Supporting Document 12.1.4
Asset Risk Management
Managing the Risk of Network Asset Failures

April 2018

Table of Contents

List of Figures

List of Tables

1. Introduction

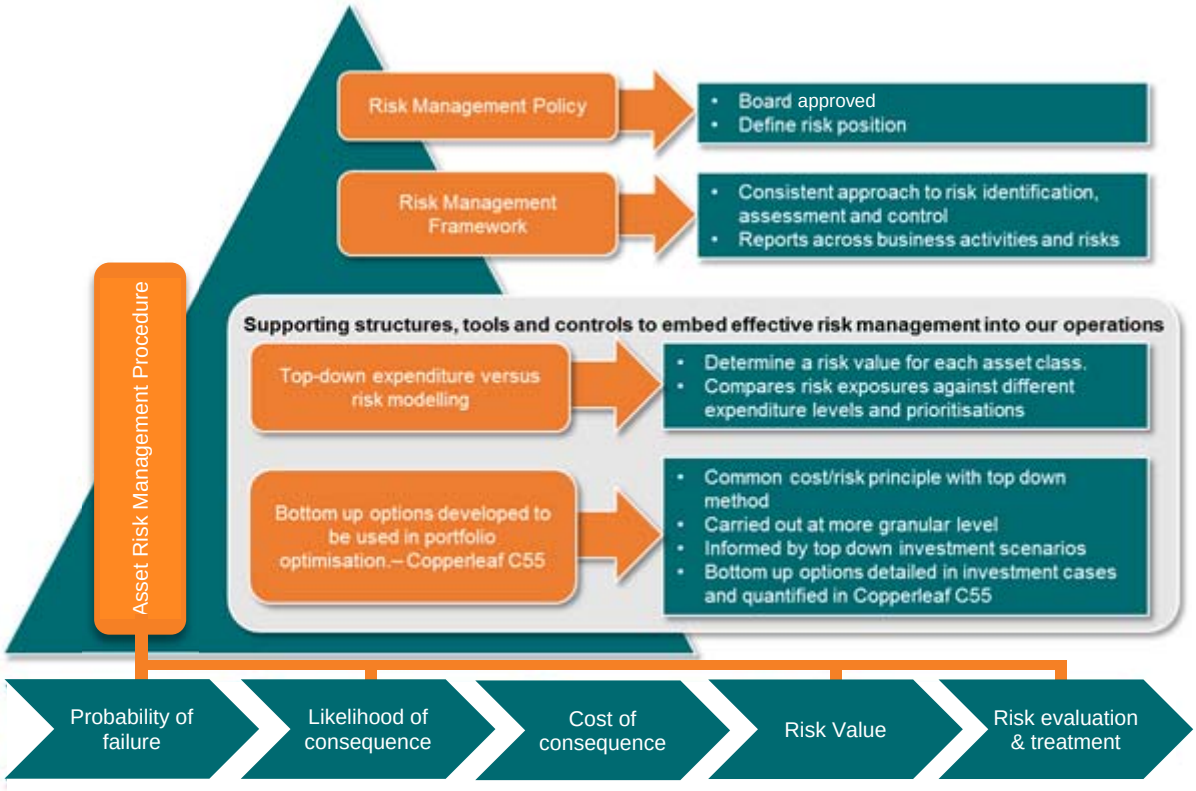
1.1 Purpose

This document is the Asset Risk Management procedure.

It has been developed to support Investment Cases and the asset renewal portfolio optimisation for the 2019-24 Regulatory Submission. As such, the intended audience in the short term is Investment Case owners and the Essential Energy team involved in putting together the regulatory submission. Going forward, the expectation is that the document should be used to underpin all network asset investments. The principles described may also be used in other scenarios e.g. for operational asset management.

Figure 1 shows the context, scope and main application of this document.

Figure 1 – Context, scope and main application of the Asset Risk Management Procedure



The Asset Risk Management procedure supports management of Essential Energy's Network Assets in line with the Corporate Risk Management Framework. It provides:

- Contextualisation and additional granularity required to support network asset risk management
- Guidance on requirements for options analysis between risk treatments
- Guidance on required levels of documentation, including before and after risks for preferred treatment options.

A key aim of the procedure is to support a consistent approach to network asset risk management across Investment Cases and portfolio optimisation activities. As such, it is intended that the output of this procedure will be used to assist with investment decisions and the investment optimisation processes.

It is acknowledged that this represents a subset of the total asset risk management process, which includes operational asset management and system control activities and decision making. It is also recognised that the

approach to asset risk management set out in this document marks a particular point within a longer-term maturity journey towards enhanced and more effective risk-based asset management.

1.2 Scope

The scope of the Asset Risk Management procedure is overall network risk, including:

- Safety
- Network Reliability
- Environment (including Bushfire)
- Compliance
- Reputation
- Financial

The procedure defines the overarching risk assessment framework for use within Investment Case development and the asset renewal portfolio optimisation used for the 2019-24 Regulatory Submission. This includes detailed guidance on approaches to:

- estimating 'Probability of Failure' and 'Likelihood of Consequences' for network assets
- calculating the combined risk value
- undertaking risk evaluation and identifying risk treatments.

Detailed guidance on the Cost of Consequence is provided in the Appraisal Value Framework. The framework itself sits within the context of the Corporate Risk Management Framework.

The procedure has been developed primarily to support network asset risk management in the context of network asset health and renewal. However, as stated above, the core principles may be applied to other types of asset management decision making.

The procedure is structured to align with the requirements of ISO31000:2009[1] and AS5577[2], as follows:

- Context (Section 2)
- Risk Identification (Section 3)
- Risk Analysis (Section 4)
- Risk Evaluation (Section 5)
- Risk Treatment (Section 6)
- Monitor & Review (Section 7)
- Communicate & Consult (Section 8)
- Documentation (Section 9)

Section 10 then sets out some additional guidance documents that may be used to support network asset risk management.

[1] ISO 31000:2009 Risk management – Principles and guidelines

[2] AS5577-2013 Electricity network safety management systems

2. Context

2.1 Operating environment

Essential Energy has many external stakeholders with significant influence and/or interest in the risk management decisions we make. This includes government (in their role as shareholder), customers and regulators.

This operating environment creates a healthy tension between the need to be able to demonstrate that we are doing enough to manage risk, so that risks are tolerable, while not doing too much, such that we are not over-investing in risk reduction.

2.2 Requirements for risk management

Essential Energy has risk management obligations placed upon it through various safety and environmental legislation and regulations.

In addition, Essential Energy Risk Management, Asset Management and Electrical Safety policies[3] establish clear requirements for risk management.

These documents set the framework for undertaking risk management in line with:

- ISO31000:2009 Risk management – Principles and guidelines, and
- AS5577-2013 Electricity network safety management systems.

2.3 Objectives for risk management

The objectives for asset risk management consider both the level of residual risk of asset failure and the maturity of approach, including tools, methodologies and decision making criteria.

Objectives for safety risk management are defined separately to objectives for other types of risks. This is reflective of specific requirements for safety risk, as set out in relevant legislation, regulations and good practice.

The target for residual safety risk is to ensure that all safety risks are tolerable and managed So Far As Is Reasonably Practicable, within deliverability and resource constraints.

For all other risk types, the target residual risk level is the level at which the risk is managed As Low As Reasonably Practicable[4].

Objectives for the approach to asset risk management (safety and non-safety) are to ensure a fit for purpose, proportionate and whole of life approach to risk management decision making that is consistently applied and aligned with the corporate approach and industry good practice.

[3] CECP8096 Company Policy: Electrical Safety

[4] The term ‘ALARP’ is used specifically for non-safety risks, where the term ‘SFAIRP’ is used solely for safety risks. While the use of terms is intended to differentiate between the different types of consequences, the principles applied are similar in that they identify the point at which additional controls are not reasonably practicable, based on the balance of cost and benefit.

2.4 Risk criteria

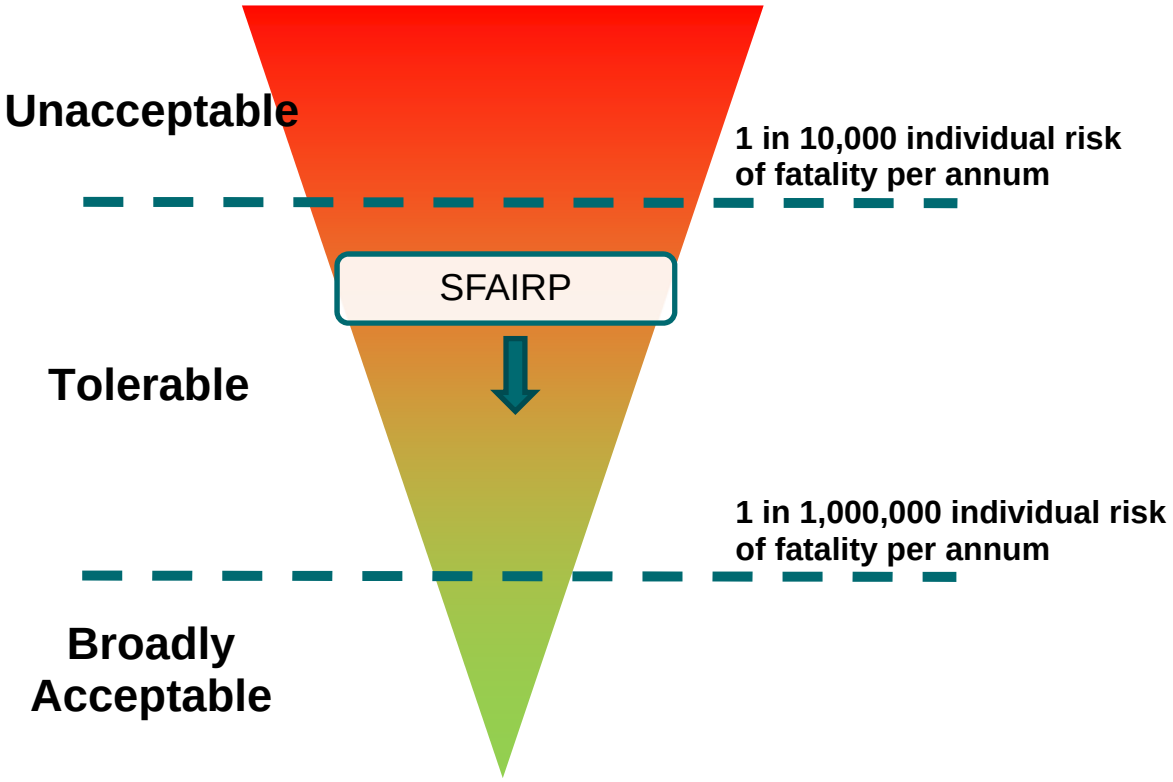
Criteria to evaluate the significance, tolerability and acceptance of risk are derived from relevant industry standards and good practice and the corporate risk framework.

2.4.1 Industry Standards and good practice

Figure 2 shows the framework and criteria for safety risk tolerability and acceptance. The is aligned with relevant industry standards and good practice, as set out in:

- AS7000[5]
- EG-0[6]
- Institute of Asset Management Subject Specific Guidelines[7]

Figure 2 - Safety Risk Tolerability and Acceptance Criteria



Within this framework:

- Risks in the Unacceptable region cannot be justified save in extraordinary circumstances; controls must be put in place to reduce the risk into either the Tolerable or Broadly Acceptable region.
- Risks falling within the Tolerable region are tolerated in order to secure some level of benefit and provided the risks are managed SFAIRP.
- Risks falling within the Broadly Acceptable region are generally regarded as insignificant and adequately controlled. Further actions to manage risks falling in this region are generally not required and should not be pursued unless they are reasonably practicable i.e. accepted good practice and low cost.

[5] AS/NZS 7000:2010 Overhead line design – Detailed procedures

[6] EG-0 Power system earthing guide Part 1: Management principles

[7] Institute of Asset Management SSG 31: Risk Assessment and Management

Once risks are managed SFAIRP, they are considered 'acceptable', noting that this may result in a level of risk that is above the Broadly Acceptable threshold level. It is not a requirement within this framework to reduce all risks into the Broadly Acceptable region (below 1 in 1,000,000 individual risk of fatality), unless that is reasonably practicable.

In this context, an 'acceptable' risk is a 'tolerable' risk which we are willing to live with as-is, without requiring further controls or action. For example, an asset risk may be 'tolerable' for a period of time, but not 'acceptable' until rectified.

2.4.2 Corporate risk criteria

Table 1 sets out the corporate risk appetite, as defined in the Essential Energy Risk Management Policy[8].

Table 1 – Corporate Risk Appetite

Risk Criteria	Risk Appetite
Safety	Very Low
Network Reliability	Moderate
Environment	Low
Compliance	Low
Reputation	Low
Financial	Moderate

Corporate criteria for evaluating the significance of risks are set out in the Essential Energy corporate risk matrix. This is provided in Appendix A for reference.

2.4.3 Application to Portfolio Risks

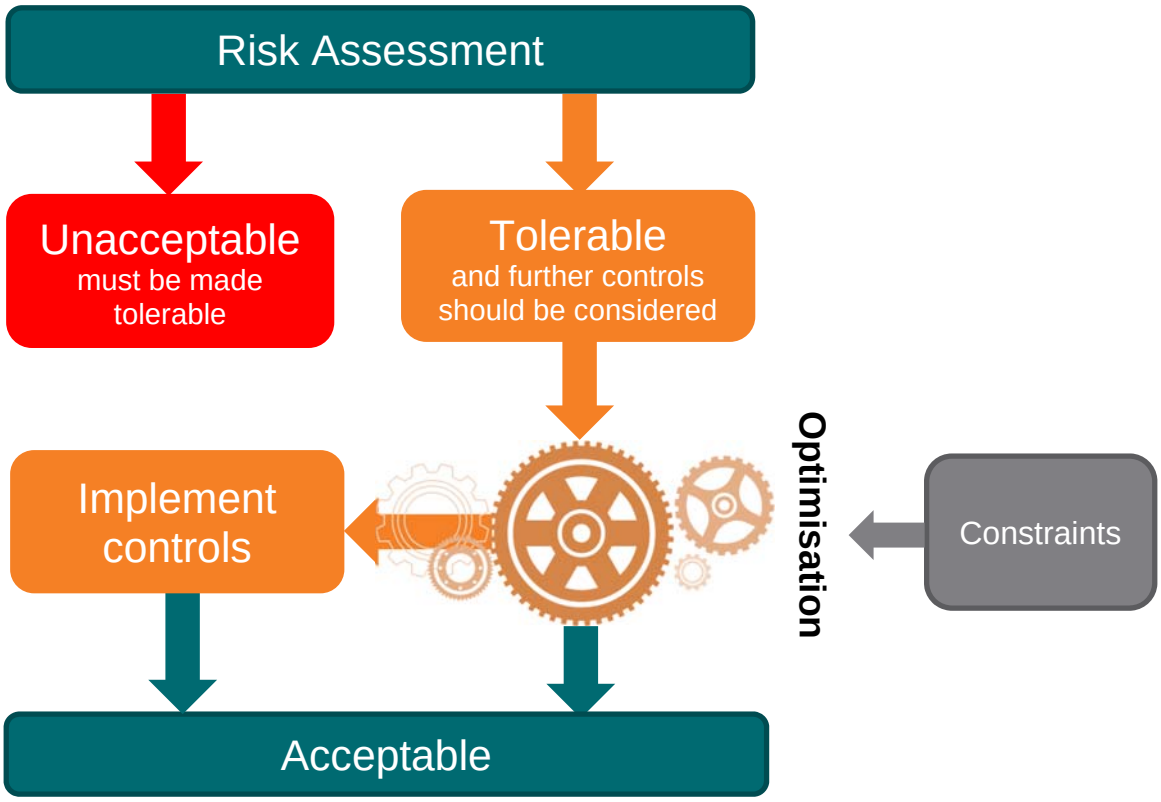
A portfolio of investment is qualitatively determined to meet the identified tolerability and acceptance criteria if:

- All unacceptable risks are made tolerable; and
- All compliance requirements are met; and
- Identified SFAIRP/ALARP treatment actions for risks are implemented, within constraints and with the aim of maximising collective risk reduction across the portfolio for the available resources

The application of the tolerability and acceptance criteria at a portfolio level is shown in Figure 3.

[8] Risk Management – CECP0002.03 – Issue 6

Figure 3 – Ensuring portfolio safety risks are managed SFAIRP/ALARP



2.5 Tools and methodologies

Asset risk management makes use of a variety of tools and methodologies, dependent upon the situation and ensuring that the technique and associated effort is proportionate to the risk.

Table 2 sets out guidance on different techniques to be considered for any situation, mapped against the different stages of the risk assessment process. This is based on similar guidance provided in IEC-ISO 31010: 2009 *Risk management – Risk assessment techniques*.

Table 2 – Techniques for Consideration in Asset Risk Management

Technique	Risk Assessment Process						Risk Treatment
	Risk / Cause Identification	Control Environment/ Effectiveness/ Options	Risk Analysis			Risk Evaluation	
			Consequence	Probability	Level of Risk		
Brainstorming or SME Workshop	✓	✓	✓	✓	✓	✓	✓
Structured Interviews	✓	✓	✓	✓	✓	✓	✓
Delphi	✓	✓	✓	✓	✓	✓	✓
Checklists	✓	✓	×	×	×	×	×
Failure Mode Effects Analysis	✓	✓	✓	✓	✓	✓	✓
Failure Mode Effects & Criticality Analysis	✓	✓	✓	✓	✓	✓	✓
Event Tree Analysis	✓	✓	✓	✓	✓	×	×
Fault Tree Analysis	✓	✓	×	✓	✓	×	×
Bow-Tie Analysis/ Threat Barrier Diagram	✓	✓	✓	✓	✓	×	×
Reliability Centred Maintenance	✓	✓	✓	✓	✓	✓	✓
Consequence/ probability matrix	×	×	✓	✓	✓	✓	×
Risk Indices	×	×	✓	✓	✓	✓	×
Cost/benefit analysis	×	×	×	×	×	✓	✓
Multi-Criteria Decision Analysis	×	×	×	×	×	✓	✓

Any technique will have blindspots, and therefore it is preferable to use more than one technique. Further guidance on the choice of technique for risk analysis is provided in Section 4.

2.6 Governance

Governance of this procedure is provided by a team of independent risk SMEs, with responsibility to review individual Investment Cases and the portfolio optimisation process and agree the appropriate application of the procedure.

3. Identification

The first step in managing asset risk is to thoroughly understand the hazards, their causes and consequences, and the current control environment. The most effective way of achieving this is through workshops with subject matter experts.

3.1 Hazard Identification

The purpose of hazard identification is to identify electricity network hazards (sources of risk – events, situations, agents or objects) that could cause an electricity related incident. As a minimum, this should consider:

a) Safety related aspects of the loss of supply;
b) Electrical work on or near network assets;
c) Other activities that may involve electrical hazards, including work being carried out in the vicinity of electrical assets;
d) Single and multiple failure modes, including knock-on effects as appropriate;
e) The design of network assets and the condition and operation methodologies for electricity network assets;
f) External hazards and natural disasters; and
g) Intentional and unintentional human activities
h) Lack of/ incorrect knowledge and uncertainty
i) Systemic issues which may aggravate, hide or create vulnerabilities

The risk analysis is centred around one or more hazardous events related to the need for the investment, such as functional failures of assets. When identifying hazardous events, consideration should be given to the scenario which allowed them to occur.

A key aim of hazard identification is completeness. As such, evidence should be drawn both on what has happened in the past, and what could have happened in the most plausible worst-case scenario. This may include relevant incidents that have occurred on other electricity networks, within Australia and internationally.

3.2 Areas of impact

What things of organisation value may be affected if the source of risk were to eventuate. This relates to the value matrix and more broadly to corporate values, priorities and goals, and impacts in the corporate risk procedure. These would typically include:

a) Safety - including serious injuries to severe events affecting the public or an employee, and harm as a result of supply loss
b) Network (reliability and security) – including SAIDI, SAIFI, VCR, damage to other network assets, and reputation impacts
c) Bushfire
d) Environment – other than bushfire
e) Compliance
f) Reputation - where not incorporated in one of the other consequences
g) Finance – where not addressed elsewhere
h) Customer and community
i) Operational

3.3 Consequence Identification

It is important to identify how risk will affect the areas of impact (eg degrade, harm, delay, prevent), including consequences to the network workforce, the public, other stakeholders, and safety related environmental impacts. This should include consideration of consequences that are reasonably foreseeable as well as those that have occurred in previous known events.

The risk assessment also considers the potential for cascading and cumulative consequences.

To avoid double counting, it is important to indicate how consequences are apportioned across the relevant areas of impact for each risk event.

3.4 Cause Identification

To effectively manage risk, an understanding is needed of the causes of hazardous events. Each hazard will typically have several causes or failure modes (e.g. rot and weather). Root causes are often identified through processes such as Failure Mode, Effects and Criticality Analysis (FMECA), although simpler methods may also be used, provided they are systematic, involve the right people and are documented. While considering each cause, consider the circumstances which led to its occurrence and what could have prevented it. In some cases, causes need to occur in a particular order or in combination for a risk event to arise. At times the risk cause may not be evident, or may be as a result of 'normal deviation'. The significance of the cause in relation to the risk event also should be considered.

3.5 Risk Event

This is a statement that combines the source of risk, impact to objectives and cause. This is typically the focal point or 'stake in the ground' upon which the risk is assessed. A range of scenarios can be used to model how changes in the size and nature of the risk source may alter the risk consequences. This is a particularly useful technique when modelling the risk implications of a change in business practice.

3.6 Human and Organisational Factors

These are systemic issues that will (typically negatively) affect controls, causes, risk events or consequences (e.g. poor employee engagement).

3.7 Control Environment

An important part of the 'Identification' stage is to understand the current, or minimum control environment e.g. to satisfy compliance requirements.

Two key methods for understanding the control environment are:

- Threat Barrier Diagrams
- Bow Tie Diagrams

Figure 4 shows a simple Threat Barrier Diagram for the example of explosive failure of an asset. The Threat Barrier Diagram allows visualisation of the relationship between causes (threats), controls (barriers) and consequences. Importantly this includes 3rd party actions, which can help build the understanding of the extent to which Essential Energy can influence the nature and magnitude of outcomes or consequences of an incident.

Figure 4 - Threat-Barrier Diagram

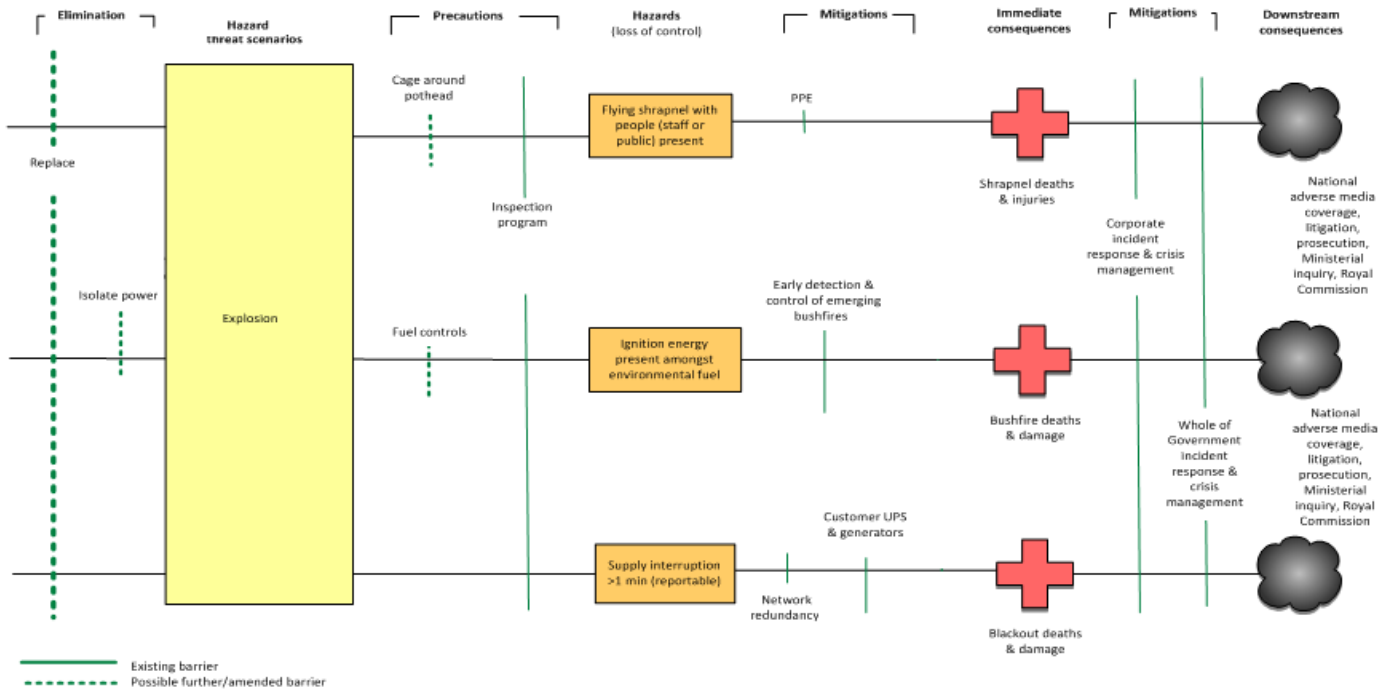
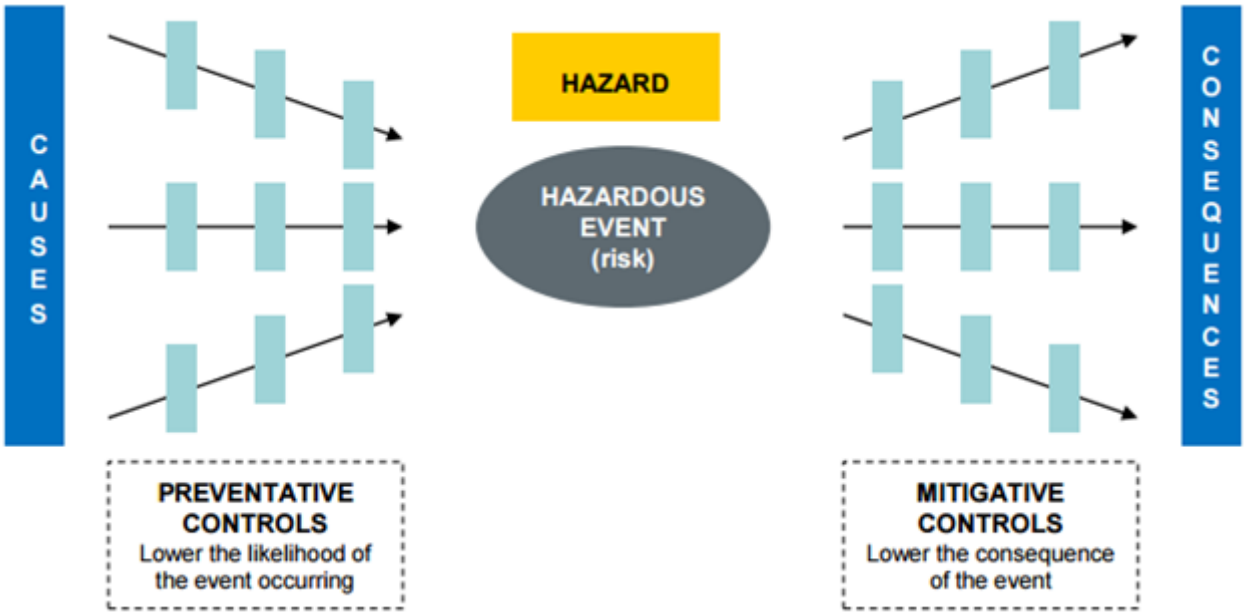


Figure 5 shows a conceptual example of a Bow-Tie diagram. In situations where there is a single hazardous event with no downstream consequences or knock-on effects, this can be used as a simple way of representing the threat-barrier diagram.

Figure 5 – Bow-Tie Diagram



Regardless of the method used, for each cause, the realistic preventative controls should be included. These are controls which reduce the likelihood of the hazardous event occurring, but do not prevent or mitigate the consequences if it were to occur. For each consequence, the realistic mitigative controls should be included. These are controls which reduce the likelihood or impact of a consequence occurring.

A key outcome from both Threat Barrier and Bow Tie Diagrams is an understanding of the effectiveness of the overall control environment and the criticality of individual controls.

The effectiveness of existing controls individually and combined, enhancements to the system of control, as well as escalation factors would be considered here.

4. Analysis

The purpose of risk analysis is to calculate the level of risk. Analysis can be qualitative, semi-quantitative or quantitative. Whichever method is chosen, risk is fundamentally analysed as the product of the consequences and their likelihood of occurring. Figure 6 shows the risk calculation:

Figure 6 – Risk Calculation

Key considerations in risk analysis include:

- Choosing an appropriate technique
- Factors affecting the likelihood, consequences and effectiveness of controls in different scenarios
- Levels of uncertainty in the analysis and the need to perform any sensitivity analysis
- The need to document any supporting assumptions, limitations, data sources and who was involved

The outputs of risk analysis may be used as a direct input to risk evaluation and decision making. Alternatively, they may be used to determine the need to undertake more investigative work.

The effort and methods used to calculate risk should be proportionate to factors including:

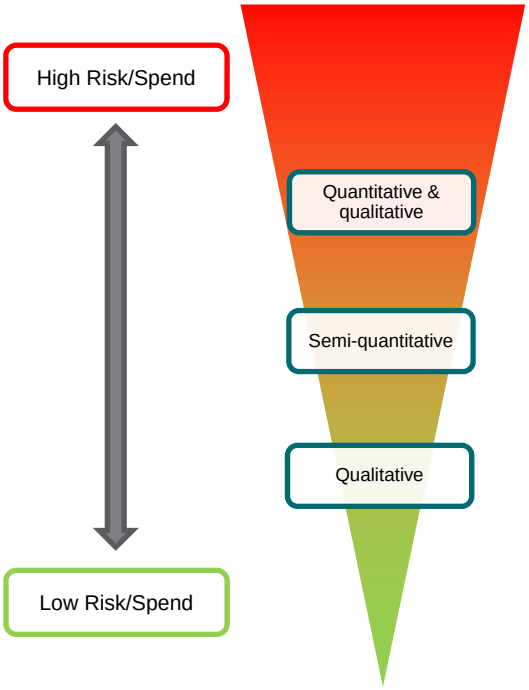
- The level of risk
- The level of spend or effort associated with control of the risk
- The level of uncertainty around the risk calculation and the importance of this for decision making

Figure 7 shows broad guidance on the relationship between methods used, and the level of risk.

In situations where there is high uncertainty or complexity, or high levels of societal concern, multiple techniques should be considered, including consideration of company and community values and tolerability.

Guidance set out in this document represents the expected application of risk analysis methods for Investment Cases and feeding into portfolio optimisation.

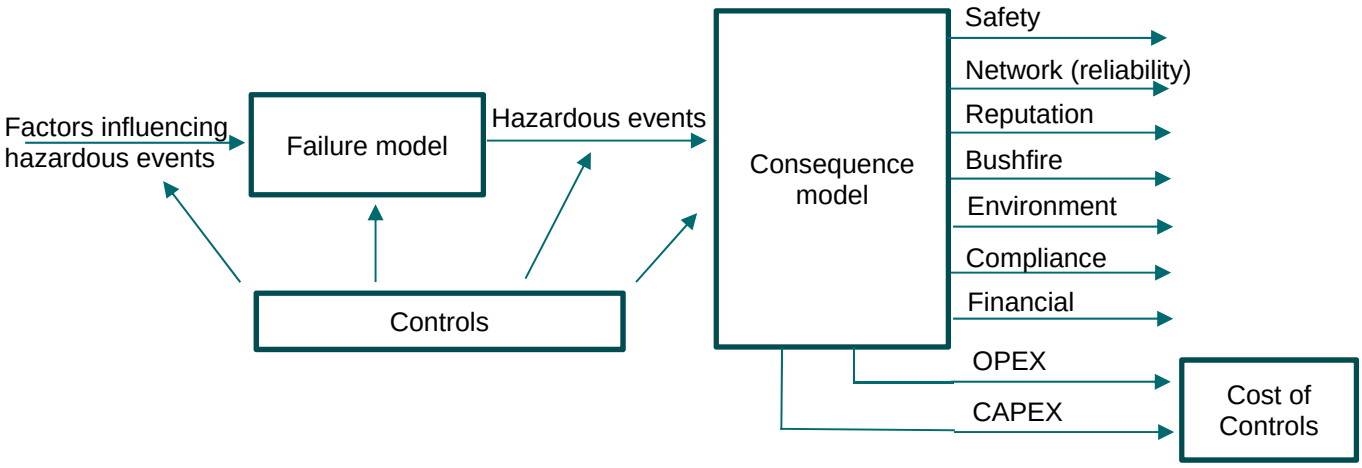
Figure 7 – Expected application of alternative risk analysis methods



4.1 Conceptual Risk 'Model'

Establishing the level of a risk requires clear specification of the actual components of the risk being considered, i.e. the specific sequence of events including the nature of consequences to be considered, the exposure to the chosen hazard, and finally the probability or likelihood of that scenario taking place. In assessing and determining both the exposure and the probability, the existing controls are considered. This general framework is set out in Figure 8 which shows the conceptual risk 'model' for asset risk management.

Figure 8 – Conceptual Risk Model for Asset Risk Management



Any scenario involving a given hazard can lead to different consequences depending on the sequence of exposure events. Hence one risk assessment may require many risk analyses as any risk should be assessed separately for each chosen sequence of events.

The remainder of Section 4 provides guidance on the component parts of the conceptual risk model as:

- Likelihood of hazardous events
- Likelihood of consequence
- Control effectiveness
- Cost of controls

As stated in Section 1.2, the 'cost of consequence' is described elsewhere, in the Appraisal Value Framework.

4.2 Likelihood of Hazardous Events

Where applicable, the likelihood ratings from the corporate risk matrix may be used to assess the likelihood of hazardous events (see Appendix A). However, often this rating scale does not provide sufficient granularity to inform asset risk management. Where this is the case, alternative methods of estimating the likelihood of hazardous events should be used.

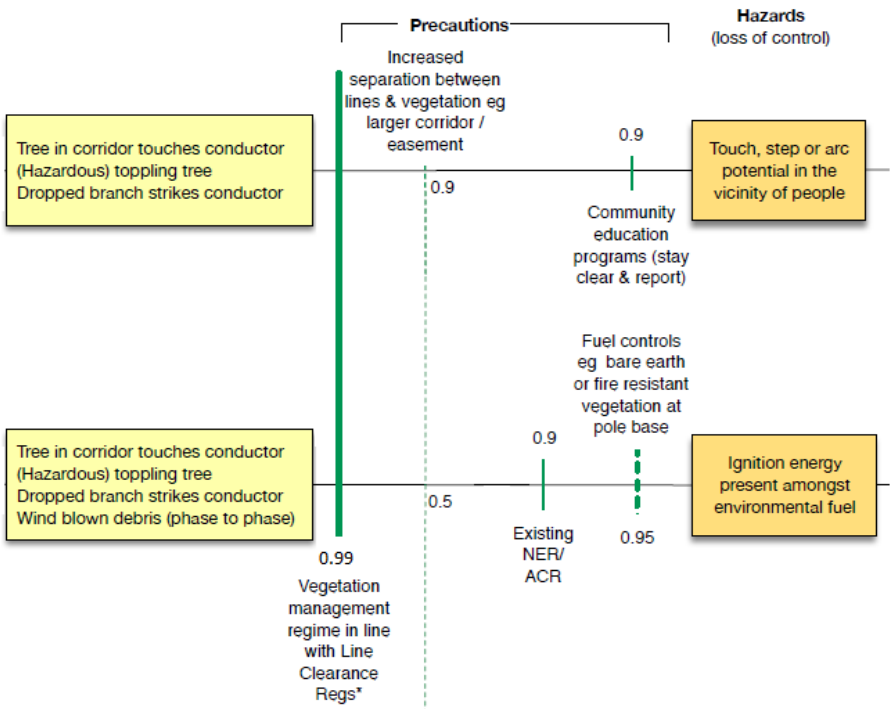
Not all assets are equally likely to fail or result in a hazardous event. The probability of the hazardous event occurring should be based on the asset health assessment and can often be supported by historic data.

Asset health assessment can be done through a conditional assessment, such as defects or measurements taken on inspection, using age as a proxy for health, or through expert judgement.

Where appropriate, a probabilistic distribution (for example, Weibull distribution) should be applied to the asset health to probabilistically predict the likelihood of failure. This can represent the most foreseeable failure mode, or the combined effects of multiple failure modes.

The likelihood of hazardous events occurring with different controls can be quantified by first quantifying the effectiveness of the controls. Consider the left-hand side of the threat-barrier diagram shown in Figure 9, where solid lines show existing preventative controls and dashed lines show preventative controls which are not presently used.

Figure 9 – Threat-barrier diagram for vegetation contact



The present controls for each hazardous event have an effectiveness of 99% and 90%. Assuming each of the controls is independent, the effectiveness of the controls at managing each of the hazardous events is $0.99 +$

$(1 - 0.99) \times 0.9 = 0.999$, or an effectiveness of 99.9%. This means that removing all the existing controls would result in $\frac{1}{1-0.999} = 1000$ times more hazardous events than present. So, if each of the hazardous events currently occurs once every ten years we can deduce that without controls they would occur 100 times every year.

This approach can be extended to calculate the likelihood of the hazardous events occurring under different options. In the case of widening easements, the touch/step likelihood is reduced by 90% while the fire start likelihood is reduced by 50%. In the case of removing vegetation from the base of poles, only the fire start likelihood is reduced by 95%.

If both controls are implemented, the touch/step likelihood is reduced by 90% ($\frac{1}{1-0.9} = 10$ times less events) while the fire start likelihood is reduced by $0.5 + (1 - 0.5) \times 0.95 = 0.975$, or an effectiveness of 97.5% ($\frac{1}{1-0.975} = 40$ times less events).

4.3 Likelihood of consequence

The likelihood of consequences occurring should be assessed having regard to relevant information on historical fault frequencies and level of exposure of persons to the hazard. This may be derive from internal sources of from relevant data from the broader electricity industry.

A key concept in determining the likelihood of consequences is that of 'consequence differentiators'. These are discussed in Section 4.3.1. The remainder of this section then sets out specific guidance on estimating the likelihood of the different types of consequences considered within asset risk management.

4.3.1 Consequence Differentiators

Consequence differentiators are factors related to the asset or the operating environment that influence the likelihood of a consequence occurring or the magnitude of the outcome. They should carefully be selected given a thorough understanding of the risk environment.

For example, an asset that poses a bushfire risk will generally pose a higher risk in a P1 bushfire priority zone than an equivalent asset in a P4 bushfire priority zone[9]. This risk may be due to a higher likelihood of an uncontrolled fire started by an asset turning into a bushfire, as well as a higher impact in terms of consequence if a bushfire does start. However, operational practices of the organisation such as increased inspection frequency may mean a lower likelihood of failure occurring in a P1 bushfire priority zone.

When selecting differentiators, consideration should be given to the availability of data which will allow the assets to be differentiated. Table 3 – Suggested consequence differentiators presents some examples of consequence differentiators.

[9] See CEOP8067 – *Bushfire Risk Classification* for the background and definition of bushfire priority zones

Table 3 – Suggested consequence differentiators

Risk	Consequence Differentiators
Safety	Location in areas of high public exposure
	Presence of explosive failure mode
Network (Reliability)	Number of customers affected
	Customer load affected
	Availability of redundant supply
Reputation	Proximity to high visibility public sites
Bushfire	Bushfire priority zone
Environment	Proximity to heritage site
	Availability of containment measures (such as oil bunding)
Finance	High-value assets within falling / explosion radius
	Cost of fault-and-emergency replacement

4.3.2 Consequence Scales

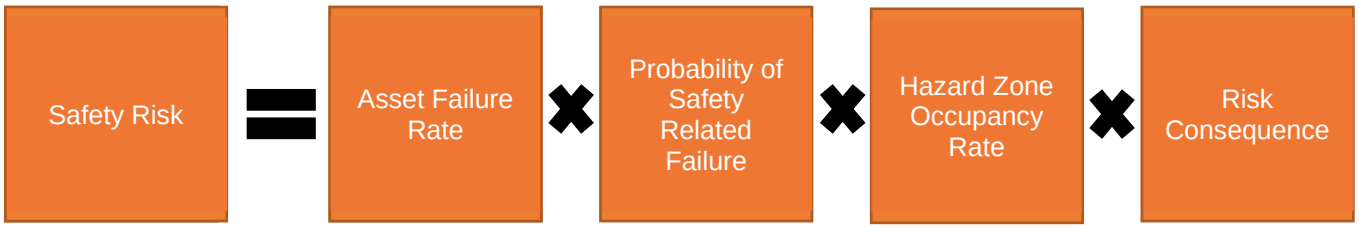
The corporate risk matrix provides a reference set of consequence scales that all asset risk assessments should align with. These are provided in Appendix A.

4.3.3 Safety

The safety category is used to categorise the direct consequences of an incident which affects safety. The most plausible worst-case scenario for most network assets involves a single severe safety incident, so this is the focus of the risk analysis. It is also possible to model the likelihood of a serious injury.

Figure 10 – Fundamental principle of safety risk calculation shows the fundamental safety risk calculation.

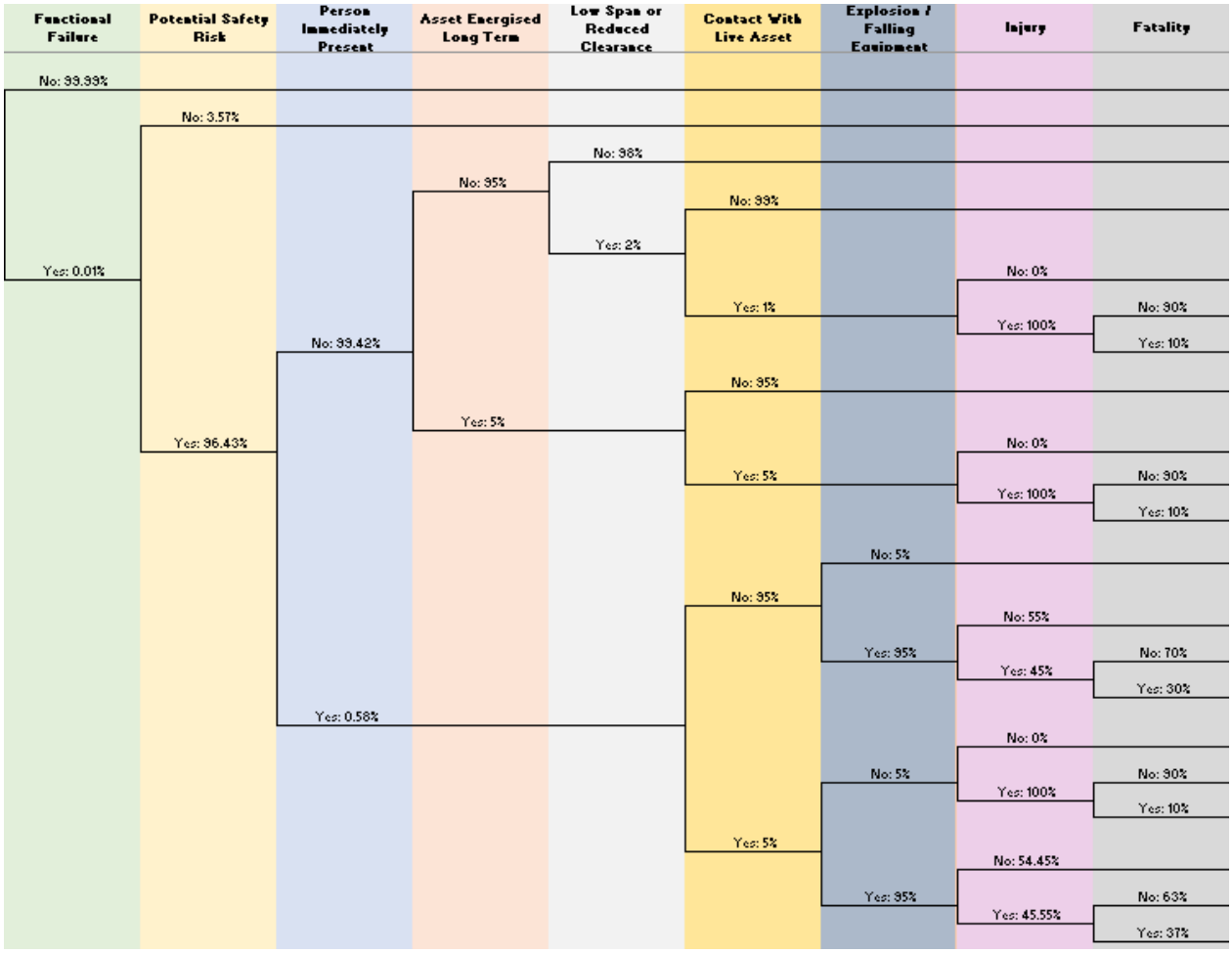
Figure 10 – Fundamental principle of safety risk calculation



It is recommended that safety risk associated with a hazardous event is analysed through use of the event tree method. At a minimum, the event tree should consider the probability of the asset failing, the probability of exposure, the probability of injury and the probability of fatality.

A Safety Event Tree tool has been developed to allow a consistent approach to calculating the likelihood of a safety event for overhead network assets where a risk is posed over the long-term and the occupancy at the time of hazard does not reflect the true risk. Circumstances that result in long-term risks include conductors being low to the ground, or where the fault impedance is too high for network protection devices. Figure 11 – Safety Event Tree Tool shows a screenshot from the Safety Event Tree tool.

Figure 11 – Safety Event Tree Tool



4.3.4 Network (Reliability)

The Network category captures all consequences associated with loss of power supply.

Reliability data for most assets can be sourced from the document 'Assessment of Reliability for Network Programs'. This should be sourced as average customers disconnected, and average duration off supply. It is important to consider whether there is sufficient data for 'statistical certainty' (see Appendix B for further detail of this concept).

For most distribution asset failures, the value of customer reliability should be calculated as follows:

$$Value\ of\ customer\ reliability$$
$$= Average\ customers\ affected\ \times (Duration\ value\ (\frac{\$}{customer-minute})$$
$$\times\ Average\ duration\ (minutes) + Flagfall\ value\ (\frac{\$}{customer})$$

The $ values for the Duration and Flagfall methods are provided in the Appraisal Value Framework.

In specific circumstances where the interrupted energy is known, or there are major industrial loads affected that are not representative of an average customer, the appropriate calculation is:

$$Value\ of\ customer\ reliability$$
$$= Enery\ interrupted\ value\ (\frac{\$}{MWh})\ \times\ Average\ load\ (MW)\ \times\ Average\ duration\ (hours)$$

The $ value for this 'Energy Interrupted' method is also provided in the Appraisal Value Framework.

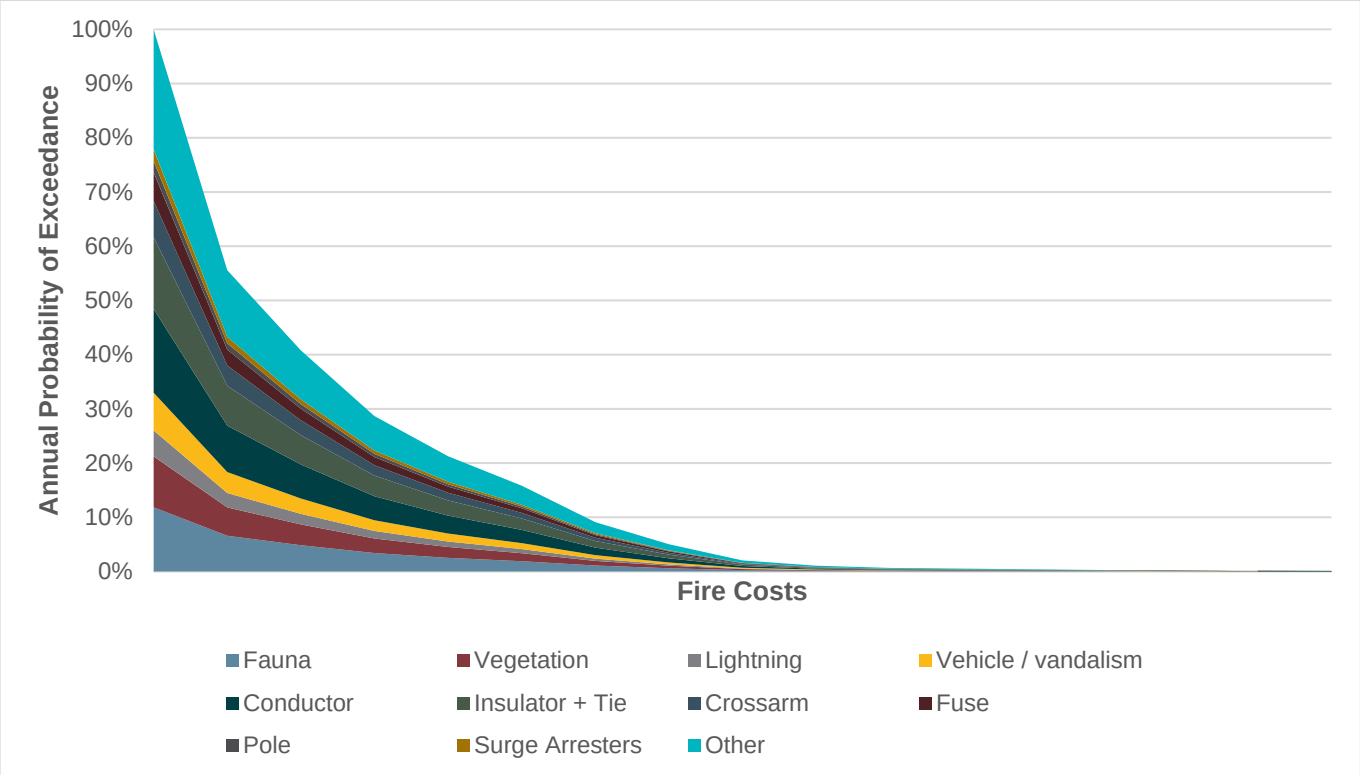
The likelihood should be calculated consistent with expected operating environment. For example, if a major network consequence occurs in 60% of failures, and there is network redundancy available in the remaining 40% of cases, then the full reliability consequence should only be considered in 60% of failures. In this case, a consequence differentiator can be considered to prioritise investing where there is no redundant supply.

4.3.5 Bushfire

Bushfires are complex events with significant uncertainty regarding predicting the circumstances which lead to their occurrence and the magnitude of the consequences. Essential Energy has used the Pheonix RapidFire empirical bushfire model to understand the property impact resulting from fires started in the worst possible conditions. For these purposes, it is assumed that property loss is a proxy for total bushfire cost.

Using historic fire start records and weighting the likelihood of fire starts by Bushfire Priority Zones, the Pheonix consequence was aligned with the probability of exceedance of fire costs related to Essential Energy's network[10]. Figure 12 – Probability of fire cost exceedance by hazardous event shows indicative results from this modelling, demonstrating the variability in outcomes from various causes of fires.

Figure 12 – Probability of fire cost exceedance by hazardous event



A model has been developed to consistently calculate the probabilities of severe and moderate bushfires occurring given the number of fire starts. This is described in the Appraisal Value Framework document.

4.3.6 Environment (Other)

The environment (other) category captures damage to the environment, other than bushfire damage. There are a wide variety of environmental risks, with a range of potential consequences. For this reason, environmental consequences are determined on a case-by-case basis. The likelihood should be calculated using historic data and

[10] Bushfire Liability Overview Essential Energy (December 2016), Aon Risk Services Australia

a quantitative understanding of the effectiveness of controls. In circumstances where historic data is not available, an event tree or other quantitative methodology should be used.

4.3.7 Compliance

The compliance category captures the need for completing programs to comply with a legislated requirement, for example a breach of the National Electricity Rules or failing to comply with an IPART directive. The consequences of non-compliance are determined on a case-by-case basis through discussion with the appropriate regulatory body (AER or IPART).

4.3.8 Reputation

The reputation category captures reputation impact to the organisation from industry, community, government, media or other stakeholders in circumstances other than those captured in the previous consequence categories. The likelihood of reputation impact should be estimated as a proportion of events which are likely to receive attention from stakeholders.

4.3.9 Financial

The financial category is used for all financial consequences associated with the hazardous event that do not fit into any of the other categories and are over-and-above the typical planned replacement costs. This might include collateral damage to Essential Energy or third-party assets. For example, a pole failure may have an associated financial cost associated with equipment on the pole, such as a pole-top transformer, recloser or regulator. The likelihood of these financial consequences should be based on historic information, data on asset distribution, or calculated using an event tree.

4.4 Control effectiveness

Risk analysis needs to consider the effectiveness of current and potential future controls. This includes identifying the effectiveness of controls at reducing the likelihood of the hazardous event or consequence occurring, particularly when the control spans multiple causes or consequences.

The control environment effectiveness should be rated using the scale described in Table 4 - Control Environment Effectiveness.

Table 4 - Control Environment Effectiveness

Descriptor	Rating
Nothing more to be done except review and monitor the existing controls, which are well designed for the risk, address the root causes, and are believed to be effective and reliable at all times.	5 - Effective
Controls are in place, well designed and effective. The operating effectiveness of some controls could be improved or there may be some doubts about their effectiveness and reliability.	4 - Satisfactory
While the design of controls maybe largely corrects, in that they treat most of the root causes of the risk, they are not currently very effective. Or: Some of the controls do not treat the root causes even if those that are correctly designed are operating effectively	3 - Poor
Significant control gaps. Either controls do not treat root causes, or they do not operate effectively.	2 - Ineffective
Virtually no controls in place and those that are in place have very limited operational effectiveness or are poorly designed	1 - None

4.5 Cost of Controls

The cost of current controls needs to be understood to support any assessment of the value of investment. This includes opex and capex costs.

Guidance on the financial principles to be used, including the costs to be included and excluded are set out in the Investment Evaluation Procedure.

5. Evaluation

Once the risk level has been estimated, it must be compared with the risk tolerability and acceptance criteria described in Section 2.4 of this document, to understand whether additional treatments are required.

5.1 Safety Risk

For individual hazards or threat scenarios, the level of safety risk is considered acceptable once it is tolerable and managed SFAIRP.

The tolerability of safety risk is determined through comparison with the criteria set out in Figure 2 and Table 1.

Guidance on the interpretation and application of the term 'reasonably practicable' is provided in the Work Health and Safety context by Safe Work Australia[11]. In this context, reasonably practicable means that which is, or was at a particular time, reasonably able to be done to ensure the health and safety, taking into account and weighing up all relevant matters including:

a) The likelihood of the hazard or the risk concerned occurring
b) The degree of harm that might result from the hazard or the risk
c) What the person concerned knows, or ought reasonably to know, about the hazard or risk, and ways of eliminating or minimising the risk
d) The availability and suitability of ways to eliminate or minimise the risk, and
e) After assessing the extent of the risk and the available ways of eliminating or minimising the risk, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.

To meet these requirements, we must meet the standard of behaviour expected of a reasonable organisation in our position and who is required to comply with the same requirements.

For practical purposes, in the context of asset management decision making, the SFAIRP test may be demonstrated through:

- Demonstrated compliance with relevant technical standards
- Application of established industry good practice
- Reasoned judgement of a competent professional
- Quantitative risk-cost-benefit analysis

The main principle in managing safety risk SFAIRP is to demonstrate that the sacrifice (in terms of cost, time or trouble) required to do more to manage the risk, would be grossly disproportionate to the benefit gained.

Where risks do not meet the tolerability or acceptance criteria, the priority for treatment will be:

1. Immediately address any intolerable risks
2. Address issues of non-compliance
3. Prioritise remaining risks based on consideration of risk and value (risk reduction per dollar invested).

[11] Safe Work Australia, Interpretive Guideline – Model Work Health and Safety Act, The Meaning of 'Reasonably Practicable'. Available at:

5.2 Non-Safety Risks

For non-safety scenarios, the level of risk is considered acceptable once it is tolerable and managed ALARP.

The tolerability of risks is determined through comparison with the corporate risk criteria set out in Table 1.

Principles for determining whether a non-safety risk is managed ALARP are similar to those used to demonstrate SFAIRP i.e.:

- Demonstrated compliance with relevant technical standards
- Application of established industry good practice
- Reasoned judgement of a competent professional
- Quantitative risk-cost-benefit analysis

The key difference between safety and non-safety risks in this respect is that the legal obligation to demonstrate 'gross disproportion' is not required. However, this is replaced by the regulatory requirement to demonstrate that risk treatments are prudent and efficient.

6. Treatment

Where it is determined that current risk controls are not yet acceptable, additional treatments must be considered.

From a safety perspective, the outputs from this step must be a robust and documented answer to the questions: *'What more could we have done to control the risk? Why haven't we done it?'*

In particular, AS5577, Appendix B3 establishes specific requirements for options analysis in that it states: "where the consequences could include fatalities, there should be an exhaustive search for alternatives, detailed evaluation of the resulting risk reductions (qualitative or numeric), and realistic estimates of the associated cost increments."

Key components to this include:

- Options identification, including application of the hierarchy of control
- Assessment of the effectiveness and impacts of identified treatment options
- Understanding the costs of identified treatment options
- Options analysis

6.1 Options Identification

The aim of options analysis is to identify practicable options for inclusion in options analysis.

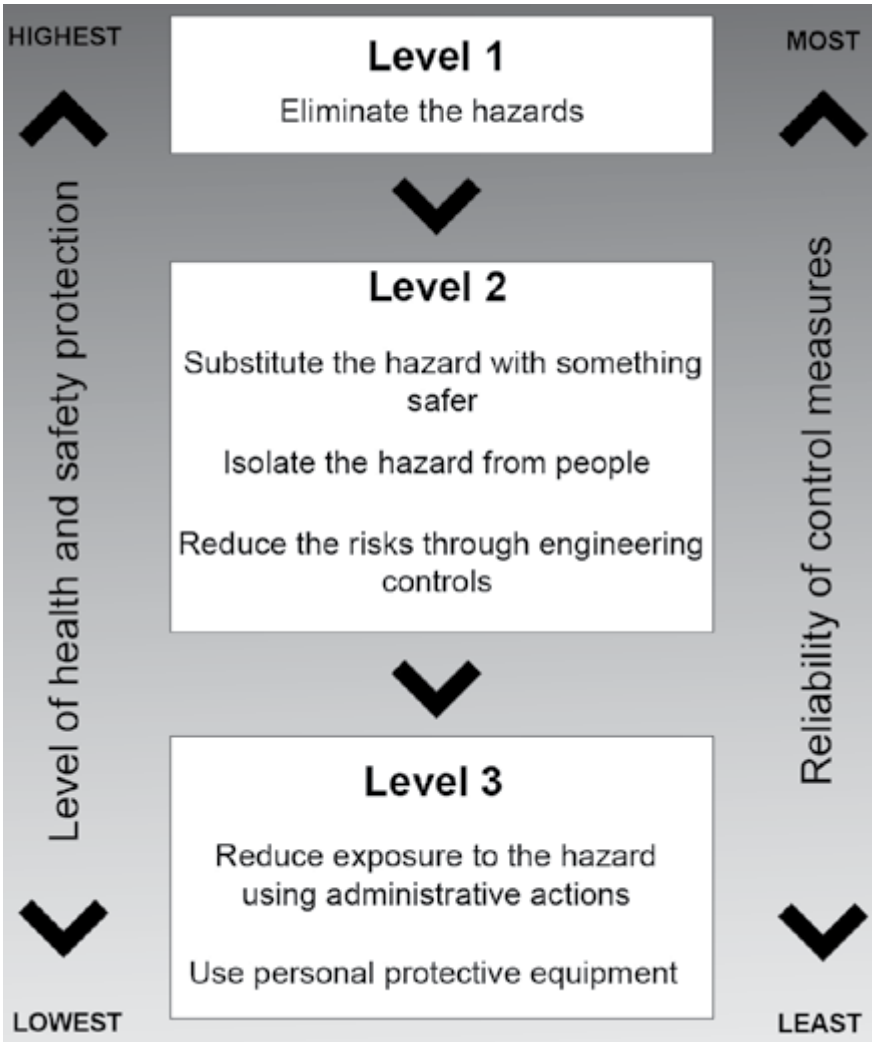
This process needs to involve the right people and consider the hierarchy of control, as set out in Figure 13.

Eliminating the hazard must always be the aim where it is reasonably practicable to do so.

Options may include variations on the extent and timing of treatments.

Where possible, options identification should consider 'optimum' and 'do minimum' treatments.

Figure 13 - Hierarchy of Risk Control



As an example, consider an asset with a manufacturing defect which poses a fatal safety risk to staff if failure occurs. Failure can also start a bushfire, and every failure results in the disconnection of customers. The most cost-effective method for eliminating risk was identified to be replacement. Where replacement is not reasonably practicable, physical barriers and changes to work practices can be used to reduce the risk.

6.2 Effectiveness/impact of options

Controls are used to modify risk. While controls are typically introduced to reduce the level of one or more risks, they may directly or inadvertently increase the level of another risk. Many controls also have a cost, which may not necessarily be financial. For example, de-energising a feeder is a control which may be used to mitigate safety and bushfire risk, while incurring a cost of network reliability. A complete understanding of the effects of using and changing controls is required before investment decisions are made.

6.3 Cost of Options

After identifying the options, estimates of the cost of completing each option should be developed. In most cases, the cost can be calculated as:

$$Planned\ replacement\ cost = number\ of\ planned\ replacements\ \times\ unit\ rate$$

More detailed estimates are required in some circumstances, such as where the cost of investment differs significantly between units.

Most asset failures require fault-and-emergency response to rectify. By preventing these failures, there is an opportunity to prevent costs from being incurred. This should be incorporated through either:

1. Failure cost, where the program budget includes the cost of failures
2. Failure benefit, where the program budget includes only the cost of planned replacements

The CAPEX failure component should therefore be calculated using one of the following methods:

$$(1)\ CAPEX\ failure\ cost = failures\ \times\ CAPEX\ cost\ per\ failure$$

$$(2)\ CAPEX\ failure\ benefit = failures\ prevented\ \times\ CAPEX\ cost\ per\ failure$$

Some costs associated with failures are not capitalised. Where the OPEX cost per failure is not able to be accurately estimated, for most assets this can be estimated using the rule-of-thumb of 70% additional cost of the planned unit rate. Similarly, the OPEX component should be calculated as:

$$(1)\ OPEX\ failure\ cost = failures\ \times\ OPEX\ cost\ per\ failure$$

$$(2)\ OPEX\ failure\ benefit = failures\ prevented\ \times\ OPEX\ cost\ per\ failure$$

where: $OPEX\ cost\ per\ failure = 0.7\ \times\ unit\ rate$

It is important to consider other sources of CAPEX and OPEX costs and benefits such as reduced inspection or maintenance requirements, or deferred network expenditure. For example, if an aging asset requires yearly inspections instead of the four-yearly inspections received by new assets, the cost of three inspections can be saved every four years if the asset is replaced.

The total CAPEX is therefore:

$$CAPEX\ cost = Planned\ replacement\ cost + CAPEX\ failure\ cost$$

$$CAPEX\ benefit = CAPEX\ failure\ benefit + other\ CAPEX\ benefits$$

Similarly, the total OPEX is therefore:

$$OPEX\ cost = OPEX\ failure\ cost + other\ OPEX\ costs$$

$$OPEX\ benefit = OPEX\ failure\ benefit + other\ OPEX\ benefits$$

6.4 Options Analysis

Possible outcomes from options analysis may include:

- Identified practicable options for inclusion in portfolio optimisation within the Asset Investment Planning System (C55 software).
- A preferred option, identified from analysis outside of C55

Options analysis may consider both the validity of options from the perspective of reasonable practicability, as well as the prioritisation of a number of reasonably practicable options (see Section 6.4.1). Alternatively, it may identify a single ‘optimum’ treatment.

Options analysis needs to take a balanced view of the risk and value of different options, taking account of the overall investment objectives while ensuring that statutory obligations e.g. around managing safety risk, are met. A key consideration in this may be inter-dependencies on other programs of work (see Section 6.4.2).

In this context, the option resulting in the lowest safety risk may not necessarily be preferred if it can be demonstrated that the impact on other obligations, objectives or plans would be gross disproportionate.

Options analysis should consider the need to undertake sensitivity analysis on any key assumptions, particularly if there are material uncertainties in any models or data underpinning the calculation.

6.4.1 Prioritisation of options

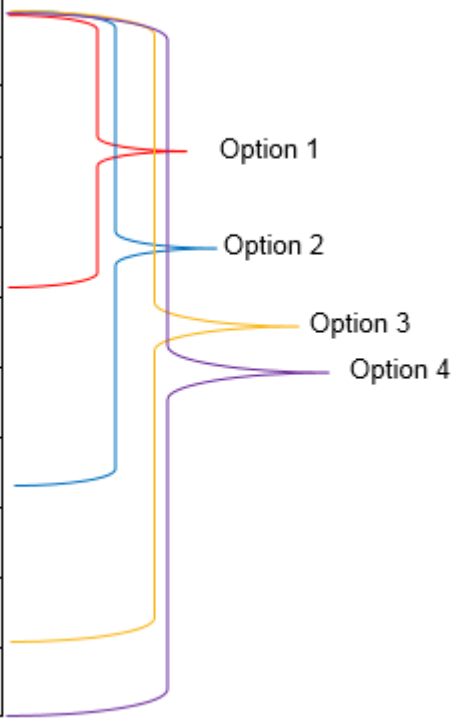
With an understanding of the effectiveness of controls and the available nonhomogeneous asset groups, controls should be grouped into possible investment options using a priority order.

Figure 14 shows an example scenario where asset health was assessed and rated from one to five. The consequence differentiators selected were bushfire priority zone and number of customers affected. In this case, a safety differentiator is not selected as the consequence scenario is expected to be the same once a hazardous event has occurred.

The next step is to order the nonhomogeneous groups by priority for replacement. In this case, health is the largest driver for replacement, followed by bushfire zone and finally customers affected. This priority ordering should be conducted in workshops by leveraging on the experience of subject matter experts.

Figure 14 – Prioritisation by health and consequence differentiators

Health	Bushfire zone	Customers Affected	Priority
5	-	-	1
4	P1	-	2
4	P2	Top 25%	3
4	P3	Top 25%	4
4	P4	Top 25%	5
4	P2	Bottom 75%	6
4	P3	Bottom 75%	7
4	P4	Bottom 75%	8
3	P1	-	9



Finally, the prioritised order should be grouped into investment options. Options should be chosen which require different levels of expenditure and provide different levels of risk mitigation.

In circumstances where there is a very limited number of assets, the priority order can be determined by assessing individual assets.

6.4.2 Inter-dependencies with other programs

Electricity distribution systems are complex not only due to the vast number of assets, but also because many of these assets are dependent on others. For example, the act of replacing a distribution pole mitigates both the direct risk of the pole but also the associated risk of the pole-top assets such as cross-arms. Redundancy is often incorporated into systems which have high failure impact, further complicating the risk environment.

Due to this complexity, qualitative risk analysis is often performed on programs independently. For example, analysis of the cross-arm replacement program assesses the relationship between cross-arm replacements and cross-arm failures, assuming other programs continue unchanged.

7. Monitoring & review

Once the investment portfolio is agreed, there is an ongoing need to monitor and review its continuing appropriateness. Requirements for this process step are to:

1. Monitor the risk environment/context for any changes
2. Identify emerging risks
3. Ensure risk management approaches (tools and techniques) are working/still adequate
4. Ensure risk controls are still effective and efficient and keep the organisation's risk profile within acceptable tolerances.

8. Communication & consultation

Communication and consultation with stakeholders should take place during all stages of the process. It is advisable to plan up front who needs to be involved and informed and when. A variety of perspectives is required to prevent 'group think' and add depth and better understanding to appreciation and treatment of risk. For communication to be effective, it should facilitate truthful, relevant, accurate, understandable exchanges of information.

9. Documentation

It is important to be able to evidence the risk assessment that underpins asset investment decisions. As such, it is expected that the types of analysis described in this document will form the basis for individual Investment Cases.

Key supporting information that should be captured includes:

- People who were involved in the risk assessment, ensuring that this is suitable to the scope
- Underpinning information and data sources
- Key assumptions, limitations, uncertainties and sensitivities

10. Additional Guidance

The appendices to this document provide additional guidance to support asset risk management as follows:

- Appendix A – Corporate Consequence Assessment Table
- Appendix B – Statistical Certainty
- Appendix C – Estimating Future Probability of Failure
- Appendix D – Approach When Zero Events Have Been Observed
- Appendix E – Common Assumptions For Use in Asset Risk Analysis
- Appendix F – Useful References
- Appendix G – Glossary of Terms

Appendix A – Corporate Risk Criteria

Figure 15 – Corporate Risk Criteria

LIKELIHOOD	CONSEQUENCE: Insignificant	Minor	Moderate	Major	Severe
Almost Certain	Medium	Medium	High	Extreme	Extreme
Likely	Low	Medium	High	High	Extreme
Possible	Low	Medium	Medium	High	High
Unlikely	Low	Low	Medium	Medium	High
Rare	Low	Low	Low	Medium	Medium

Likelihood Assessment Table

	Almost Certain	Likely	Possible	Unlikely	Rare
Likelihood Criteria	Likelihood of event occurring - more than 5 times a year	Likelihood of event occurring - more than once a year but no more than 5 times a year	Likelihood of event occurring - more than once in 10 years but no more than once a year	Likelihood of event occurring - more than once in 25 years but no more than once in 10 years	Likelihood of event occurring - less than once every 25 years

Consequence Assessment Table

	Insignificant	Minor	Moderate	Major	Severe
Safety	Low level injury/symptoms requiring first aid only	Non-permanent injuries/work related illnesses requiring medical treatment	Significant non-permanent injuries/ work related illnesses requiring emergency surgery or hospitalisation for more than 7 days	Permanent injuries/ work related illnesses to one or more persons	One or more fatalities Significant permanent injuries/ work related illnesses to one or more persons
Network	**Corporate SAIDI: Note (1)** < 0.25 minute **Outage Duration to a small group of customers: Note 2** < 4 hours **Outage to 1 or more Sensitive Load Customers: Note (3)** Any event where the community/ economic impact to the customers is considered to be insignificant	**Corporate SAIDI: Note (1)** 0.25 minute to 1 minute **Outage Duration to a small group of customers: Note 2** 4 to 12 hours **Outage to 1 or more Sensitive Load Customers: Note (3)** Any event where the community/ economic impact to the customers is considered to be minor	**Corporate SAIDI: Note (1)** < 1 minute to SAIDI exclusion threshold **Outage Duration to a small group of customers: Note 2** 12 hours to 36 hours **Outage to 1 or more Sensitive Load Customers: Note (3)** Any event where the community/ economic impact to the customers is considered to be moderate	**Corporate SAIDI: Note (1)** SAIDI exclusion threshold to 20 minutes **Outage Duration to a small group of customers: Note 2** 36 hours to 1 week **Outage to 1 or more Sensitive Load Customers: Note (3)** Any event where the community/ economic impact to the customers is considered to be major	**Corporate SAIDI: Note (1)** >20 minutes **Outage Duration to a small group of customers: Note 2** > 1 week **Outage to 1 or more Sensitive Load Customers: Note (3)** Any event where the community/ economic impact to the customers is considered to be severe
	Not (1) A measure of the impact of the event on the overall System Average Interruption Duration Index (SAIDI) performance calculated using the organisation's total connected customers as the base. Note (2) A small group of customers is generally considered to be less than 100 non-sensitive load customers. Note (3) Sensitive load customers are customers whose supply is substantively Network reliant and where an interruption to their Network supply has the potential to cause widespread community or economic impact				
Finance	<= $250k	= $250K - $5M	= $5M - $25M	= $25M - $50M	> $50M
Compliance	Indication of interest from Regulator No fines incurred but administration costs may be payable No litigation	Warning/ notifications from Regulator Minor financial penalties Short term duration litigation	Medium financial penalties Medium duration litigation	High financial penalties Lengthy litigation	Significant financial penalties Potential jail term for individuals Extensive litigation Loss of Operational Licence

Consequence Assessment Table

	Insignificant	Minor	Moderate	Major	Severe
Customer	Grade of service >75% (GOS = % of calls answered within 30 secs – Emergency Line) Minor increase in call wait time (General Enquiries) Service Other completion > 90%	Grade of service 75%-50% Call wait time 10 to 30 minutes Service Other completion 75%-89%	Grade of service 49%-34% Call wait time 31 to 60 minutes Service Other completion 60%-74%	Grade of service < 35% Call wait time > 60 minutes Service Other completion 50%-59%	No communication channels available Service Other completion < 50%
Reputation	Public concern restricted to local complaints or intra-industry knowledge / awareness	Attention from media and or heightened concern from local community / external stakeholders Criticism from multiple sources for one or two days	Adverse national media/public/stakeholders attention sustained over 1-2 weeks	Significant adverse national media/public/stakeholders attention sustained over 1-2 weeks Loss of confidence by State government minister Directive to amend practice received from regulators	Significant adverse national media/public/stakeholders outcry Sufficient outcry to cause irreparable damage to brand Ministerial enquiry / Royal Commission
Environment	Limited localised damage to minimal area of low significance	Minor impact on biological or physical environment or heritage item over a limited area Little or no need for remediation	Moderate damage over a large area or affecting ecosystem, or heritage item Moderate remediation is required	Serious widespread, long term damage to ecosystem or heritage item Significant rectification is required	Very serious long term, wide spread impairment of ecosystem or heritage item

Appendix B – Statistical Certainty

Making investment prioritisation decisions does not require detailed knowledge of the exact history and condition of every asset. Sampling the data that is readily available is often sufficient, if a statistically significant number of samples are made. When determining if a sample size is statistically significant, consideration should be given to the population and the confidence level, standard deviation, and margin of error required.

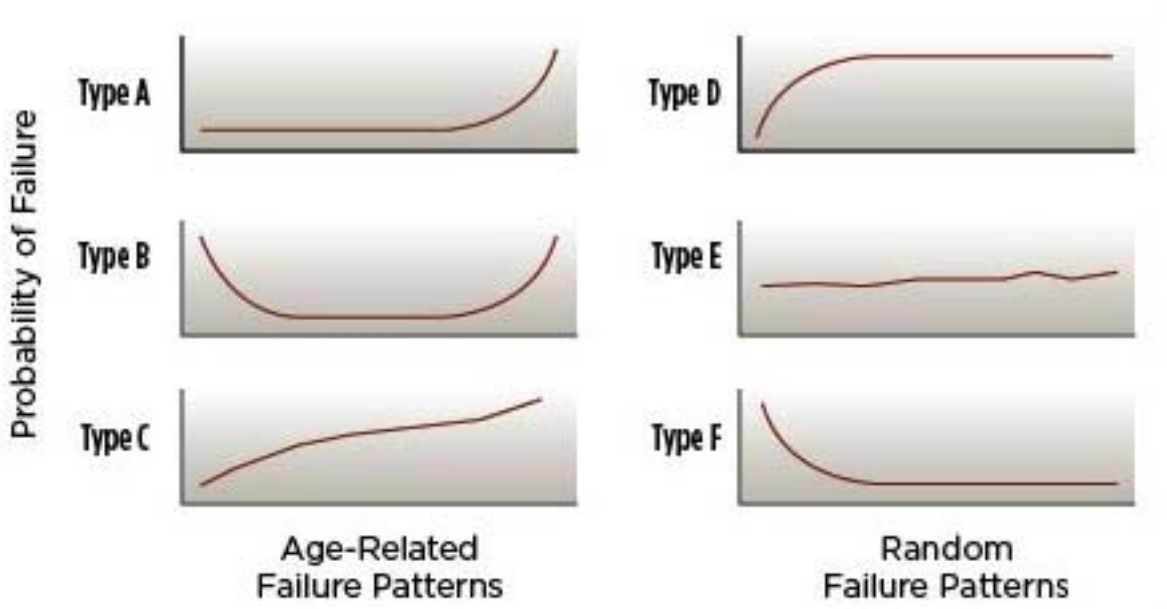
While larger sample sizes generally lead to increased precision when estimating unknown parameters, in some situations, the increase in precision for larger sample sizes is minimal. For example, if we wish to estimate the number of assets with a manufacturing defect, a more precise estimate would be obtained by examining 200 rather than 100 assets. However, if there are only 200 total assets in the population, and 50% of random samples have shown a manufacturing defect, then for most purposes it is reasonable to use the 100 samples. Sample sizes should be judged based on the quality of the resulting estimates.

Appendix C – Estimating Future Probability of Failure

Where future probability of failure is required it is important to understand the likely curve of failure probability for the asset in question. This can be best estimated using a curve which relates probability of failure to age or condition. Figure 16 sets out the generic asset failure patterns to be considered when estimating the probability of asset failure.

- Type A is an accelerated wear-out curve.
- Type B is a bathtub curve, typical of multiple failure modes. It can be calculated as the sum of a Type A and Type F curve.
- Type C is a constant wear-out curve.
- Type D is a random failure curve with a low infant mortality
- Type E is a random failure curve
- Type F is an accelerated wear-in curve with high infant mortality

Figure 16 – Asset failure patterns[12]



[12] http://www.plantservices.com/articles/2011/09-asset-manager-understanding-asset-failure/

Appendix D – Approach when zero events have been observed

In some circumstances, while there is a fundamental understanding that a consequence is possible to occur given some event, there are no records of the consequence occurring.

This may be the case due to:

1. Events have occurred; however, records of consequence were never made, or the records have been lost

   In this case, subject matter experts should provide advice on how often the consequences have occurred. The results of FMECA analysis may be useful in this situation.

2. Events have occurred; however, the consequence has not been observed and records would have been kept if it was observed

   This often occurs for very low probability events such as a fatality. In this case, the 'rule of threes' should be used to estimate an upper bound of probability of the consequence occurring.

3. No events have occurred, and records would have been kept if it was observed

   This may occur for small asset populations. In this case, the 'rule of threes' should be used to estimate an upper bound of probability of the event occurring. The probability of the consequence occurring should be developed using the methodology in (4).

4. No records of event or consequence exist

   Industry experience (such as technical papers, industry working groups or FMECA analysis) should be leveraged to estimate the likelihood of both the event and consequence occurring.

The Rule of Three[13]

Hazards often present high-consequence, low-probability events which have never occurred. In circumstances where these consequences have never occurred, we often seek an upper-bound estimate given only this lack of evidence.

When no events have been observed in N statistically significant observations, there is 95% confidence that the probability p of an event occurring is:

$$0 \leq p \lesssim \frac{3}{N}$$

Suppose we had 10 years of running a fleet of 469 transformers, we have had 57 failures, but there has never been a safety incident relating to transformer failures.

$$57\ faults\ in\ 469 \times 10 = 4{,}690\ asset\ years$$

$$0\ safety\ incidents\ in\ 57\ failures$$

Then, with a 95% confidence interval, the probability of a safety incident if a fault occurs lies within the bounds:

$$0 \leq p_{safety\ incident\ |\ failure} \lesssim \frac{3}{57}$$

Knowing the likelihood of failure in a single asset-year is

$$p_{failure} = \frac{observed\ failures}{observation\ asset-years} = \frac{57}{4{,}690} = 0.012$$

We can therefore determine the upper bound of the probability of a safety incident in a single asset-year

$$p_{safety\ incident} = p_{failure} \times p_{safety\ incident\ |\ failure} = 0.012 \times \frac{3}{57} = 6.3 \times 10^{-4}$$

[13] *Evidence-Based Diagnosis,* Thomas B. Newman, Michael A. Kohn

Assuming the probability of a safety incident is consistent across the sample set (for example, that age or a change in applied controls is not a factor) then sensitivity analysis can be performed on each component of the event tree to determine if the estimation falls within the upper limit bounds.

Appendix E – Common Assumptions For Use in Asset Risk Analysis

A foundation of qualitative risk assessment is the use of consistent models. Many model inputs have a significant metric of uncertainty associated with them. For this reason, assumptions about the value of notable model inputs have been documented in Table 5 – Consistent assumptions below.

Table 5 – Consistent assumptions

Assumption	Value	Basis
Average walking speed	1.4 m/s	Preferred walking speed of normal-weight adults[14]
Hours of exposure per day	14 hrs	6 am – 8pm
Average people entering exposure radius (urban)	2 pp / hr	Equivalent to 112 pp / sqkm spending 2 hrs outside / day
Average people entering exposure radius (rural)	0.1 pp / hr	Equivalent to 2 pp / sqkm spending 5.5 hrs outside / day
Outdoor exposure rate within zone substations	5.7%	170 pp spending 60% of time outdoors in 423 sites
Indoor exposure rate within zone substations	2.9%	170 pp spending 30% of time indoors in 423 sites

[14] Browning, R. C., Baker, E. A., Herron, J. A. and Cram, R. (2006). "Effects of obesity and sex on the energetic cost and preferred speed of walking". Journal of Applied Physiology.

Appendix F – Useful References

Internal

Board Policy (Governance) – Governance – CECP0002

Board Policy (Governance) – Compliance – CECP0002.02

Board Policy (Governance Risk Management) - CECP0002.03

Company Procedure (Governance) Risk Management - CEOP0002.21

Annexure A – Board Charter and Board Committee Charters – Board Policy (Governance) – Governance – CECP0002

Health Safety and Environmental Manual Risk Management - CECM1000.02

External

AS / NZS / ISO 31000:2009 – Risk Management – Principles and guidelines

IEC/ISO 31010 Risk Management – Risk Assessment Techniques

ISO Guide 51:2014 Safety Aspects

ISO Guide 73:2009 - Risk Management vocabulary

NSW Treasury Risk Management Toolkit for the NSW Public Sector (TPP12-03)

Electricity supply regulation (Safety and Network Management) 2014

AS 5577-2013 Network Safety Management Systems

AS 7000 Overhead Line Design – Detailed Procedures, 2010

AS/IEC 61508-5 – 2011 Functional safety of electrical / electronic /programmable – electronic safety related systems, Part 5

Work Health and Safety (WHS) Act 2011

Appendix G – Glossary of Terms

Where applicable, definitions are consistent with AS/ NZS / ISO 31000:2009 – Risk Management – Principles and guidelines.

As Low As Reasonably Practicable (ALARP)

Core to this concept is “reasonably practicable”. If it is not reasonably practicable to eliminate a risk, then it should be minimized to as low as reasonably practicable (in accordance with the hierarchy of controls). ALARP is the level of risk that is tolerable and cannot be reduced further without the expenditure of cost, time and/or effort that is disproportionate to the benefit gained or where the solution is impractical to implement.

Bow-Tie Methodology

The Bow-Tie methodology is used to understand the control environment. It provides a graphical means to describe the relationship between hazards, hazardous events (centre), causes (left side) and consequences (right side). Barriers are used to display what measures an organisation has in place to control the risk. Sometimes called a threat-barrier diagram.

Consequence

Outcome of an event affecting objectives. Note that: an event can lead to a range of

consequences; a consequence can be certain or uncertain and can have positive or negative effects on objectives; consequences can be expressed qualitatively or quantitatively; and initial consequences can escalate through knock-on effects[15].

Control

Measures that modify risk. Controls include policies, procedures, processes, devices, practices or other actions which modify risk. These may also be described as “barriers”.

Corporate Risk Management Plan

The Corporate Risk Management Plan details the risks to the achievement of the company’s strategic and operational objectives. This includes the company risk profile, results of the risk assessments, key risk indicators and the treatment action plans.

Document Control

Employees who work with printed copies of document must check the BMS regularly to monitor version control. Documents are considered “uncontrolled if printed”, as indicated in the footer.

Hazardous event

An event which has the potential to cause harm (i.e. loss or damage), typically the point at which the organisation loses control.

Hierarchy of controls

Elimination of a hazard is the most effective control and if this is not reasonably practicable to achieve, implementation of additional controls should be considered based upon their degree of effectiveness. This order is referred to as the hierarchy of controls and comprises elimination, substitution, isolation, engineering controls, administrative controls and finally use of personal protective equipment.

Likelihood

Chance of something happening, whether defined, measured, or determined objectively or subjectively, qualitatively or quantitatively, and described using terms or mathematically (such as probability or a frequency over a given time period)[16].

Operational Risk

A hazardous event linked to day-to-day activities undertaken by the company.

[15] ISO Guide 73:2009 - Risk Management vocabulary

[16] ISO Guide 73:2009 - Risk Management vocabulary

Positive risk culture is evident in a company when employees are aware of the company's activities, operations and objectives; consider the opportunities and what can go wrong; and takes action to harness the opportunities and address the consequences.

Residual risk

The risk remaining after the present level of risk treatment, taking into account the existing controls and their known level of effectiveness.

Review date

The review date displayed in the header of the document is the future date for review of a document. The default period is three years from the date of approval however a review may be mandated at any time where a need is identified due to changes in legislation, organizational changes, restructures, occurrence of an incident or changes in technology or work practice.

Risk

The effect of uncertainty on objectives.

Risk management

Coordinated activities to direct and control the company with regard to risk.

Risk treatment

The development and implementation of measures to modify risk. Risk treatment measures may include:

- avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk;
- taking or increasing risk to pursue an opportunity;
- removing the risk source;
- changing the likelihood;
- changing the consequences;
- sharing the risk with another party or parties (including contracts and risk financing); and
- retaining the risk by informed decision.

Sensitivity Analysis

A technique used to determine the impact on a dependent variable when varying an independent variable within reasonable bounds.

So Far As Is Reasonably Practicable (SFAIRP)

To reduce risk to a level so far as is reasonably practicable involves balancing

reduction in risk against the time, trouble, difficulty, and cost of achieving it. This requires consideration of:

(a) the likelihood of the hazard or risk concerned eventuating

(b) the degree of harm that would result if the hazard or risk eventuated

(c) what the person concerned knows, or ought reasonably to know, about the hazard or risk and any ways of eliminating or reducing the hazard or risk

(d) the availability and suitability of ways to eliminate or reduce the hazard or risk

(e) the cost of eliminating or reducing the hazard or risk.

Uncertainty

The state, even partial, of deficiency of information related to a future event, consequence, or likelihood.