the AER is reviewing the VCR methodology and will publish updated values for VCR by December 2024	BR1, BR2, BR5, BR6

Number	Input	Unit	Source / guidance	Relevant to risks
9	Average hourly Customer Export Curtailment Value (CECV)	$/kWh	The CECV is the AER's measure to quantify the cost to the electricity market of a loss or reduction of export capability affecting small export customers. Future versions of the CECV will include a component for the cost of greenhouse gas emissions. The AER publishes the CECV for Victoria annually in the form of a table of 30-minute $/kWh value forecasts for the following 20 years. For risk quantification, use an average of all 30-minute values for the relevant year, multiplied by two to produce an average hourly value.	BR1, BR2, BR3, BR4, BR5, BR6
9	Avg electricity consumption per customer per hour	kWh / hour	Total annual volume of energy delivered (Reset Regulatory Information Notice (RIN) Workbook 1 section 3.4) divided by total number of customers (input 1) divided by number of hours in a year (365 x 24)	BR1, BR2, BR5, BR6
10	Avg electricity export per small export customer per hour	kWh / hour	Total annual volume of energy exported (Reset Regulatory Information Notice (RIN) Workbook 1 section 7.8) divided by number of export customers (input 2) divided by number of hours in a year (365 x 24)	BR1, BR2, BR3, BR4, BR5, BR6
11	Average number of supply interruptions per customer per year (	Number / year	System Average Interruption Frequency Index (SAIFI). Align with the figures in Reset Regulatory Information Notice (RIN) Workbook 1 section 6.2. SAIFI targets are set by different feeder types (cbd, urban, short rural, long rural). For risk estimation, it will normally be appropriate to use a single network-wide weighted average, which can be calculated using the customer numbers for each feeder type, also in Reset Regulatory Information Notice (RIN) Workbook 1 section 6.2.	BR5, BR6
12	Number of individual customer interruptions per year	Number / year	Derived from input 11 multiplied by input 1	BR5, BR6
13	Average number of customers impacted per outage	Number	Historical data from Outage Management System (OMS)	BR5, BR6
14	Worst-case number of customers impacted per outage	Number	Historical data from Outage Management System (OMS) – e.g. number of customers impacted in largest single outage event recorded	BR5, BR6
15	Best-case number of customers impacted per outage	Number	For a conservative estimate of risk assume best case is a single customer outage.	BR5, BR6
16	Average number of multi-customer outages in any given hour	Number / hour	Derived from input 12 divided by input 13 divided by number of hours in a year (365 x 24)	BR5, BR6
17	Average increase in time taken to restore customer supply using manual procedures	Hours	CP/PAL/UE subject matter expert estimate. Estimated additional time taken for crews to complete supply restoration work, per outage, if the normal ICT systems they use are unavailable and manual procedures must be used instead for dispatch, switching, etc.	BR5, BR6
18	Percentage of customers covered by the automatic Fault Detection, Isolation and Restoration (FDIR) system	Percentage	CP/PAL/UE Network operations internal data. FDIR reduces the number of customers that experience a sustained supply outage when there is a fault by automatically operating switches to isolate the fault to the smallest area possible. If FDIR is unavailable then manual switching will be required to restore supply to those customers who would have been restored automatically by FDIR.	BR5, BR6
19	Estimated average time taken to manually perform the switching that FDIR would normally perform automatically, if a fault occurs while the FDIR system is offline	Hours	CP/PAL/UE subject matter expert estimate.	BR5, BR6

Number	Input	Unit	Source / guidance	Relevant to risks
20	Civil penalties that apply if CP/PAL/UE fails to meet its obligations under the rules to provide data to the market	$, $/day	Applicable civil penalty rates for a Tier 2 civil penalty as defined in the National Electricity Law clause 2AB, which include a fixed component and a daily rate for every day of non-compliance.	BC1, BC2
21	Average frequency of IT/OT software or infrastructure faults	Number / year	The likelihood of future faults should be estimated by SMEs familiar with the systems or infrastructure in question, taking into consideration age and support arrangements. Ideally these estimates should be informed by considering ServiceNow incident data or other relevant historical records of actual faults for the relevant system, systems or infrastructure. Any such data should be filtered to remove minor incidents that would not give rise to a material business impact (e.g. for ServiceNow consider incidents of priority 1 (Critical) and 2 (High) only) and cleansed to remove outliers and duplicates (e.g. eliminate records generated automatically where the same incident has a record logged by a person).	BR2, BR3, BR5, BC1, BC7, BF1, BS1, BCX1, ITO1, ITO3
22	Average system downtime arising from an IT/OT software or infrastructure fault	Hours	The expected system downtime when a fault occurs should be estimated by SMEs familiar with the systems or infrastructure in question, taking into consideration age and support arrangements. This is the time that the normal users of the system are unable to use it for its normal purpose. Ideally these estimates should be informed by considering ServiceNow incident data or other relevant historical records of actual faults for the relevant system, systems or infrastructure. Any such data should be filtered to remove minor incidents that would not give rise to a material business impact (e.g. for ServiceNow consider incidents of priority 1 (Critical) and 2 (High) only) and cleansed to remove outliers and duplicates (e.g. eliminate records generated automatically where the same incident has a record logged by a person).	BR2, BR3, BR5, BC1, BC7, BF1, BS1, BCX1, ITO1, ITO3, BS1, BCX1
23	Labour costs to restore an IT/OT system that has failed	$ / hour	CP/PAL/UE standard market rates for IT specialist, assuming contract or vendor resource	ITO1, ITO2, ITO3, ITO4, ITS2
24	Vendor costs to assist with restoring an IT/OT system	$ / hour	Any vendor costs that are not included in the support contract for the system or infrastructure in question (e.g. extra costs for out-of-hours support or parts) – should be estimated based on the current support contract. If there is or will be no support contract, costs should be estimated based on market rates for external IT specialists and/or past experience with similar issues.	ITO1
25	External consultant costs to undertake forensic investigation of cause and consequence following a major cyber incident or data breach	$	SME estimate based on market rates and any relevant experience of similar incidents	BC4
26	Penalties under the Privacy Act for disclosure of customer data	$	The maximum penalty that the Australian Information Commissioner can impose on a body corporate under Section 80W of the Privacy Act 1988 for a serious or repeated interference with privacy (s 13G).	BC5, BC6
27	Civil penalties under the Electricity Distribution Code of Practice for failure to notify life support customers of planned outages	$	The maximum civil penalty that can be sought by the Essential Services Commission of Victoria for a breach of the Electricity Distribution Code of Practice as set by the Victorian Government.	BC7, BC8
28	Number of life support customers	Number	CP/PAL/UE customer records	BC7, BC8, BS1, BS2

Number	Input	Unit	Source / guidance	Relevant to risks
29	Average time to repair a system following a cyber attack	Hours	SME estimate based on any relevant experience of similar incidents, taking into consideration current and planned measures to improve capabilities to limit damage and recover systems following a cyber breach.	BC2, BC8, BCX2, ITO2, ITO4
30	Additional cost of manual procedures for bushfire preparedness program	$	SME estimate based on assessment of the nature of the manual workarounds, depending on the affected systems	BF1, BF2
31	Cost of risk of harm or loss of life to public	$ / incident	Standard corporate values maintained in Copperleaf value framework	BF1, BF2, BS1, BS2, BS3
32	Number of customer contacts to call centre and online resources hour	Number / hour	Use Reset Regulatory Information Notice (RIN) Workbook 1 section 6.2 (number of calls to call centre per annum) for average, call centre records for worst case (peak during a recent major weather event). Other relevant sources include CP/PAL/UE historical logs from web site and other online platforms used by customers.	BCX1, BCX2
33	Customer cost of lost time	$ / hour	CP/PAL/UE customer willingness to pay research, 2024	BCX1, BCX2
34	Number of system users	Number	Source would be the SMEs responsible for administering the system in question. Some systems like SAP have very many users in multiple different groups that use different parts of the system, so risk quantification needs to consider whether the failure mode is likely to impact on the whole system (all users) or just part of the system.	ITO1, ITO2, ITS2, ITS3
35	Internal staff costs of lost work time due to a system outage, per impacted user	$ / hour / user	CP/PAL/UE standard staff rates, may use average of the hourly rates for staff roles that are users of the system in question.	ITO1, ITO2, ITS2, ITS3
36	Productivity impact factor	Number	SME estimate, which will depend on the nature of the system in question: for each hour of system downtime, how many hours of lost productivity ensues for the affected user group? This will typically be less than one as users can continue perform other aspects of their role while the system is down. For certain systems and users it could potentially be greater than one, if the users rely fully on the system to perform their role, and must undertake additional work once the system is back online to catch up. This would typically be applied as a multiplier to the expected hours of system downtime when estimating the cost of consequence.	ITO1, ITO2
37	Increase in change management costs for non-supported system	$ per annum	SME estimate by SMEs responsible for administering the systems in question, based on prior experience of similar issues.	ITS1
38	Current data storage capacity (on premises)	GB	CP/PAL/UE asset records for on-premises data storage	ITS2
39	Forecast growth in data storage requirements (on premises)	GB / year	SME estimate based on historical growth and future plans	ITS2
40	Expected duration of downtime if on-premises data storage exce	Hours	SME estimate based on the nature of the systems impacted, remediation plans, support contracts and any experience from prior incidents in ServiceNow impacting on data storage.	ITS2
41	Estimated lost productivity per annum for users when systems perform poorly due to inadequate infrastructure	Hours / year	SME estimate based on the nature of the systems in question.	ITS3

Number	Input	Unit	Source / guidance	Relevant to risks
42	Increase in maintenance costs when systems are no longer supported by the vendor or otherwise outside vendor maintenance contracts	Percentage	SME estimate based on prior experience of similar issues and/or current vendor contracts (e.g. some vendors have a standard increase in annual maintenance cost for older versions of their product that are no longer actively developed or maintained)	ITS4
43	Increase in field staff effort to perform field tasks using manual processes when systems are down	FTE	SME estimate, taking into consideration the nature of the systems at risk and hence the field work that could be impacted. This could include supply restoration tasks, new customer connections, scheduled maintenance, switching, asset inspection, vegetation management and other tasks.	ITO3, ITO4
44	Field staff hourly rate	$ / hour	CP/PAL/UE standard rates	ITO3, ITO4

EY | Building a better working world

EY exists to build a better working world, helping to create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

In line with EY's commitment to minimize its impact on the environment, this document has been printed on paper with a high recycled content.

ey.com