

Division Manual: Network Risk Management

CEOM1141.01

Managing Network Risks



July 2022

Table of Contents

1. Introduction	6
1.1 Purpose of this manual	6
1.2 Purpose of network risk management	7
1.3 The network risk management process	7
1.4 When to use the network risk management process	9
1.5 How to use the network risk management process	9
2. Network Risk Management – Scope, Context and Criteria	12
2.1 Scope of network risk	12
2.2 Sources of network risk	12
2.2.1 Risks to the network	12
2.2.2 Risks from the network	13
2.3 Objectives for network risk management	14
2.3.1 General risk management objective	14
2.3.2 Specific objectives for residual network risk levels	14
2.3.3 Maturity of network risk management approach	15
2.4 External context	15
2.5 Internal context	15
2.6 Risk criteria	16
2.6.1 Significance	16
2.6.2 Risk Tolerability and Acceptance Criteria (Corporate Risk Management Framework)	16
2.6.3 Safety Risk Tolerability and Acceptance Criteria (Individual Risk of Fatality)	17
2.6.4 Safety Risk Tolerability and Acceptance Criteria (Societal Risk)	18
2.6.5 Pursuing Opportunities	19
2.7 Tools and methodologies	19
3. Instigating and Planning a Risk Assessment	20
3.1 Recognising the need	20
3.2 Characterising the decision	21
3.3 Identifying who will lead the risk assessment	23
3.4 Identifying who to involve	24
4. Risk Assessment and Treatment	25
4.1 Establishing the Context	25
4.2 Risk Identification	25
4.2.1 Threat/Hazard/Opportunity Identification	25
4.2.2 Risk Event	26
4.2.3 Cause Identification	26
4.2.4 Impact Identification	26
4.2.5 Understanding the System of Control and Control Environment	27
4.3 Risk Analysis	29
4.3.1 Qualitative risk analysis	31
4.3.2 Semi-quantitative risk analysis	32
4.3.3 Quantitative risk analysis	33

COMMERCIAL-IN-CONFIDENCE

4.3.4	Calibration and validation of risk analysis outputs	43
4.4	Risk Evaluation and Treatment	43
4.4.1	Risk Tolerability and Acceptance	43
4.4.2	Treatment Options	44
4.4.3	Options Analysis	47
4.4.4	Verification, Calibration and Validation	51
4.4.5	Action Planning and Approval	51
4.4.6	Worked Example	52
5.	Recording, Communicating and Reporting	57
5.1	Records	57
5.2	Communication	57
5.3	Reporting	58
6.	Implementation of Risk Controls and Treatments	58
7.	Monitor and Review	58
7.1	Environmental Scanning	59
8.	Specific Requirements for Formal Safety Assessment	60
9.	Key Concepts	61
9.1	Information Sources to Support Network Risk Management	61
9.2	Critical Controls	61
9.3	Consequence Scenarios	62
9.4	Network Fatal Risks and Operational Safety Risks	62
9.5	Units/Measures of Safety Risk	62
9.6	Societal Concern	63
9.7	Risk Monetisation	63
9.8	Dynamic Risk Assessment	64
9.9	SFAIRP and ALARP	64
9.10	Removing or Relaxing Current Risk Controls	65
9.11	Documenting the SFAIRP Demonstration	65
9.12	Taking Account of Uncertainty and Limitations in Available Information	65
9.13	Human and Cultural Factors	66
9.14	Opportunities	66
9.15	Escalators	66
10.	Authorities, Responsibilities and Resources	67
10.1	Authorities and Responsibilities	67
10.2	Resources	68

COMMERCIAL-IN-CONFIDENCE

11. Manual Implementation, Review and Improvement	68
12. Additional Guidance	68
Appendix A – Subjective Probability Estimates	69
Appendix B – Generalised Asset Failure Curves	70
Appendix C – Statistical Confidence and Sample Sizes	71
Appendix D – Approach When Zero Events Have Been Observed	72
Appendix E – Common Assumptions For Use in Quantitative Risk Analysis	73
Appendix F – Useful References	74
Appendix G – Glossary of Terms	75

List of Figures

Figure 1: Relationship to Corporate Risk Management Framework	6
Figure 2: Network Risk Management Process	8
Figure 3: Relationship between network risk artefacts	10
Figure 4: Key terms in network risk management	11
Figure 5: Tolerability and acceptance criteria for individual risk	17
Figure 6: Tolerability criteria as in the NSW Government land use safety planning guide	19
Figure 7: UKOOA risk-based decision framework	22
Figure 8: Responsibilities for undertaking a risk assessment	23
Figure 9: Considerations for who to involve in a risk assessment	24
Figure 10: Example Ishikawa Diagram	26
Figure 11: Bow-Tie Diagram	27
Figure 12: Threat-Barrier Diagram	28
Figure 13: Risk Calculation	29
Figure 14: Expected application of alternative risk analysis methods	30
Figure 15: Risk calculation for qualitative risk analysis	31
Figure 16: Risk calculation for quantitative risk analysis	33
Figure 17: Generalised model of how consequences arise from risk events	38
Figure 18: Event Tree	39
Figure 19: Key steps in risk evaluation and risk treatment	43
Figure 20: Hierarchy of (Safety) Risk Control	45
Figure 21: Lifecycle effectiveness of risk controls	46
Figure 22 Process of Options Analysis	47
Figure 23: UKOOA risk-based decision framework	50
Figure 24: Final checks in UKOOA framework	51
Figure 25: Type B decision in UKOOA framework	53
Figure 26: Asset failure patterns	70

List of Tables

Table 1: Network Risk Objectives	14
Table 2: Techniques for Consideration in Network Risk Management	19
Table 3: Decision Types in UKOOA framework	22
Table 4: Stakeholders to consider in a risk assessment	24
Table 5: Effectiveness Criteria	28
Table 6: Risk Rating	31
Table 7: Converting qualitative likelihood scales to single point estimates	32
Table 8: An example of discrete distribution in crossarm failure	35
Table 9: Suggested consequence differentiators	37
Table 10: Network-level averages for unassisted and assisted asset failures	40
Table 11: Probability and consequence of severe or moderate fires	40

Table 12: Consequence severity levels for network reliability	42
Table 13: Options analysis	55
Table 14: Risk Owner Actions following a Risk Assessment	58
Table 15: Fatalities and Weighted Injuries	63
Table 16: Authorities and Responsibilities	67
Table 17: Subjective probability estimates	69
Table 18: Common assumptions for quantitative risk analysis	73

1. Introduction

1.1 Purpose of this manual

The Network Risk Management Manual (the manual) forms part of the Asset Management System (AMS) and Electricity Network Safety Management System (ENSMS).

The manual explains when and how to complete the network risk management process (shown in Figure 2) which supports the achievement of network asset objectives and effective decision-making.

The network risk management process provides an approach and tools to:

- understand the impacts of risks on objectives and decisions, then
- agree the controls and treatments required to manage them so far as is reasonably practicable (SFAIRP).

SFAIRP is achieved once all reasonably practicable controls and treatments have been implemented.

The manual satisfies Section 2.2.1 in CEOP0002.21 Corporate Risk Management Procedure where each division is expected to develop risk management practices that allow them to understand the risks related to their activities.

Intended users of the manual are facilitators of complex risk assessments (Network Risk Champions), the Network Risk and Performance Team and other risk Subject Matter Experts (SMEs) who are looking to understand the detail of Essential Energy’s approach to managing network risk. A Network Risk Management Guide is available on the [Network Risk Management SharePoint site](#) for general users who need to facilitate a simple risk assessment.

Figure 1 shows the relationship between this document and the Corporate Risk Management Framework.

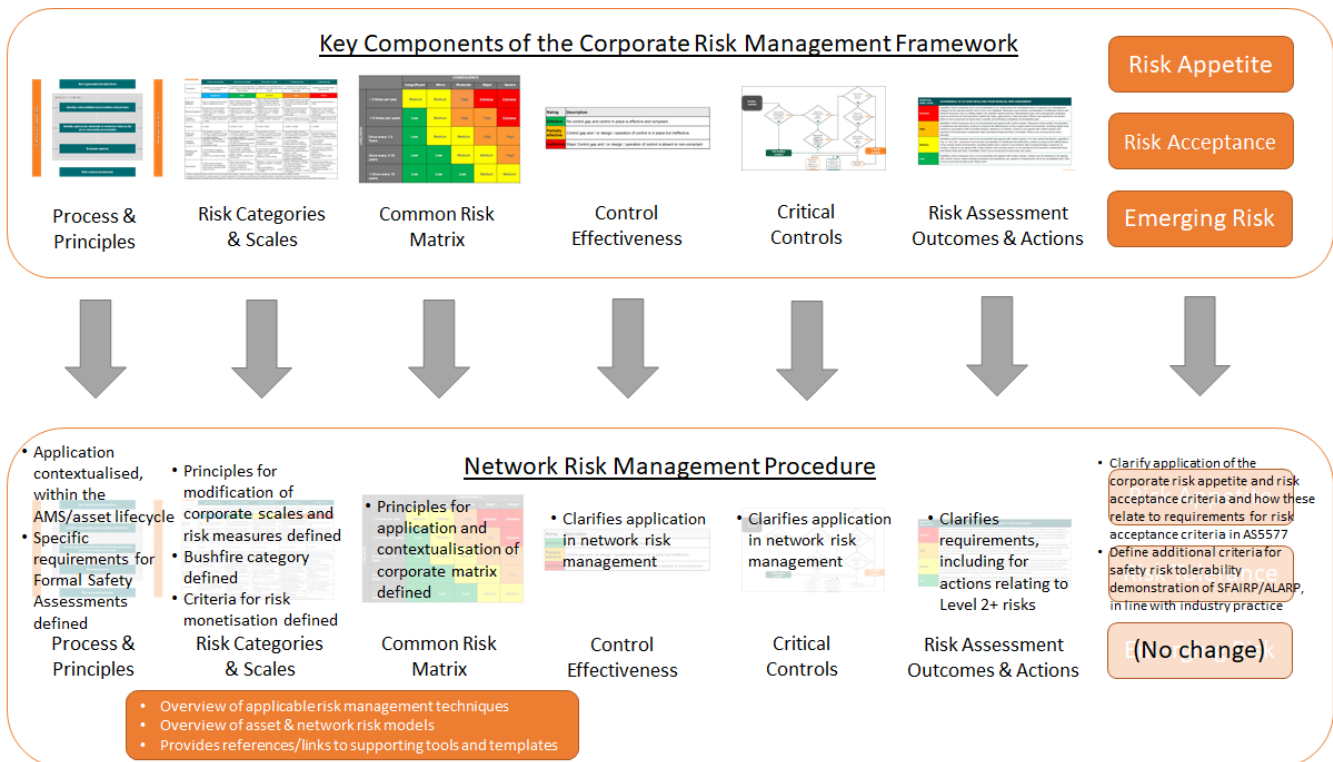


Figure 1: Relationship to Corporate Risk Management Framework

To support the application of the Corporate Risk Management Framework to network risks, the manual includes:

COMMERCIAL-IN-CONFIDENCE

- > Requirements for Formal Safety Assessments (FSAs)
- > Principles for modifying corporate risk scales and contextualisation of the Corporate Risk Matrix
- > Additional bushfire consequence category and scale
- > Criteria for risk monetisation (with reference to the Network Value Framework)
- > Application of corporate control effectiveness ratings
- > Application of the Health, Safety and Environment (HSE) critical control framework
- > Required actions in response to network risks
- > Application of the corporate risk appetite in Asset Management (AM) decision making
- > Specific network risk treatment and acceptance criteria, including for safety

1.2 Purpose of network risk management

The network risk management process helps make informed, transparent decisions that:

- > Maximise the chances of achieving asset management objectives.
- > Avoid/minimise the chances of adverse outcomes occurring on the network.
- > Make the most of opportunities, toward achievement of the asset management objectives.

The network risk management process satisfies legislative, regulatory, shareholder, customer and Board expectations for managing risk in line with good industry practice and standards. Specifically, Essential Energy Board Risk Management¹, Asset Management² and Electrical Safety policies³ establish clear requirements for managing network risk in line with:

- > ISO31000:2018 Risk management – Principles and guidelines, and
- > AS5577-2013 Electricity network safety management systems.

Key principles are that network risk management:

- > **is integrated** into decision making processes
- > **is timely**; risk assessment outputs used to inform decisions
- > **is collaborative**; conducted in and across teams, led by Risk Facilitators and championed by Risk Owners.
- > **involves the people impacted**, including internal and external stakeholder groups such as asset management, engineering, technical/operational SMEs relevant to the subject of the risk assessment, and SMEs in the network risk management process and tools
- > **deals explicitly with limitations and uncertainties** in underlying information, as well as with human, cultural and organisational factors that influence the management of network risk
- > **seeks to continuously improve**, through formal learning activities

The network risk management process does not include coverage of:

- > Project, program, or portfolio delivery risks (see Network Portfolio Delivery Risk and Issues Management)
- > Workplace, work site or task related HSE risks (see HSE Risk Management Procedure CECM1000.02)
- > Fleet, Property, Water or non-network IT risks (see Corporate Risk Management Framework CEOP0002.21).

1.3 The network risk management process

Figure 2 shows the network risk management process, which may involve several iterations of the following steps:

- > **Instigate/Plan the Risk Assessment:** This is a scoping activity which identifies the need for a risk assessment to be undertaken, identifies who will lead the risk assessment and identifies key stakeholders who will need to be involved. This step also defines the methodology and criteria to be used for the risk assessment.

¹ CECP0002.03 Board Policy: Governance: Risk Management

² CECP1004 Corporate Policy: Asset Management

³ CECP8096 Company Policy: Electrical Safety

COMMERCIAL-IN-CONFIDENCE

- > **Risk Identification:** What are the material risks and controls?
- > **Risk Analysis:** How big is/are the residual risk(s)? How effective are the controls?
- > **Risk Evaluation:** Is the residual risk level and control effectiveness identified in the risk analysis step acceptable or do we need to do more (or less) to control the risk(s)?
- > **Risk Treatment:** If the conclusion from the Risk Evaluation step is that we do need to do more (or less), then what does that involve? What will the forecast level of risk and control effectiveness ratings be, because of any changes? Is that acceptable? If yes, plan to implement the changes, including appropriate approvals.
- > **Recording and Reporting:** Document the work that has been done and who was involved; tell the people who need to know about the findings or required actions. This includes the residual risk level, required controls and treatments, plus any key assumptions to ensure the findings remain valid.
- > **Implementing Controls and Treatments:** implement the controls and treatments identified from the risk assessment.
- > **Monitor and Review:** Check to make sure the plans are implemented and working; this step also includes formal review to identify any changes or improvements.

The network risk management process satisfies the AS5577 requirement to produce FSAs, in line with the principles of AS/NZS ISO 31000. Further detail on the specific requirements for FSAs are provided in Section 8.

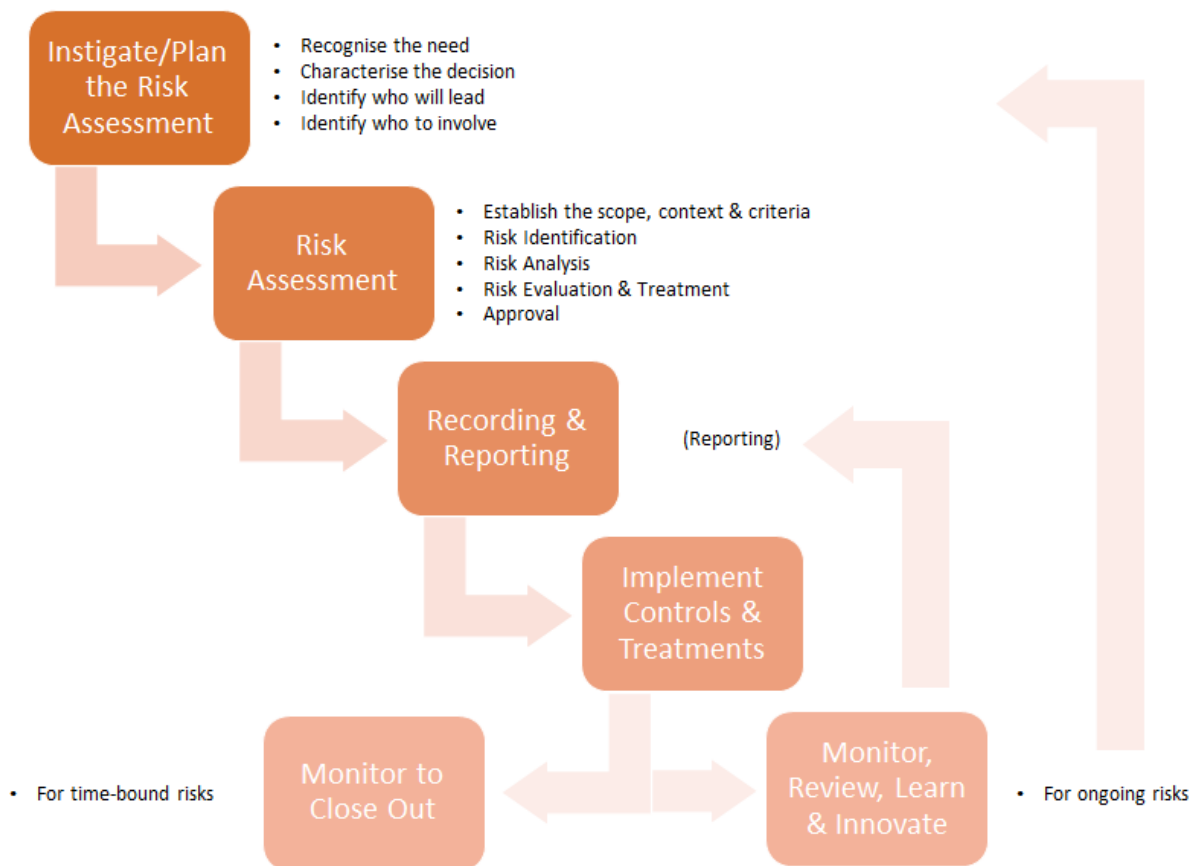


Figure 2: Network Risk Management Process

Typical responsibilities include:

- > Risk Owner is responsible for instigating the risk assessment, conducting an initial categorisation of the risk or decision and identifying and engaging with the appropriate person to lead the risk assessment (the Risk Facilitator).

COMMERCIAL-IN-CONFIDENCE

- > Risk Facilitator should then review the initial categorisation, adjust as appropriate (including checking for any prior, related risk assessments) and confirm if they are the correct person to lead the risk assessment and who else to involve.
- > Risk Facilitator will then **support** the Risk Owner by facilitating completion of the risk assessment. **Risk Facilitators do not own the risk or the risk assessment.**
- > Risk Owner is responsible for endorsing and gaining approval of the risk assessment outcomes.
- > Risk Owner is responsible for escalating and reporting key risk and control information to line management, Function owners (Level 3 managers reporting to the Chief Operating Officer) and the Network Risk and Performance Team.
- > Risk Facilitator ensures an appropriate record of the risk assessment; a central repository of approved risk assessments is then maintained by the Network Risk and Performance Team.
- > Risk Owner is responsible for implementing/monitoring implementation of actions (including controls and treatments) arising from the risk assessment.
- > Risk Owner is responsible for review and improvement, in accordance with agreed review triggers.

Further detail on the responsibilities for facilitating risk assessments is provided in Section 3.3.

1.4 When to use the network risk management process

The network risk management process should be used to understand and manage risks relating to the electricity network. As such, it needs to be considered:

- > As part of asset management planning, governance and assurance cycles
- > At decision points in the asset lifecycle that have a material impact on the residual network risk profile

It is a legal requirement to undertake a risk assessment where the safety impacts are material and reasonably foreseeable. In all other cases, Risk Owners should exercise judgement and discretion to determine when a risk assessment is prudent, using these indicators:

- > A major new undertaking e.g., introducing a new standard/procedure/strategy.
- > A major change e.g., deviating from an existing, approved requirement.
- > A major decision point e.g., planning major network connections, trials and pilots, cease work decisions.

1.5 How to use the network risk management process

As shown in Figure 3, the manual is supported by an extensive suite of guides, tools, templates and training materials which are available on the [Network Risk Management SharePoint site](#).

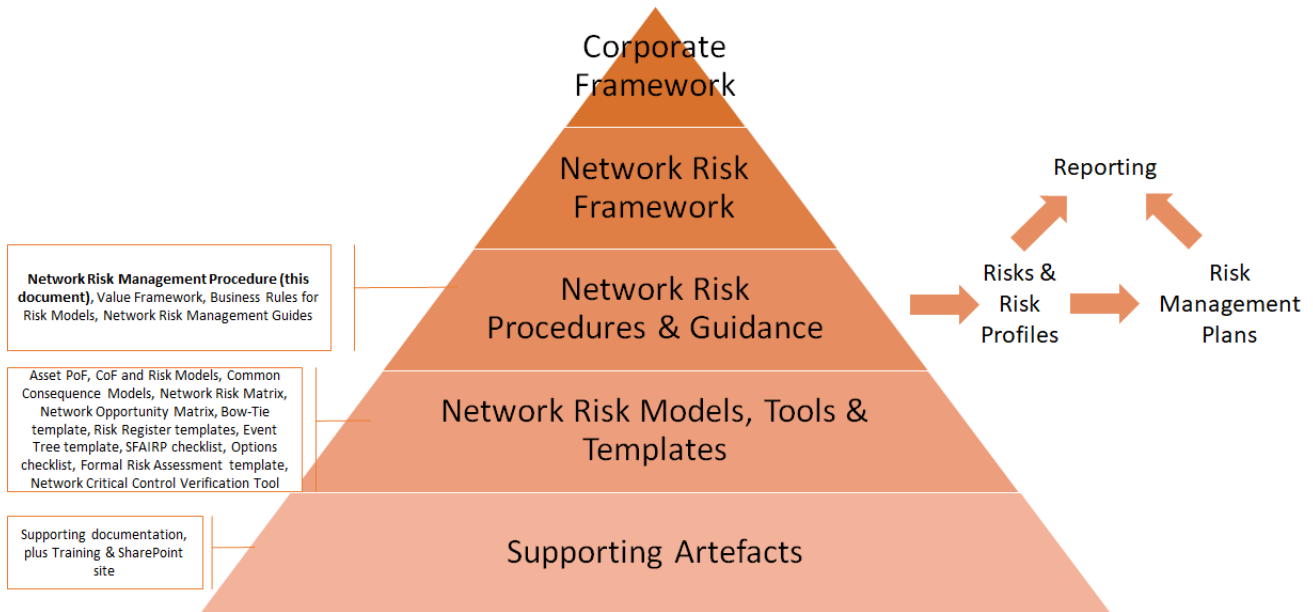


Figure 3: Relationship between network risk artefacts

The remainder of this document is structured as follows:

- > General Scope, Context and Criteria for Network Risk Management (Section 2)
- > Instigating and Planning a Risk Assessment (Section 3)
- > Risk Assessment and Treatment (Section 4)
- > Recording and Reporting (Section 5)
- > Implementation of Risk Controls and Treatments (Section 6)
- > Monitor, Review, Learn and Innovate (Section 7)
- > Specific Requirements for Formal Safety Assessment (Section 8)
- > Key Concepts (Section 9)
- > Roles, Responsibilities and Resources (Section 10)
- > Manual Implementation, Review and Improvement (Section 11)
- > Additional Guidance (Section 12)

Figure 4 explains some key terms used throughout the manual. Further guidance on terms defined in Figure 4 is provided in Section 9; additional guidance is also provided in Appendix G (Glossary of Terms).

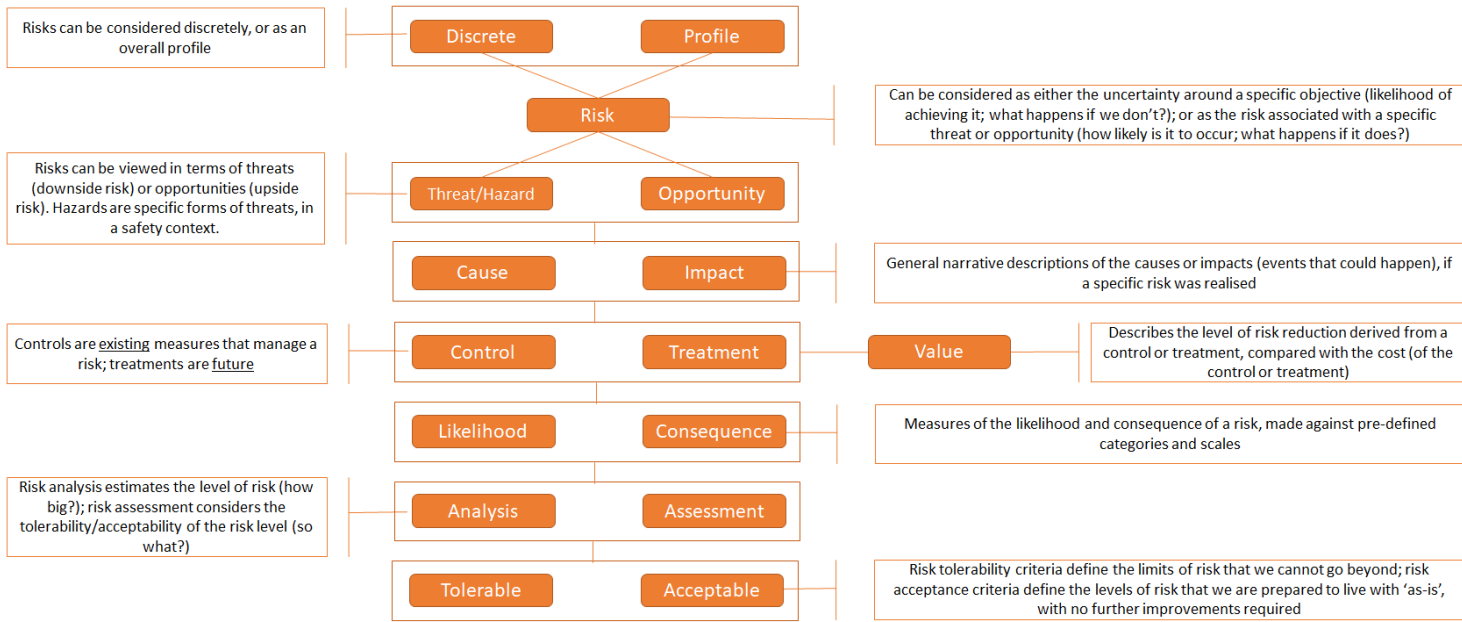


Figure 4: Key terms in network risk management

2. Network Risk Management – Scope, Context and Criteria

This section provides information about the scope, context and criteria for network risk management. For details about the scope, context and criteria for a risk assessment, see Section 4.1.

2.1 Scope of network risk

Network risk can be approached from the perspectives of understanding:

- > uncertainty in achieving an asset management or network performance objective, or
- > the risk associated with a defined hazard or threat, or
- > the risk associated with a defined opportunity.

The scope of network risk includes risks to Essential Energy, customers, shareholders, the broader community and the environment. All these dimensions are affected by actions or inaction, as well as by external factors such as the effects of climate change, changes in government energy policy and changing customer demand.

In line with the corporate risk framework, the main categories of risk considered in the context of the electricity network are:

- > **Safety** – injuries or illness to members of the public, or persons working on or near the network; includes harm resulting from a loss of supply event.
- > **Network** – associated with service interruptions (supply or dispatch), plus service capacity or quality
- > **Bushfire** – associated with network-initiated bushfires⁴
- > **Environment** – associated with environmental harm, including flora and fauna, heritage, amenity and cultural sites
- > **Legal/Compliance** – associated with any breach of legal, regulatory or contractual obligations or commitments; or with any failures to comply with internal policies or procedures
- > **Reputation and Community Standing** – resulting from poor customer or other stakeholder experience
- > **Financial** – including costs and/or loss of income to the public or to Essential Energy e.g., through property damage

Additional risk categories may be considered on a case-by-case basis.

2.2 Sources of network risk

Sources of network risk can be external (risks to the network) as well as those arising from the network itself (risks from the network).

2.2.1 Risks to the network

External sources of risk include:

- > The natural environment (including the weather, flora, fauna)
- > Human beings (through physical and cyber interactions with the network, including intentional and unintentional)
- > Customers and stakeholders (including through their energy/service demands and expectations)
- > Competition (e.g. from suppliers of off-grid solutions)
- > Upstream suppliers (e.g. TransGrid)
- > Downstream suppliers (e.g. suppliers of critical products or services)

⁴ The risks to the network from bushfires caused by external sources are considered through other risk dimensions e.g. safety risks to personnel, safety and reliability risks to customers through loss of services, financial risks due to damage or the loss of Essential Energy assets

COMMERCIAL-IN-CONFIDENCE**2.2.2 Risks from the network**

Network risk can arise from:

- > Individual assets
- > Systems of assets
- > The overall network
- > The actions of persons working on or controlling the network

Each of these layers can be considered to have a 'system of control' applied to it. While an individual asset can be considered in the terms of the asset lifecycle, the network exists at any point in time as a combination of assets and asset systems at different stages in their respective lives. Considering network risk and controls in terms of these different layers is an important part of network risk management, to deliver an overall system of control that is appropriate and aligned with the asset management objectives. This manual applies equally to discrete risks that arise from individual assets, systems of assets and the overall network.

Sources of the various network risks described above include:

- > Decisions taken during network planning and design (including the nature of assets installed on the network and their location)
- > The quality of products and services procured by Essential Energy; the quality of construction delivered by Essential Energy, its contractors or ASPs (contributing to the quality of assets or workmanship and potentially affecting the life of assets and failure modes)
- > The approach to development of the works program (including optimisation and prioritisation rules applied)
- > The approach to delivery of the works program (contributing to the delivery of planned risk controls and treatments, including in line with compliance requirements)
- > Essential Energy's operational and maintenance practices (including works practices, network operation to manage demand, contingency planning for planned and unplanned outages, stakeholder and community communication e.g. to inform customers of planned outages, community education programs)
- > Normal operation of assets (e.g. fire risk associated with the normal operation of drop out fuses or with the residual risk of bare overhead conductor)
- > Unassisted asset failures (resulting from practices to manage the risk associated with deterioration of assets)
- > Assisted asset failures and interference with the network (e.g. overhead conductors down due to being struck by an oversize vehicle)
- > Lack of network capacity (affecting Essential Energy's ability to meet customer demand for new connections or leading to loss of supply or inability to dispatch for generation assets)
- > Decisions taken around growth/new connections (e.g. arising from the connection of photovoltaic systems to the network)

These sources of network risk can of themselves be considered as risks in the context of the AMS. For example⁵:

- > Sub-optimal selection of an asset solution when an alternative may better to manage the stakeholder need
- > Poor specification and request to tender process for assets that are not actually required or that do not adequately address the identified needs
- > Inadequate quality control in design due to inappropriate allocation of design approval or lack of rigorous design reviews and not controlling quality of delivery through effective verification and validation process.
- > Insufficient consideration of longer-term impacts such as reliability and maintainability during acquisition thus causing adverse performance and life cycle cost issues
- > Failure to provide additional system capability to allow for likely growth during design
- > Deficient hazardous material assessments, inadequate or do not address likely changes in community expectations

The process of network risk management defined here is intended to apply to any of these sources.

⁵ Adapted from Asset Management Council's *Asset Management Fundamentals Participants' Workbook* (October 2018)

COMMERCIAL-IN-CONFIDENCE

2.3 Objectives for network risk management

This section sets out specific network risk management objectives which should inform risk assessments and decisions around managing the overall network risk profile.

2.3.1 General risk management objective

The Board Policy for Risk Management (CECP0002.03) sets an overarching risk management objective to **manage risk so far as is reasonably practicable (SFAIRP)**.

2.3.2 Specific objectives for residual network risk levels

Essential Energy has defined several specific risk objectives for a subset of the risk categories listed in Section 2.1. These reflect a mix of statutory and regulatory obligations and proactive business objectives, as shown in Table 1.

Table 1: Network Risk Objectives

Risk Category	Objective	Source	Status
Network Reliability	Maintain risk	Global objective based on customer engagement feedback indicating customers are satisfied with current levels of network reliability; assumes reliability risk is a proxy for reliability performance.	Business objective, based on customer engagement (Best Endeavours)
Safety	Manage safety risk So Far As Is Reasonably Practicable (SFAIRP)	WHS Regulations ⁶ , AS/NZS ISO 45001 and AS5577 ⁷	Minimum legal/regulatory requirement (Mandatory)
	Reduce risk	Essential Energy objective for 'continuous improvements in safety culture and performance'	Proactive business objective (Best Endeavours)
Bushfire	Manage risk SFAIRP	AS/NZS ISO 45001 and AS5577	Minimum legal/regulatory requirement (Mandatory)
	20% reduction in controllable bushfire risk	Essential Energy objective over the period FY21-FY40	Proactive business objective (Best Endeavours)
Environment	Manage risk SFAIRP	AS5577	Minimum legal/regulatory requirement (Mandatory)
	Reduce risk, where it is efficient to do so	Essential Energy objective to 'Reduce the environmental impact of Essential Energy, where it is efficient to do so'	Proactive business objective (Best Endeavours)

⁶ Including for NSW, ACT and QLD jurisdictions

⁷ The specific requirement from WHS legislation is to eliminate risks to health and safety so far as is reasonably practicable (SFAIRP), and if it is not reasonably practicable to do so, to minimise those risks SFAIRP; AS5577 then requires Network Operators to eliminate safety risks SFAIRP, and if it is not reasonably practicable to do so, to reduce those risks to *as low as reasonably practicable* (ALARP). Within this manual, the term 'manage safety risk SFAIRP' is used to reflect all these obligations.

COMMERCIAL-IN-CONFIDENCE

Within Table 1, Mandatory objectives must be met, while objectives with a status of Best Endeavours may be traded off with other performance, cost or risk objectives.

2.3.3 Maturity of network risk management approach

Essential Energy aims to have a 'Systematic' level of maturity in its network risk management approach, which will ensure:

- > an effective and fit purpose approach, that is
- > aligned with stakeholder requirements, industry good practice and the Corporate Risk Management Framework, and
- > embedded into everyday practice through the AMS.

Key indicators of a systematic approach to risk management include:

- > proactive risk management, embedded as a key enabler of performance
- > transparent risk information, including internally and externally, to support enhanced understanding and management of risk; embedded risk reporting including through a suite of effective indicators
- > a fit for purpose suite of risk procedures and tools is established and embedded across critical parts of the AMS
- > formal organisational design for network risk management is agreed and embedded; responsibilities for risk management are communicated and understood; everyone knows what to do, when to do it and how to do it
- > formal arrangements for consultation and collaboration are established and embedded
- > effective governance and assurance arrangements are established and embedded
- > monitor and review cycles are established and embedded

2.4 External context

Key external factors affecting the network risk environment include:

- > **Political** – NSW Electricity Infrastructure Roadmap; Renewable Energy Zones; increasing engagement with local councils
- > **Economic** – continued pressure for reductions in distribution network charges; competition for emerging distribution services
- > **Social** – increased expectations around network resilience and control over personal energy supply; changing consumer behaviour; increasing solar penetration; increasing demand for connections; increasing decentralisation
- > **Technological** – rapidly changing technological landscape including batteries (increasing capacity and reducing cost), hydrogen storage, Standalone Power Systems (SAPS), microgrids, community batteries, smart technology (meters, asset monitoring), electric vehicles; increasing digitisation
- > **Environmental** – climate change; increasing focus on decarbonisation
- > **Legal/Regulatory** – increasing scrutiny from regulators; increasing regulator focus on cybersecurity; increasing complexity as we move towards Distributed Energy Resources (DER) and Distribution System Operator (DSO); National SAPS Framework (AEMO)

A further factor is increasing risk management maturity across other Network Service Providers; continuously raising the standards of what is considered 'industry good practice' in risk management.

2.5 Internal context

Internal factors affecting the current network risk environment include:

- > **Transformation** – resulting in multiple concurrent changes to the current 'system of control'; and the development of new data, models and tools to support network risk management
- > **Aging network** – potentially reducing the effectiveness of historical risk controls under a 'change nothing' scenario

COMMERCIAL-IN-CONFIDENCE

2.6 Risk criteria

This section sets out the criteria used to evaluate the significance, tolerability and acceptance of risk, opportunity and controls on the electricity network. These are derived from relevant industry standards and good practice, as well as from the Corporate Risk Management Framework (as set out in CECF0002.03 and CEOP0002.21).

For ease of reference, these criteria are summarised in the Network Risk Matrix and the Network Opportunity Matrix.

2.6.1 Significance

Risk significance is evaluated using the Network Risk Matrix, which sets out:

- > network risk categories,
- > likelihood and consequence scales,
- > risk ratings,
- > critical risk criteria
- > control effectiveness ratings,
- > critical control criteria, and
- > risk assessment outcomes and actions.

Opportunity significance is evaluated using the Network Opportunity Matrix, which sets out:

- > likelihood and consequence scales,
- > opportunity ratings, and
- > opportunity assessment outcomes and actions.

2.6.2 Risk Tolerability and Acceptance Criteria (Corporate Risk Management Framework)

The Corporate Risk Management Framework does not set a maximum tolerable level of residual risk but requires specific actions based on the combination of residual risk rating and Board risk appetite. This includes a requirement to consider additional, alternative and higher-level controls to improve the effectiveness of the overall control environment:

- > if the residual risk is rated as 'Medium' and the Board's risk appetite is 'Low' or 'Very Low'; or
- > if the residual risk is rated as 'High' or 'Extreme' (regardless of the Board's appetite for the risk).

Risk categories where the Board risk appetite is Low or Very Low are:

- > Safety,
- > Bushfire,
- > Environment,
- > Compliance,
- > Reputation, and
- > People.

Risks are acceptable once they are managed SFAIRP. Within this, controls are considered reasonably practicable when they are:

- > necessary, *and*
- > prudent and efficient, *and*
- > in the long-term interests of the community, *and*
- > aligned with Essential Energy's strategic objectives, *and*
- > achievable within resource constraints.

Risks are also considered to be managed SFAIRP once a formal, resourced treatment plan is in place.

The final point in the list of SFAIRP criteria needs careful consideration. While resources are never limitless, in the short-term the allocation of resources can be changed and in the longer-term resources may be increased, subject to appropriate justification and approvals. The definition of SFAIRP controls should therefore consider both an

COMMERCIAL-IN-CONFIDENCE

unconstrained and a constrained view. The unconstrained view can be thought of as demonstrating an absolute SFAIRP limit – beyond which controls would not be considered because they are demonstrably grossly disproportionate to the risk. The constrained view then demonstrates the best or optimum SFAIRP controls that can be achieved within available resources, **where hard limits on those resources have been tested and can be defended**. It must be noted that affordability cannot be a consideration for determining WHS controls; if we cannot afford to do a work activity safely then we should not be doing it.

2.6.3 Safety Risk Tolerability and Acceptance Criteria (Individual Risk of Fatality)

As well as the criteria defined in the Corporate Risk Management Framework, Essential Energy also implements maximum safety risk tolerability and acceptance criteria as per the framework set out in Figure 5.

Within this framework:

- > Risks in the **Unacceptable** region cannot be justified except 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 to secure some level of benefit and provided the risks are managed SFAIRP (see below)
- > Risks falling within the **Broadly Acceptable** region are generally regarded as insignificant and adequately controlled. Further actions to manage risks falling in this region should be considered, but only be pursued if they are reasonably practicable i.e., accepted good practice and low cost.

Safety risks are managed SFAIRP once the effort required to reduce the risk further, in terms of expense, difficulty, inconvenience, or other conflicting responsibilities is grossly disproportionate to the risk reduction. Further guidance on demonstrating SFAIRP for safety risks is provided in Section 4.4 of this document. Guidance on calculating individual and societal risk of fatality is provided in the [NRM Guide: Individual Risk](#).

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

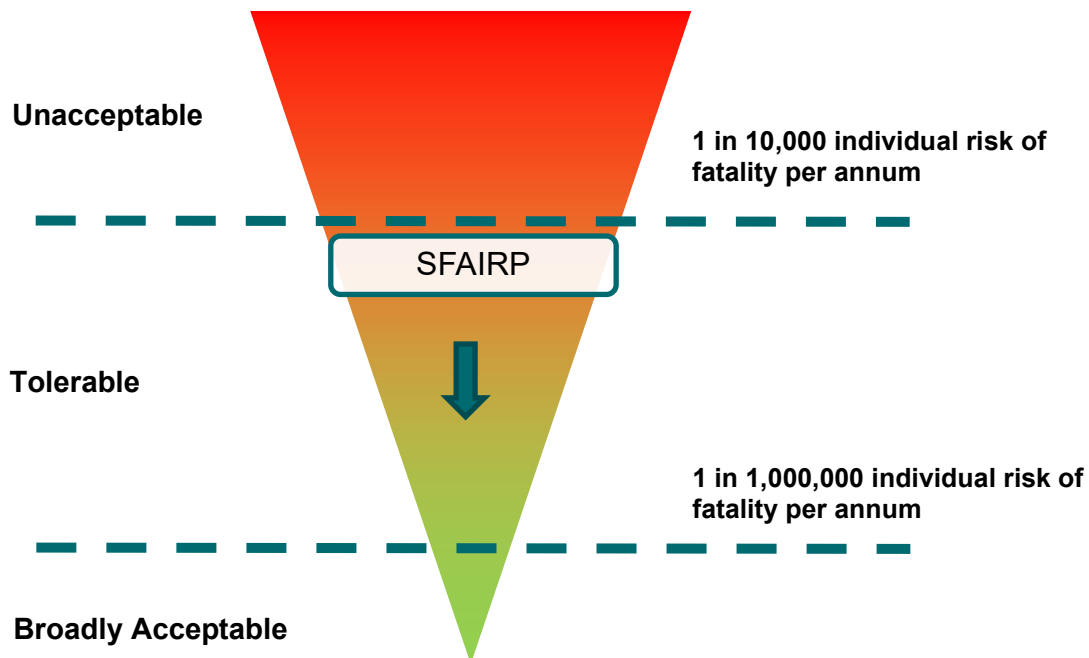


Figure 5: Tolerability and acceptance criteria for individual risk

It is important to note that the maximum tolerable threshold of 1 in 10,000 individual risk of fatality indicated in Figure 2 is an absolute maximum tolerable limit that must not be exceeded anywhere on the network. This limit may be *reduced* in specific circumstances to reflect (i) levels of heightened societal concern/reduced societal tolerability in relation to a specific risk, or (ii) the extent of the risk in question.

COMMERCIAL-IN-CONFIDENCE

To illustrate this second point, if the whole network was at a level of risk that was just below 1 in 10,000 individual risk of fatality per annum, then we could expect to see upwards of 170 fatalities per annum⁸. Society and key stakeholders would not tolerate this level of risk. If the whole network was at a level of risk that was around the 1 in 100,000 individual risk of fatality per annum, then we could expect approximately 17 fatalities per annum⁹. Again, this level of risk is unlikely to be tolerated by society or stakeholders. A network-wide risk level of 1 in 1,000,000 would be expected to result in approximately 1.7 fatalities per annum¹⁰. It is assumed that this level of risk may be tolerated by society and by stakeholders, albeit dependent on the circumstances of the risk events (e.g. assisted versus unassisted) and the effort required to further reduce the risk.

In sum, the practical maximum tolerable risk threshold will likely depend on the extent of the risk (how much of the network is at that level); it may also depend on recent events, e.g. if several recent safety incidents have resulted in a reduced level of tolerance amongst society and/or stakeholders for further safety incidents. This approach is reinforced by NSW Government guidance on 'risk acceptability criteria' for land use safety planning¹¹ which proposes limits of:

- 1 in 1,000,000 risk of fatality per annum for residential areas and places of continuous occupancy (such as hotels and tourist resorts)
- 0.5 in 1,000,000 risk of fatality per annum for hospitals, schools, child-care facilities and old age housing developments
- 5 in 1,000,000 risk of fatality per annum for commercial developments, including offices, retail centres and entertainment centres
- 50 in 1,000,000 for industrial sites (albeit contained within the boundaries of the site, where applicable)

These criteria are included for context and consideration when determining safety risk tolerability limits for use in a specific risk assessment.

2.6.4 Safety Risk Tolerability and Acceptance Criteria (Societal Risk)

If there is a need to consider tolerability and acceptance criteria for societal risk (risk of multi-fatality event), it is suggested that indicative criteria from the NSW Government land use safety planning guide are used. These are derived from the reference listed in Section 2.6.3 and are provided in Figure 6 for reference. The reference to ALARP in Figure 6 should be taken as synonymous with SFAIRP.

⁸ Assuming a risk level of 1 in 10,000 per annum experienced by an estimated population of 1.7 million people exposed to the Essential Energy network

⁹ Assuming a risk level of 1 in 100,000 per annum experienced by an estimated population of 1.7 million people exposed to the Essential Energy network

¹⁰ Assuming a risk level of 1 in 1,000,000 per annum experienced by an estimated population of 1.7 million people exposed to the Essential Energy network

¹¹ NSW Government Planning, Hazardous Industry Planning Advisory Paper No. 4, Risk Criteria for Land Use Safety Planning. Available at: <https://www.planning.nsw.gov.au/-/media/Files/DPE/Other/hazardous-industry-planning-advisory-paper-no-4-risk-criteria-for-land-use-safety-planning-2011-01.pdf?la=en> (accessed June 2021)

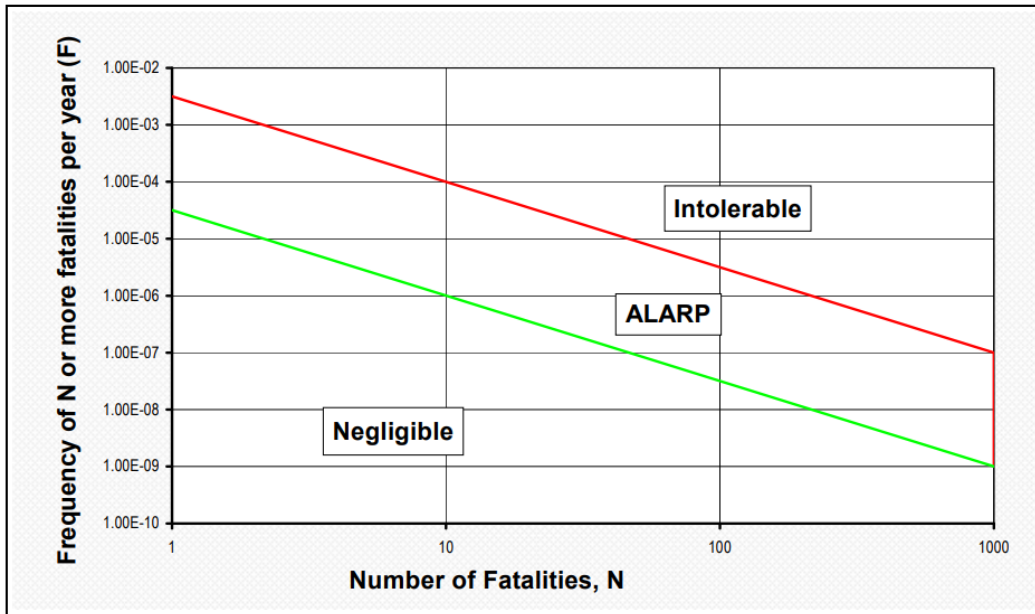


Figure 6: Tolerability criteria as in the NSW Government land use safety planning guide

2.6.5 Pursuing Opportunities

Criteria for pursuing opportunities are defined within the Network Opportunity Matrix.

2.7 Tools and methodologies

Table 2 Other techniques may also be used, as applicable to a specific situation.

Table 2: sets out different techniques that may be relevant for network risk management, mapped against the different stages of the risk management process. Further guidance on each technique is provided in AS/NZS IEC 31000:2020 *Risk management – Risk assessment techniques*. Other techniques may also be used, as applicable to a specific situation.

Table 2: Techniques for Consideration in Network Risk Management

Technique	Risk Assessment Process						Risk Treatment
	Risk / Cause / Impact Identification	Control Environment/ Effectiveness/ Options	Risk Analysis			Risk Evaluation	
			Consequence	Likelihood	Risk		
Brainstorming or SME Workshop	✓	✓	✓	✓	✓	✓	✓
Structured Interviews	✓	✓	✓	✓	✓	✓	✓
Delphi or IDEA Protocol	✓	✓	✓	✓	✓	✓	✓
Checklists	✓	✓	✗	✗	✗	✗	✗
SWOT Analysis	✓	✓	✗	✗	✗	✗	✗
FMEA/FMECA	✓	✓	✓	✓	✓	✓	✓
Scenario Analysis	✓	✓	✓	✓	✓	✓	✗

COMMERCIAL-IN-CONFIDENCE

SWIFT	✓	✓	✓	✓	✓	✓	✗
Ishikawa method	✓	✓	✗	✗	✗	✗	✗
Bow-Tie Analysis/ Threat Barrier Diagram	✓	✓	✓	✓	✓	✗	✗
LOPA	✓	✓	✓	✓	✓	✗	✗
Fault Tree Analysis	✓	✓	✗	✓	✓	✗	✗
Event Tree Analysis	✓	✓	✓	✓	✓	✗	✗
Markov Chain	✓	✓	✓	✓	✗	✗	✗
Monte Carlo Simulation	✗	✗	✓	✓	✓	✗	✗
HEART	✓	✓	✓	✓	✓	✓	✓
Reliability Centred Maintenance	✓	✓	✓	✓	✓	✓	✓
Consequence/ Probability Matrix	✗	✗	✓	✓	✓	✓	✗
Risk Indices	✗	✗	✓	✓	✓	✓	✗
Cost-Benefit analysis	✗	✗	✗	✗	✗	✓	✓
Decision Tree Analysis	✗	✗	✓	✓	✓	✗	✗
Multi-Criteria Decision Analysis	✗	✗	✗	✗	✗	✓	✓
Risk Register	✓	✓	✓	✓	✓	✓	✓

The rationale for the choice of technique should be documented as part of the risk assessment. It is preferable to use more than one technique. Further guidance is provided in Section 4.3.

Toolkit

- [Network Risk Matrix](#)
- [Network Opportunity Matrix](#)
- [Network Risk Management SharePoint Site](#)

3. Instigating and Planning a Risk Assessment

The section describes the process for instigating and planning a risk assessment, including:

- Recognising the need for a risk assessment to be undertaken (Section 3.1)
- Characterising the decision that the risk assessment is required to inform (Section 3.2)
- Identifying who will lead the risk assessment (Section 3.3)
- Identifying who needs to be involved (Section 3.4)

3.1 Recognising the need

Section 1.4 sets out the generic situations when a risk assessment is required; putting these situations into an AM context with some examples includes:

COMMERCIAL-IN-CONFIDENCE

- > a new risk is identified e.g. a previously unseen type fault
- > defined triggers are reached for the review of existing risks e.g. the agreed 2-year review period for an existing risk
- > departing from an existing risk control e.g. reducing the volumes of maintenance in a particular year due to delivery constraints
- > there is a change to an existing control e.g. changing an agreed AM strategy, engineering standard or works practice
- > introducing a new risk control onto the network, including through any pilots or trials e.g. a trial of a new piece of network equipment
- > changes to the risk environment are detected e.g. increase in inherent risk of weather-related events; increase in the inherent public safety risk at a site, due to adjacent housing development
- > a significant incident or failure of a critical control (should trigger a review of any existing risk assessment, or a new risk assessment if the circumstances are outside of the scope of any existing risk assessment)

3.2 Characterising the decision

The primary purpose of risk assessment is to inform decisions on how to manage risks, usually by one of the following strategies:

- > Eliminate/avoid
- > Treat/reduce
- > Transfer/share
- > Accept (live with as-is)

To appropriately 'design' the risk assessment, it is important to characterise the type of decision that needs to be made. This includes the:

- > Inherent level of understanding/uncertainty around the risk
- > Extent of existing, established practice for managing the risk
- > Level of stakeholder interest in the risk or decision
- > Lifecycle or economic implications of the decision
- > Level of any risk trade-offs or transfers, including any perceptions of a reduction in safety standards

These dimensions are captured in the UK Offshore Operators Associated (UKOOA) Risk Decision-Making Framework¹² (see highlighted section of Figure 7). The right-hand side of the framework characterises decisions as Type A, B or C, based on the above dimensions. The central part of the framework then sets out the relative significance of different inputs to the decision-making process. Finally, the left-hand side of the framework sets out various means of calibrating the decision.

¹² Available at: <https://www.icheme.org/media/10257/xv-poster-03.pdf> (accessed August 2021)

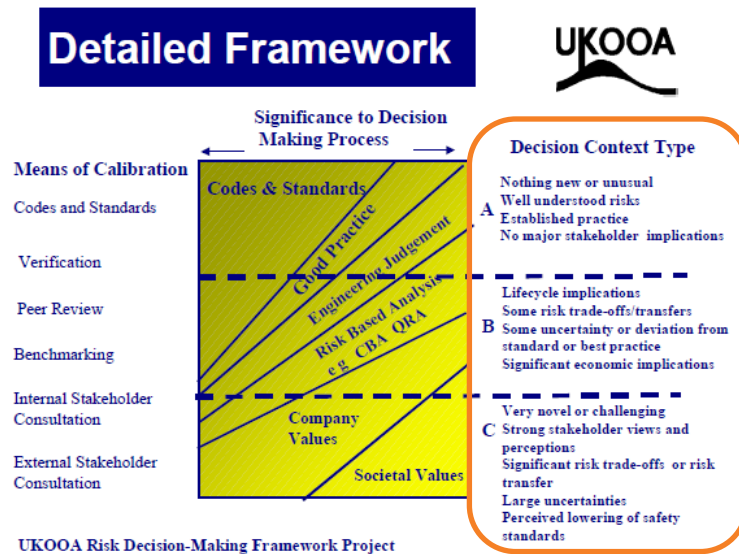


Figure 7: UKOOA risk-based decision framework

Table 3 sets out a range of example decisions, characterised using the UKOOA framework.

Table 3: Decision Types in UKOOA framework

Example	UKOOA Type
Routine planning or design decision falling within existing standards and practices	Type A
Re-prioritise existing works program in line with pre-defined criteria	Type A
Appropriate control environmental around Hydrogen SAPS pilot	Type B
Response to newly identified type fault in equipment with catastrophic (explosive) failure mode	Type B
Change to extend the existing pole inspection cycle	Type B/C
Change from rules-based compliance with ISSC3 to risk-based compliance	Type C
Whether to continue with planned work during Covid-19 outbreak	Type C

COMMERCIAL-IN-CONFIDENCE

Implications for the underpinning risk assessments are that most decisions are Type A or B; there should be very few Type C decisions, specifically:

- > **Type A decisions** will require only a simple qualitative or semi-quantitative risk assessment; most of the decision should be based off demonstrated compliance with relevant codes and standards, application of industry good practice and the reasoned judgement of competent professionals
- > **Type B decisions** will be less able to draw on established codes, standards or industry practice; they will therefore rely more heavily on risk assessment to support the decision, which will likely include some level of quantitative analysis as well as reference to company and societal values
- > **Type C decisions** will be mostly based on risk and value-based evidence; they will likely require multiple risk methods to be applied and may also require the use of more sophisticated scenario and probabilistic analysis techniques.

3.3 Identifying who will lead the risk assessment

The person leading the risk assessment is generally responsible for:

- > Facilitating the risk assessment process
- > Coordinating any supporting risk workshops
- > Ensuring there is an appropriate record of the risk assessment

Figure 8 sets out the responsibilities for undertaking a risk assessment, alongside the UKOOA framework referred to in Section 3.2 above.

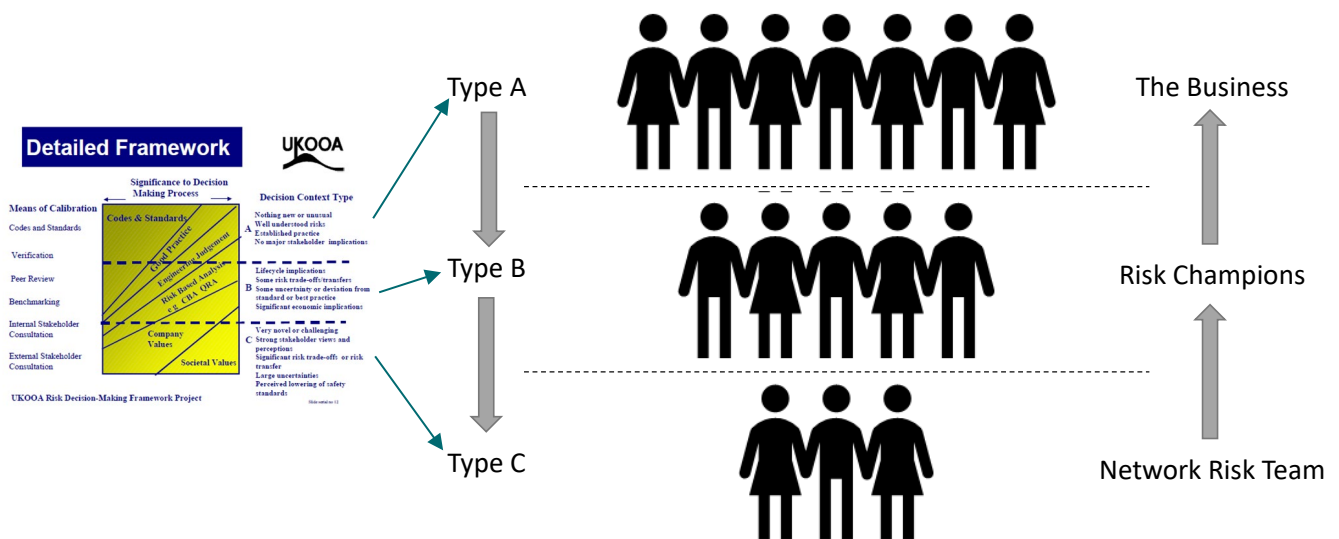


Figure 8: Responsibilities for undertaking a risk assessment

Within this model, risk assessments are generally led by the business, supported by a community of local Risk Champions and by the Network Risk and Performance Team.

Toolkit

- [Training Page on Network Risk Management SharePoint site](#)
- [Contact for Network Risk and Performance team and Risk Champions](#)

COMMERCIAL-IN-CONFIDENCE

3.4 Identifying who to involve

Identifying who best to involve in a risk assessment ensures:

- > A thorough understanding of the context and risks
- > Fit-for-purpose design of controls and treatments
- > Support for the final decision and associated actions

Not all stakeholders need to be involved in every step of the risk assessment; to keep the process efficient it is important that the role of each stakeholder is clear upfront. The main considerations are shown in Figure 9.



Figure 9: Considerations for who to involve in a risk assessment

Table 4 provides a more detailed list of stakeholders to consider.

Table 4: Stakeholders to consider in a risk assessment

Stakeholders who...	Internal Groups to Consider	External Groups to Consider
<ul style="list-style-type: none"> • Understand the internal and external context • Can help identify the risks, causes or impacts • Understand the realities of the current controls and their effectiveness • Can feed into the risk analysis (likelihood and consequence) • Can help to co-design treatment options • Understand the costs, risks and benefits of treatment options • Will need to agree to any ongoing controls or new treatments and to any monitoring requirements • Need to know about the residual risks or the required controls and treatments going forward • Need to know about any key assumptions or limitations affecting the validity of the risk assessment 	<ul style="list-style-type: none"> • Corporate Strategy • Corporate Risk and Insurance • Legal • Regulation • HSE • AM Strategy • Network Planning • Engineering (including ESO) • System Control • Network Delivery • Network Ops • Customer Experience • Operational Excellence • Innovation • Corporate Comms (including Customer Engagement) • eTech • Procurement 	<ul style="list-style-type: none"> • Customer Advisory Group • Industry Groups • Peer DNSPs • Suppliers • Regulators • Government Departments • Community Groups • Emergency Services

It is important to keep accurate records of stakeholders consulted and workshops completed throughout the risk assessment.

Toolkit

- [Stakeholder Consultation and Engagement Form \(CEOF0002.21a\)](#)
- [Network Risk Assessment Phases Template](#)
- [Network Risk Assessment Template](#)

4. Risk Assessment and Treatment

This section describes the process for undertaking a risk assessment and determining treatments, including:

- Establishing the Context (Section 4.1)
- Risk Identification (Section 4.2)
- Risk Analysis (Section 4.3)
- Risk Evaluation and Treatment (Section 4.4)

It also covers requirements for calibration and validation of risk assessment outputs (Section 4.5).

4.1 Establishing the Context

Define the context upfront and revisit it as new information becomes available to help guide the completion of the risk assessment. This should include consideration of:

- Organisational Context – vision, purpose and values of Essential Energy and summary of key operations.
- Purpose – the key objective(s) of the risk assessment.
- Scope – the boundaries of the risk assessment including specific inclusions and exclusions.
- Assumptions and Constraints – any preconditions, or circumstances in which the risk assessment is being undertaken.
- Methodology/Approach – assessment methods (see Section 4.3), evaluation criteria (see Section 4.4) and metrics to measure results (see Section 7).
- Related Risks – review any related risks including Corporate Level 1 risks, risks defined in existing risk registers (link to SharePoint), or Formal Safety Assessments (FSAs).

Toolkit

- [Network Risk Assessment Template](#)
- [Library of Existing Risk Registers](#)

4.2 Risk Identification

Thoroughly understand the risks under consideration including their causes and impacts, the current system of control and the control environment (i.e., the effectiveness and criticality of controls and any human or organisational factors). This includes consideration of internal and external factors for the above.

This is one of the most important steps in the overall risk management process as risks cannot be managed if they have not been identified.

Ways of identifying network risks include through reviewing existing Essential Energy and industry data, plus structured workshops or interviews with SMEs. Specific techniques are listed in Table 2, with further guidance provided in AS/NZS IEC 31000:2020 *Risk management – Risk assessment techniques*.

Note that AS5577 requires consideration of all reasonably foreseeable consequences as well as those that have occurred in previous known events. The remainder of this section sets out specific requirements and guidance on the various aspects of risk identification.

4.2.1 Threat/Hazard/Opportunity Identification

Specific threats, hazards and opportunities can be identified from:

- > historical data and knowledge, including from Essential Energy and broader domestic and international industry experience, or from
- > brainstorming and other structured 'what if' techniques, such as Structured What If Technique (SWIFT).

COMMERCIAL-IN-CONFIDENCE

The choice of technique should be guided by the quality and/or availability of data and knowledge relevant to the specific risk assessment.

A key aim and challenge for this step is completeness. If a particular risk assessment requires high levels of confidence that all material threats, hazards or opportunities have been identified then it will be appropriate to use multiple techniques.

4.2.2 Risk Event

Risk events are specific occurrences that form the basis for the risk assessment. They are typically described in terms of the impact to an objective and/or the source of the risk. For example, the 'risk of':

- > Network-initiated bushfire
- > Insufficient distribution supply capacity (at a specific location)
- > Harm or loss to a member of the public due to network encroachment (excluding vegetation)
- > Unassisted failure of a wood pole
- > Life-support customer de-energised without appropriate notification
- > Inability to respond to a black start event
- > Cyber security breach within the control domain

A range of scenarios can be used to model how changes in the size and nature of the source may alter the risk. This is a particularly useful technique when modelling the risk implications of a change in business practice.

4.2.3 Cause Identification

Causes are factors that could lead to a risk event arising. Each risk event will typically have several causes. Root causes can be 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. Examples include Ishikawa (or 'fishbone') diagrams or 5 Whys.

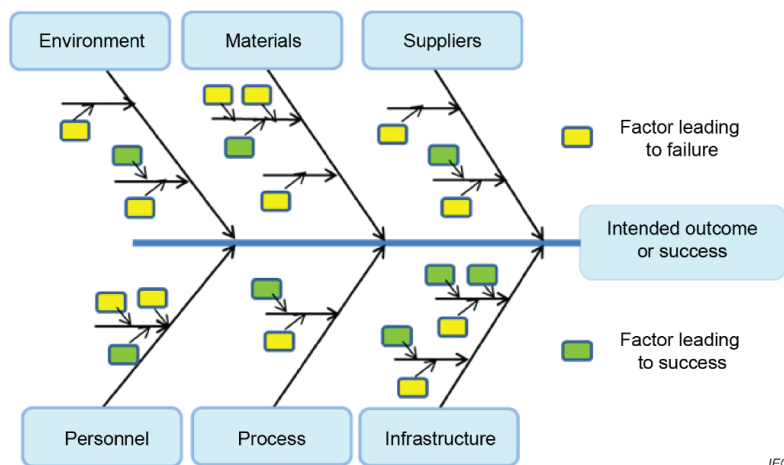


Figure 10: Example Ishikawa Diagram¹³

While considering each cause, consider the circumstances which could lead to its occurrence and what could prevent it. In some cases, causes need to occur in a particular order or in combination for a risk event to arise. At times, the cause may not be evident or may be due to 'normal deviation'. The significance of the cause in relation to the risk event should also be considered.

4.2.4 Impact Identification

Impacts are the outcomes of a realised risk event. They are typically described in a qualitative statement, that can then be used to guide consequence analysis through the Network Risk Matrix and Value Framework.

¹³ Sourced from ISO 31010

COMMERCIAL-IN-CONFIDENCE

It is important to identify the areas of impact associated with a risk event, including consequences to the network workforce, the public, the environment and other stakeholders. This should include consideration of consequences that are reasonably foreseeable as well as those that have occurred in previous known events.

The risk assessment should also consider the potential for cascading and cumulative impacts and consequences.

To avoid double counting, it is important to indicate how specific consequences are apportioned across the relevant areas of impact for each risk event. Structured methods such as event trees, risk maps or logic diagrams may help with this.

If impact identification identifies a consequence type that is not addressed by the Network Risk Matrix or Value Framework, contact the Network Risk and Performance Team for advice on how to proceed.

4.2.5 Understanding the System of Control and Control Environment

An important part of the ‘Identification’ stage is to understand the:

- > current control environment (for existing risks), or
- > minimum control environment required by relevant standards or compliance obligations (for new risks).

The effectiveness of these controls in managing the risk should also be identified, along with any material escalators that affect the inherent likelihood or consequences of a risk event.

Two key methods for understanding the current system of control and control environment are:

- > Bow-Tie Diagrams
- > Threat Barrier Diagrams

Figure 11 shows an example of a Bow-Tie diagram which is best used in situations where there is a single risk event with no indirect consequences.

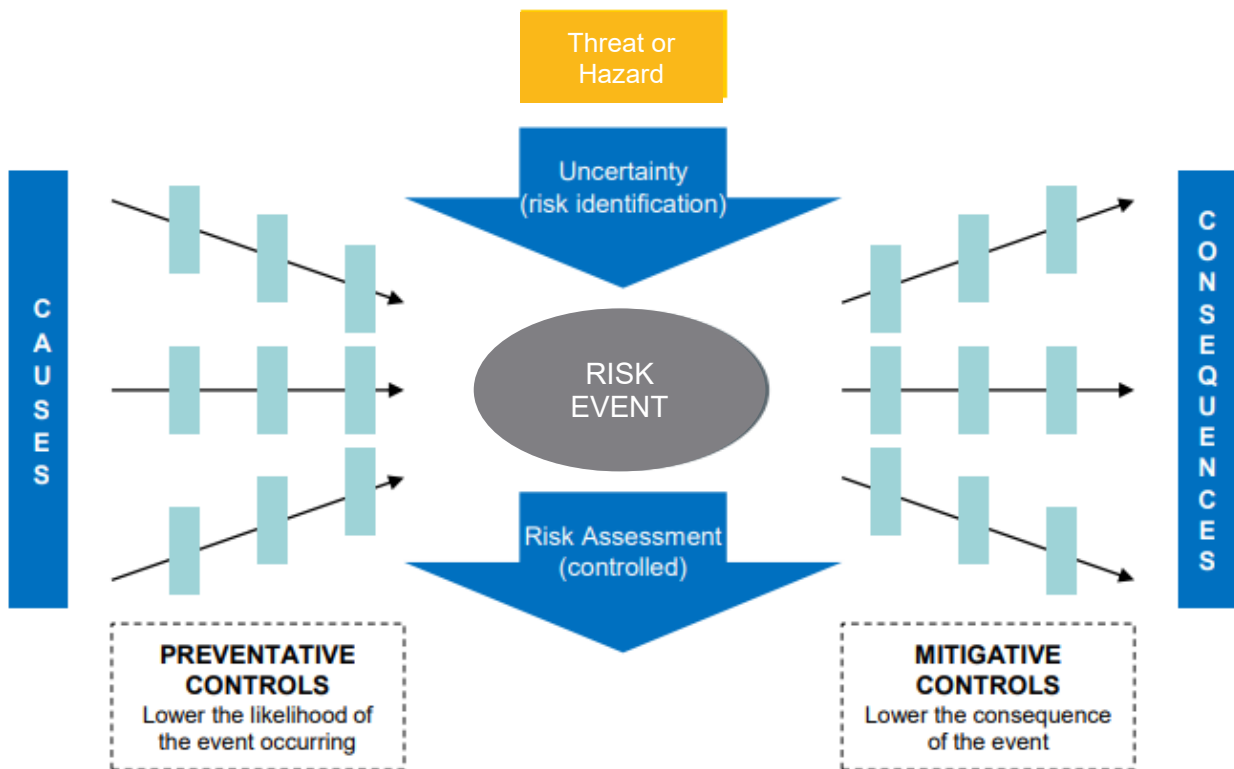


Figure 11: Bow-Tie Diagram

Figure 12 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

COMMERCIAL-IN-CONFIDENCE

consequences. Importantly this includes 3rd party actions and flow-on (downstream) consequences, which can help build the understanding of the extent to which Essential Energy can influence the nature and magnitude of the full range of outcomes or consequences of an incident.

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

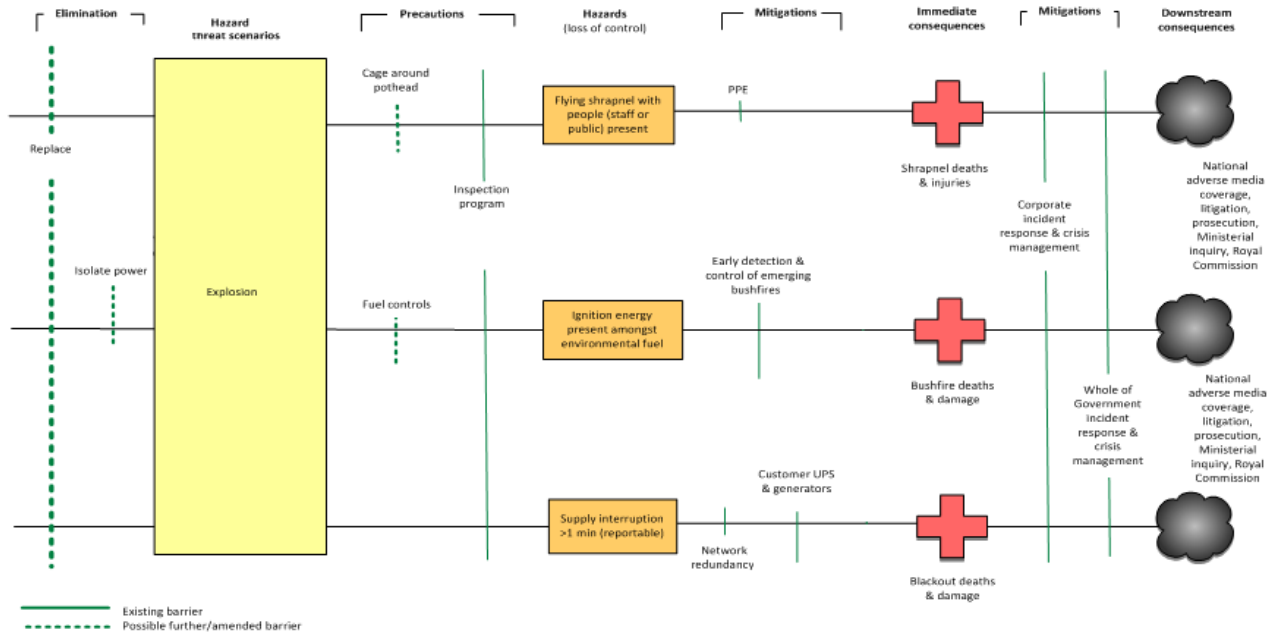


Figure 12: Threat-Barrier Diagram

The effectiveness of controls should be evaluated in accordance with Table 5. Note that the effectiveness rating is the **net** position from the design and implementation/operation of a control, considering the impacts of human and organisational factors.

Table 5: Effectiveness Criteria

Rating	Description
Effective	No control gap and control in place is effective and compliant.
Partially effective	Control gap and / or design / operation of control is in place but ineffective.
Ineffective	Major Control gap and / or design / operation of control is absent or non-compliant

Depending on the context and granularity of a risk assessment, control ratings may be applied to individual controls or to an overall system of control. Risk assessments may also identify risk escalation factors that lead to increased or decreased levels of underlying (inherent) risk, or to enhanced or reduced effectiveness of controls. Identification of 'critical controls' enables prioritisation of management activity, see Section 9.2 for further detail.

Toolkit

- [IEC31010:2019 Risk Management - Risk Assessment Techniques](#)
- [Library of Existing Bow-Ties](#)
- [Library of Existing Risk Registers](#)
- [Bow-Tie Template](#)
- [Corporate Threat-Barrier Example \(CEOF0002.21b\)](#)
- [Network Risk Matrix](#)

4.3 Risk Analysis

The purpose of risk analysis is to calculate the level of risk. Analysis can be qualitative, semi-quantitative or quantitative. It can also be probabilistic. Whichever method is chosen, risk is fundamentally analysed as the product of the likelihood and consequences of a risk event. Figure 13 shows the risk calculation:



Figure 13: Risk Calculation

A key aspect of risk analysis is to understand the type of the risk being analysed and specifically whether it is:

- > **Inherent** – with no controls in place – may go up and down dependent on the status of specific escalators e.g. due to particularly good or bad fire season conditions
- > **Residual** – with current/standard controls in place (e.g. minimum required by standards/current practice)
- > **Forecast** – with any alternative or additional risk treatments in place

Typically, inherent network risks are not assessed and are included for background understanding only.

The first step in any risk analysis is choosing an appropriate technique(s). Detailed guidance on the selecting specific techniques can be found in [IEC31010 – Annex A](#). Considerations include:

> **Requirements:**

- Levels of granularity or accuracy needed to underpin the decision(s) to be taken from the outputs of the risk analysis
- Final audience for the outputs of the risk analysis, and whether numerical and/or more visual methods (e.g. bow-ties or event trees) would be more effective ways to communicate
- Extent to which the analysis needs to explicitly consider human factors, including heuristics and biases and behavioural factors

> **Constraints:**

- Levels of organisational capability, including through its people and/or any specialist IT tools or software
- Availability of data to support the chosen method
- Time available to undertake the risk analysis

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

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

Figure 14 shows broad guidance on the relationship between methods used, and the level of risk.

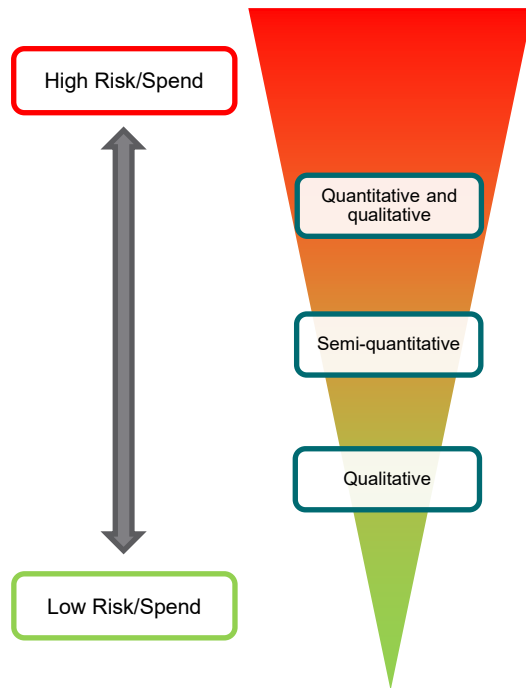


Figure 14: Expected application of alternative risk analysis methods

In situations where there is high uncertainty or complexity, high levels of societal concern or stakeholder scrutiny, multiple techniques should be considered. Where multiple methods are used, it may be useful to apply fewer complex methods in the first instance, to inform those parts of the risk assessment where more sophisticated methods will add value.

Potential risk analysis techniques are listed in Table 2, with further supporting explanation provided in ISO31010 and IEC31010. The basis for the choice of technique should always be recorded as part of the risk assessment.

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 remainder of this section sets out minimum requirements and guidance for undertaking qualitative, semi-quantitative and quantitative risk analysis.

Regardless of the method chosen, risk analysis should consider factors affecting the background level of inherent risk¹⁴ and factors impacting the effectiveness of controls at a specific time or within the scope of a specific risk assessment, including:

- > any variability in time, or dependent on escalators e.g. likelihood of a fire start on a total fire ban day as opposed to during fire season more generally or outside of fire season; likelihood of fire starts during a 'good' fire season versus a 'bad' one. The same concepts also apply for storm-initiated risks.
- > the effects of any permanent or variable/temporary controls e.g. the presence of network redundancy, status of variable protection settings
- > the operation or contribution of external controls e.g. the public response to fires or other safety hazards, emergency service availability and response. The risk analysis should make all reasonable efforts to ensure realistic assumptions about the range of possible likelihood and consequences factors, including factors that are inside and outside of Essential Energy's direct control.

AS5577 also requires that (as a minimum) any FSAs consider the potential for single and multiple failure modes, as well as cascading failures or 'knock-on' effects, as appropriate.

A library of templates, standard assumptions/parameter values and models is available via the Policy Library and the [Network Risk Management SharePoint site](#). As a minimum, these should be reviewed for relevance and to

¹⁴ Further explanation of the concept of inherent risk is provided in Section 9

COMMERCIAL-IN-CONFIDENCE

ensure a consistent approach. Any gaps identified through this review process should be identified to the Network Risk and Performance Team.

4.3.1 Qualitative risk analysis

The primary resource used to undertake qualitative risk analysis is the Network Risk Matrix.

Figure 15 shows the practical application of the generalised risk formula shown in Figure 13, when used for qualitative risk analysis. This combines the 'Likelihood of Risk Event' and 'Likelihood of Consequences' ratings into a single 'Likelihood' rating.



Figure 15: Risk calculation for qualitative risk analysis

Often a risk event will have multiple consequence types associated with it e.g. pole failure may result in safety, reliability, bushfire, environment, financial, compliance, and/or reputation consequences. The risk analysis only needs to consider material consequence categories, relevant to the specific risk assessment.

Qualitative risk analysis should generally consider two alternative risk scenarios:

- > The plausible worst-case consequence
- > The most likely foreseeable consequence

Both scenarios should be analysed, and the highest overall risk level used to describe the risk against the specific consequence category. In some circumstances, the lower severity/higher likelihood (most likely foreseeable) scenario can result in a higher risk rating than the higher severity/lower likelihood (plausible worst case) scenario.

The chosen likelihood rating must match the chosen consequence rating e.g. if an assessment is undertaken in terms of the plausible worst case consequence scenario, then the risk must be assessed in terms of the likelihood of that consequence scenario occurring and not the likelihood of any threat scenario.

Risks with a residual consequence rating of severe are 'critical risks'. Where multiple consequence categories are assessed, the overall risk rating is taken as the highest from all consequence categories assessed. Table 6 illustrates these principles for a hypothetical example:

Table 6: Risk Rating

Risk Rating	Risk Type				
Risk Scenario	Safety	Bushfire	Reliability	Compliance	Financial
Plausible worst case	Medium	High	High	N/A	Medium
Most likely foreseeable	High	High	Medium	N/A	Medium
Consequence-specific risk rating	High	High	High	N/A	Medium
Overall Risk Rating	High				

Where the standardised Network Risk Matrix does not provide sufficient granularity to inform a specific risk assessment, it can be modified. Examples include modifications to the likelihood and/or consequence scales, to

COMMERCIAL-IN-CONFIDENCE

provide more granularity and/or to extend the standard scales to provide for higher or lower values. Changes can also be made to vary the units of likelihood e.g. to include chance (%), probability or the rate of occurrence per operation.

Bespoke matrices can also be created e.g. to contextualise the likelihood or consequence categories or scales, or to simplify them e.g. into a 3x3 matrix (instead of 5x5). This is allowable, provided any modifications maintain strict alignment to the Network and Corporate Risk Matrices and the rationale for any modifications is appropriately documented. Wherever possible, the choice of likelihood and consequence ratings should be supported by evidence.

The Network Risk and Performance Team must be engaged to review modified risk matrices before they are used to inform any risk assessments.

Toolkit

- [Network Risk Matrix](#)
- [Simple Qualitative Risk Register Template](#)

4.3.2 Semi-quantitative risk analysis

Semi-quantitative risk analysis can be performed where a numerical representation of risk is required. This can be done by monetising the consequence values (as set out in [CECG1140 Network Value Framework](#)) and using standard assumptions for converting the qualitative likelihood scales defined in the Network Risk Matrix into single point estimates. The standard assumptions to be used in this approach are outlined in Table 7:

Table 7: Converting qualitative likelihood scales to single point estimates

Likelihood Rating as per CECG0002.21a	< Once every 10 years	Once every 3-10 years	Once every 1-3 years	1-5 times per year	> 5 times per year
Standard Single Point Estimate	Once in every 20 years	Once every 6.5 years	Once every 2 years	3 times per year	5 times per year

Subjective probability estimates can also be used. Guidance on subjective probability estimates is provided in Appendix A.

Alternatively, the likelihood and consequence scales from the [Network Risk Matrix](#) can be converted to interval or ratio scales or indices. As with the standard equation (Figure 15) risk is then calculated as the product of the likelihood and consequence indices.

A key benefit of semi-quantitative analysis is the ability to aggregate risks. This can be done simplistically by summing the risk score/index or monetised value across all the identified risks. However, care should be taken to understand and articulate the level of accuracy of any resulting numbers that come from this approach, to reflect:

- > the granularity of the matrix used
- > the choice of a single consequence scenario (where in reality the total risk is the product of a probability distribution across a range of consequence scenarios)
- > the potential for real-world overlaps and dependencies between risks, which will result in many fluctuations within the final aggregated risk number.

Contact the Network Risk and Performance Team for further advice and support.

Toolkit

- [Network Risk Matrix](#)
- [Advanced Monetised Risk Register Template](#)

4.3.3 Quantitative risk analysis

Quantitative risk analysis uses numerical values for both likelihood and consequences, and therefore gives a specific numeric estimate of risk.

Numeric estimates of likelihood and consequence can be derived directly from data or using expert elicitation techniques e.g. to determine the probability or expected consequence of a defined risk event. Alternatively, estimates can be derived through numerical techniques such as Fault Tree Analysis, Event Tree Analysis or Markov Chain, or through the development of a bespoke engineering or numerical model. Where appropriate, probabilistic simulation techniques such as Monte Carlo Analysis may also be used.¹⁵

Further guidance on the use of alternate data sources to inform quantitative risk analysis is provided in Section 9.1. Additional guidance that may be of use in estimating the parameters needed to support quantitative risk analysis is provided in Appendices B, C and D. A list of common assumptions for use in quantitative risk analysis is provided in Appendix E.

A quantitative risk analysis will be built up of two separate components, the 'Likelihood' or 'Probability of Failure' (PoF) component and the 'Consequence' or 'Consequence of Failure' (CoF) component. The relationship between these components and the generic risk equation is shown in Figure 16.

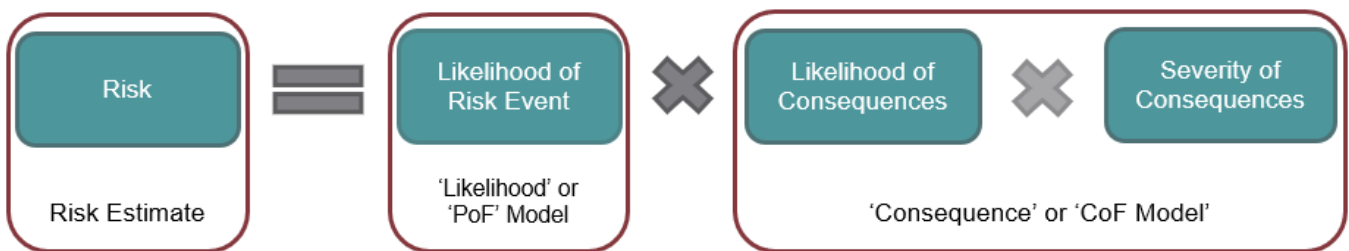


Figure 16: Risk calculation for quantitative risk analysis

When creating a new quantitative risk model it is essential that the appropriate stakeholders are included in the:

- > validation of the modelled scenarios,
- > modelling logic,
- > parameter assumptions made, and
- > calibration of any outputs.

Stakeholder groups that should be considered include SMEs relevant to the technical content and use of the model, custodians of the underlying enterprise data sources and analytics SMEs.

The 'risk model' must also be appropriately documented to a standard that would allow someone who was not involved in the model creation to understand the:

- > Context
- > Assumptions
- > Data source availability, choice rationale, traceability and confidence levels
- > Risk calculation methodology including its description, inputs, operation, limitations and outputs, including appropriate confidence limits
- > Quality control methodology
- > Areas for future improvement.

It is essential that any confidence limits associated with the outputs from quantitative risk models are clearly articulated; this is key to ensuring that model outputs are treated appropriately, including in any subsequent decision making.

Complex models must undergo appropriate quality checks. This may be achieved through:

¹⁵ Quantitative models may be deterministic or probabilistic. Deterministic models will output a single point estimate for each risk analysed, for example Risk = 0.002 fatalities per annum, or (if the consequences are monetised), Risk = \$94,672. Probabilistic models output a distribution of values for risk and allow for confidence intervals to be calculated around the risk value. For example, we are 90% confident the annualised (monetised) risk is between \$85,230 and \$103,265 with the expected (mean) risk = \$94,672.

COMMERCIAL-IN-CONFIDENCE

- > Building logical checkpoints into the model (e.g. to ensure selected fields sum to a logical number)
- > Use of appropriate software tools (applied by the person who created the model e.g. Spreadsheet Detective)
- > Design and implementation of a Quality Control plan (designed and executed by the model developer e.g. for randomised checks of the completed model)
- > Independent checking by an internal person not closely involved in the development of the model
- > Independent checking by an external person not involved in the development of the model

The level of checking should be appropriate to the complexity and criticality of the model.

It is beyond the scope of this document to provide a comprehensive description of all relevant methods plus the detail of all existing Essential Energy models and their application across the Asset Management System. As such, the remainder of this section sets out:

- > An overview of the Asset PoF, CoF and Risk models developed within the 2020-21 Asset Strategies project
- > A generalised approach to creating a Likelihood or PoF model
- > A generalised approach to creating a Consequence model
- > An overview of Essential Energy Common Consequence models (safety, bushfire, reliability, environment)
- > Generalised requirements for quantitative risk models
- > Guidance for calculating the individual or societal risk of fatality

A comprehensive description of the various methods available for quantitative risk analysis can be found within IEC31010, section B.5. Further detail is provided via the [Network Risk Management SharePoint site](#). **Contact the Network Risk and Performance Team for further advice and support.**

Overview of Asset PoF, CoF and Risk models developed within the 2020-21 Asset Strategies project

Recent work to refresh Essential Energy's Asset Strategies developed a suite of Asset PoF, CoF and Risk models associated with network asset failure events. The models were developed using a combination of:

- > data analysis (including direct estimation of model parameters, plus statistical curve fitting techniques), and
- > expert elicitation techniques.

Some PoF models made use of the Common Network Asset Indices Methodology (CNAIM)¹⁶; CoF models were based on Event Tree analysis; consequences were all monetised using the Value Framework (CECG1140).

The models were built at an individual asset level and aggregated to population (or sub-population) level and/or failure mode level. As such, the models may be used to inform prioritisation of asset-level work, albeit within an understanding of the accuracy and confidence level of each model. A model maturity assessment has been developed to support with this assessment.

The project also developed spatial maps of risk, including aggregated risks at network, depot and operational areas. Where a relevant Asset PoF, CoF or Risk model exists, this must be used to inform quantitative risk analysis.

As part of developing the models, the project also developed a suite of common assumptions, sub-models and modelling principles that can and should be used when developing other asset risk models or in other risk assessments. This is important, to ensure consistency in the organisational approach to modelling risk or risk events.

Once validated and approved, the asset models and supporting documentation will be made available on the [Network Risk Management SharePoint site](#).

Any queries related to the asset risk models should be directed to the Network Risk and Performance team in the first instance via networkrisk@essentialenergy.com.au

¹⁶ https://www.ofgem.gov.uk/sites/default/files/docs/2017/05/dno_common_network_asset_indices_methodology_v1.1.pdf

COMMERCIAL-IN-CONFIDENCE

Generalised approach to creating a Likelihood or PoF model

This section sets out general considerations for the development of quantitative Likelihood estimates or PoF models.



Quantitative measures of likelihood may include:

- > probability (number between 0 and 1)
- > chance (%)
- > frequency or rate (e.g. events per year)

When creating a likelihood estimate or model it is essential to consider the period over which any event occurrence is measured. For instance, is it the likelihood the event will occur in the next day, year, month or decade? Or on the next operation of a piece of equipment or performance of a defined task?

Generally, in situations where quantitative risk analysis is used to analyse risk over the short term a single point estimate for likelihood will be sufficient, for example probability of crossarm failure over the next year = 1.34×10^{-3} .

In situations where the model is needed to inform risk estimates over the medium to long term it may be necessary to develop a probability distribution. This can be discrete (defined by a series of discrete data points) or continuous (defined by a numerical function). For example, if analysing the risk associated with crossarm failure in the next 10 years, the probability of failure could be represented by the discrete distribution shown below in Table 8.

Table 8: An example of discrete distribution in crossarm failure

Year	1	2	3	4	5	6	7	8	9	10
PoF ¹⁷	9.23×10^{-4}	8.67×10^{-4}	6.34×10^{-4}	2.16×10^{-4}	9.67×10^{-3}	7.23×10^{-3}	4.15×10^{-3}	7.23×10^{-2}	4.10×10^{-2}	1.98×10^{-2}

A consideration in the development or use of any probability distribution is the type of distribution function, including:

- > probability density function (pdf)
- > cumulative distribution function (cdf), or
- > hazard rate.

Each may be valid, depending on the context and intended use of the risk estimate. The model developer should make a deliberate choice of the type of distribution function they are using and document the rationale for their choice.

Where a probability distribution is used, the decision on the type of distribution (e.g. random, uniform, normal, lognormal, PERT, Weibull) and on the associated distribution parameters must be deliberate and justified. General advice and considerations regarding how to select a probability distribution will be provided on the [Network Risk Management SharePoint site](#). For complex models, the decision-making process should include input from appropriate SMEs, e.g. from Network Analytics or Network Intelligence teams.

Once the method of likelihood modelling has been determined, a relevant and representative dataset will need to be sourced. Data should cover a sufficient period and be representative of the risk being modelled; it should also be sourced from enterprise systems and in consultation with appropriate data custodians.

Advice on appropriate statistical analysis techniques, statistical functions or distributions should be obtained from appropriate SMEs, including from the Network Analytics and Data Science and Analytics teams.

Where it is not possible or reasonably practicable to obtain a relevant and representative data set for a particular failure mode, expert elicitation techniques can be used to estimate relevant distribution parameters. Further

¹⁷ PoF here refers to the annual probability of failure given survival to the year listed, otherwise referred to as the Hazard rate.

COMMERCIAL-IN-CONFIDENCE

information on simple expert elicitation can be found on the [Network Risk Management SharePoint site](#). Alternatively, contact the Network Risk and Performance Team or local Network Risk Champion for advice.

Toolkit

- [IEC31010:2019 Risk Management - Risk Assessment Techniques](#)
- [Link to Risk Models](#)
- [PoF Training Materials](#)
- [Eliciting Input and Expert Judgement Guide](#)

Generalised approach to creating a Consequence or CoF Model

Consequence estimates or models are generally split into two parts. The first part estimates the likelihood of a certain consequence being realised and the second part estimates the severity of that consequence:



Wherever a risk event can result in multiple consequence types and/or severity levels, the model can be further broken down by splitting out the 'Likelihood of Consequences' parameter into a 'Likelihood of Consequence Type' parameter and a 'Likelihood of Consequence Severity Level' parameter:



The likelihood of different types or severity of consequences occurring, given a particular network risk event should be assessed having regard to specific risk events and location characteristics. For example, in considering pole failure, we would expect the likelihood of consequences to vary across the different scenarios of a:

- > wood pole versus a composite pole (affects the likelihood of failure resulting in public safety hazard)
- > pole in a paddock versus outside a busy shopping centre (affects the likelihood of someone being there when the pole fails)
- > simple pole versus a complex pole (affects the time to replace and therefore the length of any outage; also the cost to replace)
- > pole supplying one customer versus a pole supplying a key industrial load (affects the amount of unserved energy)

These types of factors are generally referred to as consequence differentiators. These are factors related to an asset, system or the operating environment that influence the likelihood of a consequence occurring or the severity of the outcome. They should be carefully selected given a thorough understanding of the risk environment through consultation with relevant SME's. Table 9 presents some examples of consequence differentiators.

Table 9: Suggested consequence differentiators

Risk	Consequence Differentiators
Safety	Levels of public/worker exposure (how many people, for how long, how often)
	Nature of failure mode (detectable/visible, gradual/explosive, short-lived/persists in hazardous state until detected/addressed)
Network (Reliability)	Number of customers affected/level of unserved energy
	Customer type
	Time to effect repairs (including due to nature of work required and distance from depot)
	Availability of redundant supply/back feed or other contingency options
Bushfire	Bushfire priority zone (P1, P2, P3, or P4)
Environment	Proximity to environmentally sensitive area or heritage site or national park
	Availability of containment measures (such as oil bunding)
Finance	Value of assets affected (primary or secondary failures)
	Cost of fault-and-emergency response
Reputation	General level of stakeholder concern or scrutiny
	Recent performance, which may act as an escalator for stakeholder concern or scrutiny

For a given risk event, there will often be a distribution of possible consequence types and severity levels that could be realised. As with all types of risk analysis, only material consequences and severity levels should be modelled.

Alternative approaches to modelling risk events where there are a range of possible severity levels include:

Minimal approach:

- > Risk = (probability of risk event) x (likelihood x most likely foreseeable consequence severity), or
- > Risk = (probability of risk event) x (likelihood x plausible worst case consequence severity)

Model selective consequence severities only, for example:

- > Risk = (probability of risk event) x ((likelihood x severe consequence) + (likelihood x moderate consequence))

Model all consequence severity levels:

- > Risk = (probability of risk event) x ((likelihood x severe consequence) + (likelihood x major consequence) + (likelihood x moderate consequence) + (likelihood x minor consequence) + (likelihood x insignificant consequence))

Event Trees are a useful tool to support consequence modelling. Where a related event tree model has been developed as part of the 2020-21 Asset Strategies that should be reviewed and used or adapted as appropriate. An [event tree template](#) has been created for situations where a relevant event tree model does not already exist. This can be accessed via the [Network Risk Management SharePoint site](#).

As with semi-quantitative risk analysis, the Severity of Consequence can be monetised using the network risk consequence criteria and the corresponding cost of consequence from the Network Value Framework. Alternatively, the monetised cost of consequence can be estimated directly. For consistency, direct estimation should be limited to financial consequences. The Network Value Framework should be used for all other consequence types.

COMMERCIAL-IN-CONFIDENCE

When consequences are monetised, it is important to include costs to customers **and** costs to Essential Energy. Estimates of monetised risk should also include relevant Disproportion Factors, as defined in the Value Framework (CECG1140). This ensures estimates of monetised risk fully represent the ‘value’ of risk to all parties impacted.

Toolkit

- [Business rules for PoF, CoF and asset risk models](#)
- [Library of Risk Models](#)
- [Event Tree Template](#)

Essential Energy Safety Consequence ‘CoF Model’

When modelling safety consequences, the following generalised consequence equation should be used:

Likelihood of Consequences

×

Severity of Consequences

=

$$p(\text{safety hazard, given failure}) \times p(\text{someone comes into contact with the hazard}) \times p(\text{consequence severity level(s) from risk matrix}) \times (\text{consequence severity})$$

‘CoF Model’

Common safety consequences for network risk events include injuries due to physical impact, electric shock, fires, arc flash, and projectiles. Figure 17 shows a generalised model for thinking about how these consequences arise:

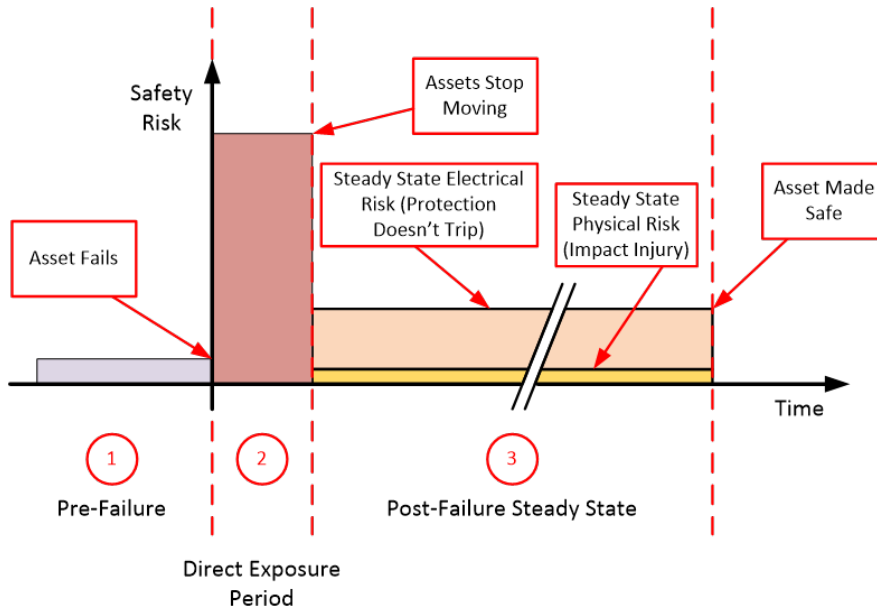


Figure 17: Generalised model of how consequences arise from risk events

If safety is a particular concern or focus for the risk assessment, the development of an event tree should be considered. As a starting point, a generic event tree structure based on the principles in Figure 17 is provided below in Figure 18:

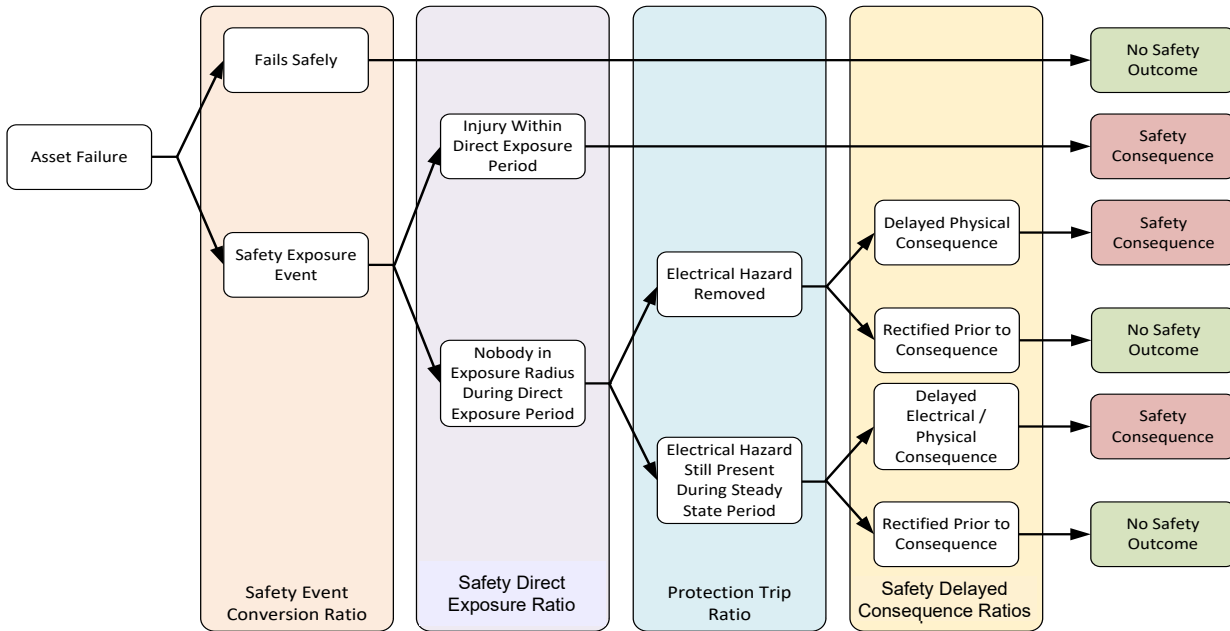


Figure 18: Event Tree

While this model has been developed to support modelling of safety risks associated with asset failure events, it can be used as a generic template for all 'network safety risk' events.

Within Figure 18:

- > **Safety event conversion ratio** – is dependent on the nature of the risk event/asset failure mode.
- > **Safety direct exposure ratio** – depends on the nature of the risk event and land use surrounding the risk events' location. Generic public and worker exposure assumptions are listed in Appendix E. Public safety exposure zones are also being developed for use in assessing public safety risks associated with overhead network assets. These will be analogous to bushfire priority zones and are expected to be defined in terms of several categories including Very High, High, Urban, Rural, Remote, Backyard, Road/Rail Crossing. It is expected that a subset of these categories will also be applicable for use with Zone Substations e.g. Backyard, Urban. More information is available on the [Network Risk Management SharePoint site](#).
- > **Protection trip ratio** – this is dependent on the type of protection device sensing the line, the distance along the line from the protection device where the failure occurs, amongst other things. Generic ratios will be made available on the [Network Risk Management SharePoint site](#) once developed.
- > **Delayed consequences ratios** – will depend on the nature of the risk event/failure mode; they are mostly applicable when considering risks associated with dropped conductors.
- > **Safety consequences** – are dependent on the nature of the hazard as well as many other environmental and 'people' parameters, for example what clothing a person was wearing, a persons' underlying health conditions, personal choices or actions in response to a network event.

A list of common assumptions for use in quantitative modelling of safety consequences is provided in Appendix E.

Quantitative risk analysis may use a range of units or measures of safety risk, depending upon the decision that the risk assessment is intended to inform; further guidance is provided in Section 9.5. Alternatively, safety risk may be monetised, as per the Network Value Framework (CECG1140).

Essential Energy Bushfire Consequence Model

When modelling bushfire consequences, the following generalised consequence equation should be used:

$$\begin{array}{|c|c|} \hline \text{Likelihood of} & \text{Severity of} \\ \text{Consequences} & \text{Consequences} \\ \hline \end{array} \times \text{CoF Model} = p(\text{fire ignition, given risk event}) \times p(\text{severe or moderate fire, given ignition}) \times (\text{consequences of severe or moderate fire})$$

COMMERCIAL-IN-CONFIDENCE

The probability of fire ignition, given a risk event will vary dependent on the nature of the risk event (e.g. asset involved and failure mode) and on locational factors, such as the physical environment directly adjacent to the asset and the time of year (e.g. total fire ban day, or at a time of year when heavy rain is common).

If specific data is not available and the effort to obtain specific data is disproportionate to its importance to the risk assessment, network-level average figures may be used. These numbers are summarised in Table 10 for unassisted and assisted asset failures¹⁸.

Table 10: Network-level averages for unassisted and assisted asset failures

Year	2017	2018	2019	2020	2021
Number of unassisted asset failures	3,861	5,359	4,615	6,043	5,312
Number of fires from unassisted asset failures	165	170	152	145	125
p(fire ignition, given unassisted asset failure)	4.27%	3.17%	3.29%	2.40%	2.35%
Number of assisted asset failures	4,260	4,133	4,305	6,770	4,238
Number of fires from assisted asset failures	106	94	73	72	67
p(fire ignition, given assisted asset failure)	2.49%	2.27%	1.70%	1.06%	1.58%

Further breakdown of the asset failure data by asset class is available from the 'Network Asset Failure Report' which can be found [here](#). Further breakdown of the fire start data by asset class is contained within the 'Essential Energy Fire start register' which is held and maintained by the Network Failure Investigations team.

The probability and expected consequences of a severe or moderate fire, given ignition are described by the Essential Energy [Fire Model](#). This sets out estimated probabilities and consequences for fires, differentiated by bushfire priority zones P1 – P4 (see Table 11). Within the Essential Energy Fire Model, consequences of bushfires are monetised; the basis for monetisation is described in the Network Value Framework (CECG1140).

Table 11: Probability and consequence of severe or moderate fires

Bushfire LoC by BFP zone	P1	P2	P3	P4
Probability of Severe bushfire, given fire start	2.29E-03	2.55E-04	4.97E-06	2.74E-05
Probability of Moderate bushfire, given fire start	4.03E-03	1.01E-03	7.15E-04	1.36E-04
Expected consequence including disproportion factors (\$2020) -				
Severe	\$2,406,008	\$268,552	\$5,231	\$28,833
Moderate	\$31,753	\$7,964	\$5,636	\$1,073
Combined	\$2,437,761	\$276,516	\$10,867	\$29,906

Note that the monetised consequences of bushfire events defined in CECG1140 do not include for any network reliability impacts associated with bushfire events.

¹⁸ Data correct as of 04/08/2021

COMMERCIAL-IN-CONFIDENCE

Bushfire priority (BFP) zones consider Essential Energy’s fire risk modelling and Phoenix house loss modelling to categorise each vegetation maintenance area within Essential Energy by bushfire risk priority P1 to P4. Generally, P1 zones represent the highest bushfire risk zones, with P3 and P4 zones representing the lowest risk. For further information regarding BFP zones refer to [CEOP8067](#).

Network (Reliability) Consequence Model

When modelling reliability consequences the following generalised consequence equation should be used:

The diagram shows a box labeled 'CoF Model' containing two rounded rectangular boxes: 'Likelihood of Consequences' and 'Severity of Consequences', connected by a multiplication symbol (X). To the right of this box is an equals sign followed by the equation: $p(\text{outage, given risk event}) \times p(\text{consequence severity}) \times (\text{consequence severity})$.

Generic values for the probability of an outage, given a risk event will be made available via the [Network Risk Management SharePoint site](#).

Quantitative estimates of the consequence severity from network outages can then be calculated via one of two methods:

- Unserved energy method— requires the amount of unserved energy (MWh) by customer type to be known,
- Customer minutes lost method— requires a count of customers without power and the duration these customers are without power.

The energy interrupted method is the preferred method as this can be used for all customer types, whereas the customer minutes lost method is limited to determining the consequences associated with residential customer outages. The customer minutes lost method should only be used where the unserved energy is not known and cannot reasonably be determined for the purpose of the risk assessment.

In practice, network reliability consequences are usually monetised. Guidance on the monetisation of reliability consequences is provided within Section 3.3 of [CECG1140](#).

When monetised, the network reliability consequence includes two components:

1. Value of customer reliability (VCR)
2. Costs to Essential Energy

Note that the VCR and other monetised consequences of network reliability events defined in CECG1140 do not include for any safety impacts associated with Loss of Supply events.

The VCR calculation methods are as follows:

1. Unserved energy method:

$$VCR = U * R_C$$

Where:

- VCR = Value of customer reliability (\$)
- U = Unserved energy (MWh)
- R_c = VCR rate by customer type (\$/MWh)

2. Customer minutes lost method:

$$VCR = N * (R_{ff} + D * R_D)$$

Where:

- VCR = Value of customer reliability (\$)
- N = Number of customers interrupted
- R_{ff} = VCR flag fall rate (\$/customer)
- D = Outage duration (minutes)

COMMERCIAL-IN-CONFIDENCE

$$R_D = \text{Duration rate (\$/customer*minute)}$$

When using the customer minutes lost method, the number of customers interrupted (N) is taken as the number of customers downstream of the nearest upstream protection device.

There are several customer categories by which the VCR rate (R_c) is differentiated, details of which are found within CECG1140. These categories align the Australia and New Zealand Standard Industrial Classification (ANZSIC) codes. ANZSIC codes have been matched with each premise connected to Essential Energy’s network, to assist with this calculation.

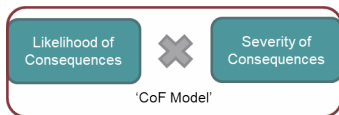
Once VCR has been determined, the second step to calculate the total monetised network consequence is to determine the costs to Essential Energy. The table below has been adapted from CECG0002.21a to assist with the cost to Essential Energy severity selection. Monetised values for each consequence severity are provided in the Network Value Framework CECG1140.

Table 12: Consequence severity levels for network reliability

Consequence Severity Level	Insignificant	Minor	Moderate	Major	Severe
Description	Outage impact <1% of annual forecast e.g. - 10-hour outage to <2,500 customers - <2 minutes SAIDI impact	Outage impact 1-2% of annual forecast e.g. - 10-hour outage to 5,000 customers - 3 minutes SAIDI impact	Outage impact 2-5% of annual forecast e.g. - 10-hour outage to 10,000 customers - 7 minutes SAIDI impact	Outage impact 5-10% of annual forecast e.g. - 10-hour outage to 20,000 customers - 15 minutes SAIDI impact	Outage impact >10% of annual forecast e.g. - 10-hour outage to >40,000 customers - >25 minutes SAIDI impact
Unserviced Energy Equivalent	<50MWh	50MWh =< U < 150MWh	150MWh =< U < 300MWh	300MWh =< U =< 800MWh	>800MWh

Essential Energy Environment (Other) Consequence Model

When modelling environmental consequences, the following generalised consequence equation should be used:



$$= p(\text{environmental incident, given risk event}) \times p(\text{consequence severity level(s) from risk matrix}) \times (\text{consequence severity})$$

While land use codes may be useful to indicate or differentiate the likelihood or severity of environmental consequences, there are no standardised assumptions for modelling the likelihood of environmental incidents or conversion rates for resulting consequence severities. Moving forward, it is intended to address this through an environmental consequence model, similar in format to the safety, bushfire and reliability models described above. This model will likely be based upon land use codes. Further information will be provided via the Network Risk Management SharePoint site once available.

Generalised Requirements for Quantitative Risk Models

Depending on the context of the risk assessment, risk may be calculated as an annualised figure and/or as a profile of annualised risk over time. When risk has been monetised, the discounted risk profile over time can also be presented in terms of net present risk.

Risk may also be presented as an aggregate total risk amount or broken out by component risk categories. Wherever safety is a consideration, a stand-alone view of safety risk should always be produced.

Calculating the Individual or Societal Risk of Fatality

High level guidance on calculating measures of individual or societal risk, for comparison with safety risk tolerability criteria set out in Section 2.6.3 is provided in Section 9.5. More detailed guidance on calculating individual and societal risk is available in the Individual Risk Guide.

Toolkit

- Simple Qualitative Risk Register Template
- Individual Risk Guide

4.3.4 Calibration and validation of risk analysis outputs

Regardless of the technique or method used, an important final step in any risk analysis is the calibration and validation of outputs. This should include checks to ensure **as a minimum** that:

- > overall risk ratings align with relevant ‘parent’ risks e.g. from the corporate or network risk registers
- > the implied performance outcomes (frequency, type and severity of outcomes) are supported by data, historical performance observations or SME judgement.

Both these checks are essential to ensure that bottom-up risk analyses aggregate to credible and realistic estimates of the network level of risk.

4.4 Risk Evaluation and Treatment

Risk evaluation and risk treatment are highly connected, iterative parts of the network risk management process. Figure 19 shows the key steps involved:

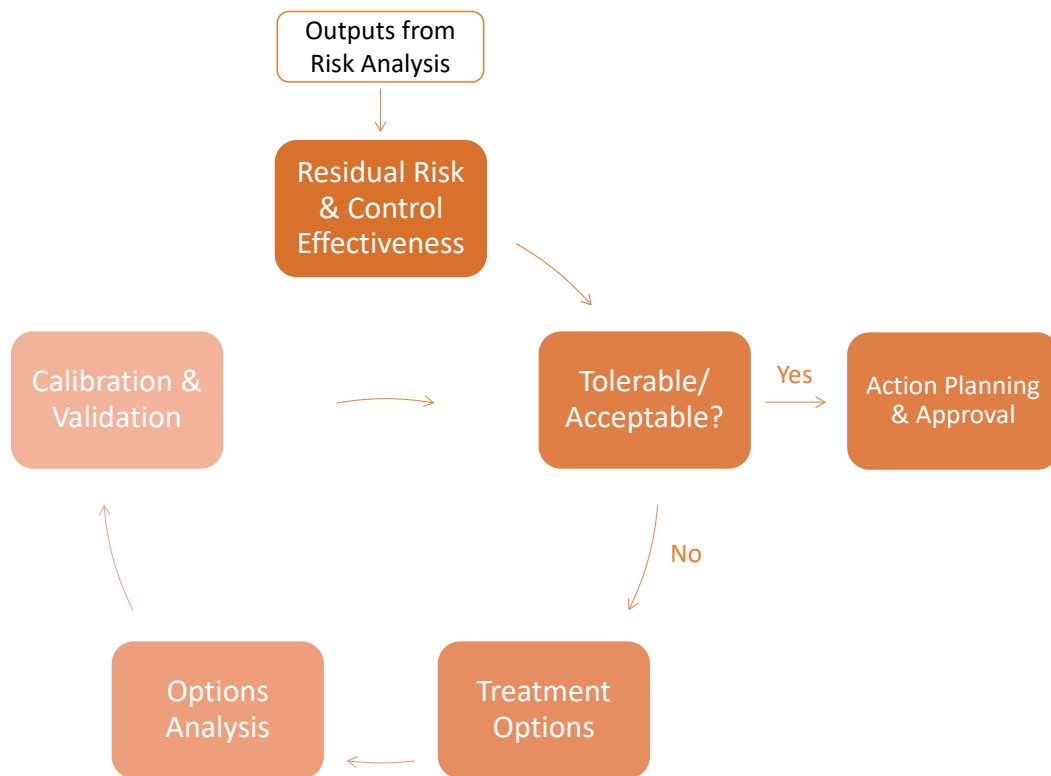


Figure 19: Key steps in risk evaluation and risk treatment

4.4.1 Risk Tolerability and Acceptance

Once the residual risk level and control effectiveness are understood from the risk analysis, they must be compared with the risk objectives (in Sections 2.3.1 and 2.3.2) and the risk tolerability and acceptance criteria (in Section 2.6), to understand whether alternative or additional treatments are required.

COMMERCIAL-IN-CONFIDENCE**Risk Tolerability**

In summary:

- > there are no hard limits in terms of tolerable residual risk ratings from the Network Risk Matrix (e.g. Extreme, High, Medium, Low risk); however,
- > hard limits exist for tolerable levels of individual and societal risk of fatality per annum (see Sections 2.6.3 and 2.6.4).

If risk evaluation identifies any unacceptable safety risks you must act immediately to (i) validate that finding, and if confirmed to (ii) bring the risks into the tolerable region. This is particularly important if you are assessing the risk associated with a 'live' situation on the electricity network. An unacceptable risk is one where the benefit of the activity is no longer tolerable, given the risk. As such, the risk must be eliminated, or reduced into the tolerable region immediately and for the period while further investigations identify and implement a SFAIRP solution. Where necessary, 'interim' risk controls may be put in place as a temporary measure whilst permanent controls are developed or sourced. Where used, interim controls must be reviewed for effectiveness at intervals determined by the residual risk level.

Risk Acceptance

The first step to accepting a risk is to consider the residual risk rating alongside the risk objectives and corporate risk appetite, to understand if there is a requirement to consider alternative or additional treatments.

There is also a need to consider alternative or additional treatments for:

- > all risks rated as Extreme or High from the Network Risk Matrix, and
- > all Safety, Bushfire, Environment, Compliance or Reputation risks rated Medium from the Network Risk Matrix, and
- > all other safety risks, to ensure those risks are managed SFAIRP as per relevant safety obligations.

Alternative or additional controls may also be considered for other risks rated as Medium or Low from the Network Risk Matrix, particularly if current controls are not effective, or if reasonably practicable controls are not yet implemented.

Particular attention should be paid to addressing existing critical controls that are not considered 'effective'.

Controls and/or treatments may be reasonably practicable if they are:

- > required to meet a defined strategic or AM objective/target, or
- > required by legislation or by industry standards or codes, or
- > already established as industry good practice, or
- > identified as recommendations from formal, authoritative reviews, audits or investigations, or
- > considered prudent by appropriate subject matter experts, and
- > supported by cost-benefit analysis.

Controls/treatments must also be strategically aligned, in the long-term interests of customers and affordable.

As a minimum, risks can be accepted once they are managed SFAIRP i.e. all reasonably practicable controls have been implemented. Additional treatments may also be required to achieve relevant discretionary or business-driven risk objectives (described as 'best endeavours' in Table 1).

The remainder of this section sets out practical considerations for meeting these requirements, in the context of the steps outlined in Figure 19, including demonstration of those considerations through a worked example.

4.4.2 Treatment Options

Actions within this step include:

- Options identification, including categorisation of safety treatments using the hierarchy of control
- Understand the benefits and risks associated with each option, to inform forecast residual risk and control effectiveness ratings that would result from each option
- Understand the costs of each option

COMMERCIAL-IN-CONFIDENCE

Options Identification

This step identifies options to:

- > Address known gaps or weaknesses in the current system of control (controls not effective)
- > Ensure risks are managed SFAIRP (even if current controls are considered effective)

Within this, options may be made up of individual/discrete treatments or may comprise bundled combinations of treatments.

For non-safety risks, there is a need to identify all 'credible' (believable) options; for safety risks, there is a need to identify all 'practicable' (possible) options.

For safety risks, options identification should include consideration of the hierarchy of control (see below). This should be used to guide options identification in the context of: What could we do to eliminate the risk? What could we do to substitute the risk?

The hierarchy of control may be used in the same way to guide options identification for non-safety risks, with the exclusion of the PPE layer.

Options identification can also be guided by the risk acceptance criteria set out in Section 4.4.1 e.g. Is there anything we are not already doing that is a requirement of legislation or industry codes or standards? Is there anything we are not already doing that is considered established industry good practice? Has anything been identified from related reviews, audits or investigations? Are there any other changes to current controls that are considered prudent by appropriate SMEs?

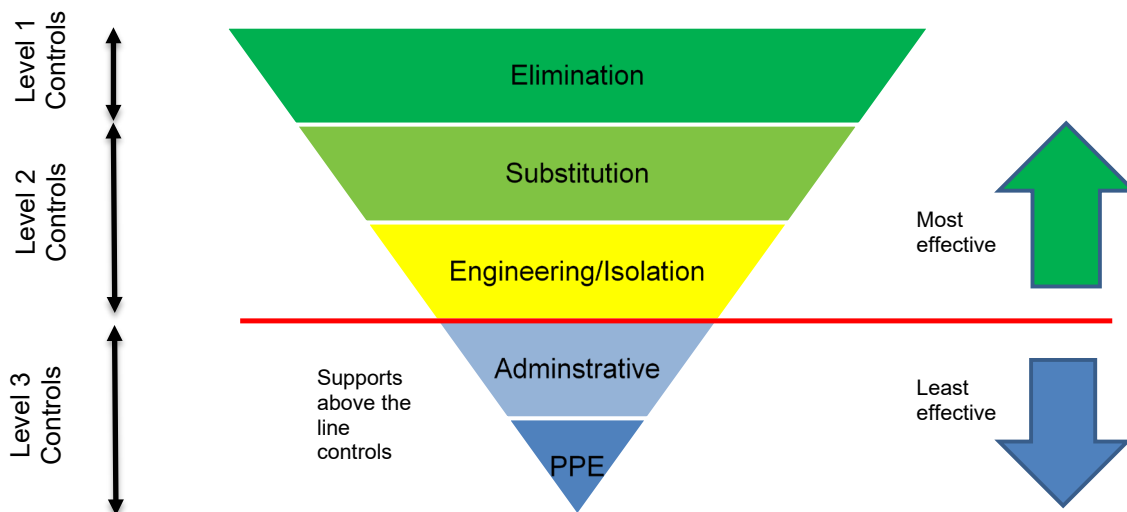


Figure 20: Hierarchy of (Safety) Risk Control

COMMERCIAL-IN-CONFIDENCE

A further concept that can be used to guide options identification is that of a bathtub 'lifecycle effectiveness' curve shown in Figure 21 below. This reflects the concept that controls targeted at the early or late stages of an asset or decision lifecycle present the greatest opportunity to influence residual risk.

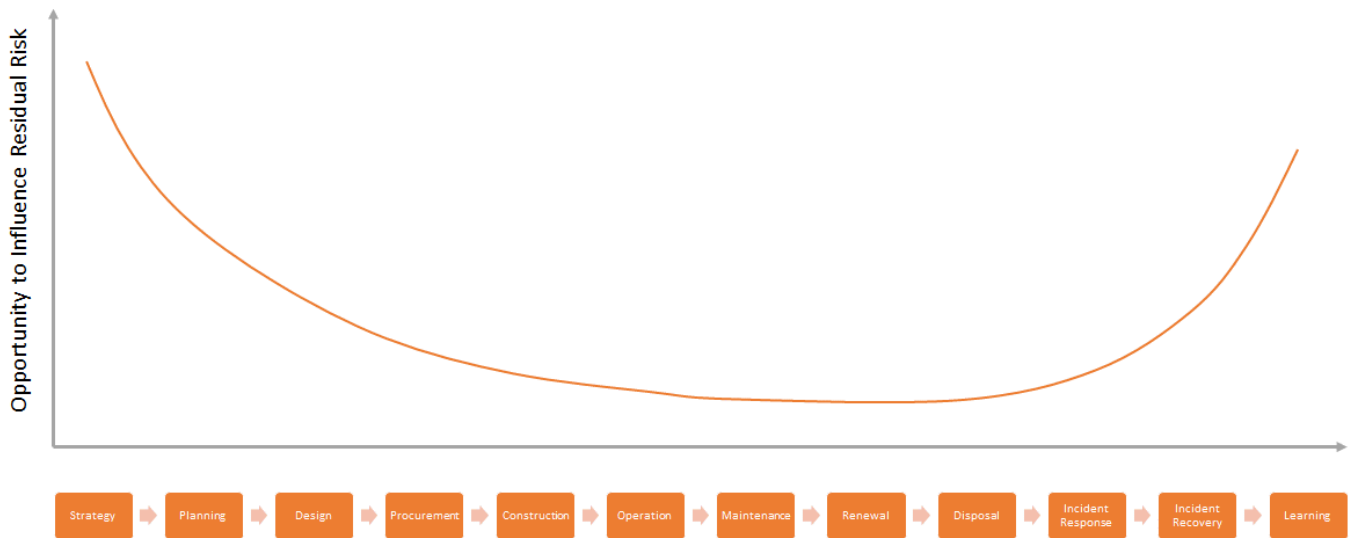


Figure 21: Lifecycle effectiveness of risk controls

Benefits, Risks, Forecast Residual Risk Rating and Control Effectiveness

There is a need to understand the benefits and risks associated with each option and to use this information to forecast the residual risk and control effectiveness ratings that would eventuate from each option once implemented.

Forecasts should establish line of sight to existing control gaps or weaknesses, demonstrating how treatment options will address these, and substantiating the extent of any forecast risk reductions or control effectiveness improvements.

Treatments introduced to reduce the level of one or more risks may directly or inadvertently increase the level of another risk or result in the transfer of risk from one party to another. A complete understanding of the effects of changing or implementing new controls is required to feed into options analysis.

Where options combine or layer a number of treatments, care is needed to avoid double-counting benefits or risks e.g. if the benefits/risks of Treatment A alone = x and the benefits/risks of Treatment B alone = y, the combined benefits/risks of treatments (A + B) when implemented together don't necessarily = (x + y).

Other considerations may include:

- > the time period over which different options deploy a particular treatment e.g. if the treatment is rolled out over a single year, or over a period of several years, resulting in an extended period of risk exposure over the rollout period, or
- > if different treatments have different expected lifespans or wear-out rates, affecting the risk exposure profile and time over which risk could return to the current level.

For safety, the level of analysis required in establishing the relevant benefits depends on the severity of the consequences. Where the consequences could include fatalities, AS5577 requires detailed evaluation of the resulting risk reductions (qualitative or numeric). Where there could be multiple fatalities, a numeric assessment may be necessary to determine the risk reductions achieved by alternative options.

Cost of Options

The costs of each option need to be understood in terms of:

- > lifecycle opex and capex costs including costs
- > costs reflecting the 'time' and 'trouble' associated with implementation.

COMMERCIAL-IN-CONFIDENCE

In certain circumstances it may also be useful to consider the opportunity cost of allocating constrained resources to one activity over another e.g. where this is practical to do and helps differentiate between options.

The format of any cost estimates will need to match the format of any benefit estimates. For example:

- qualitative (High/Medium/Low)
- semi-quantitative (>\$5m, \$1-5m, <\$1m)
- quantitative (\$3.5m net present cost).

Within this approach any quantitative calculations must follow the Investment Evaluation Procedure (CECP0002.32). For safety risks and where consequences could include fatalities, AS5577 requires that realistic estimates of associated costs be obtained.

4.4.3 Options Analysis

The options analysis step compares credible/practicable options to determine:

- > which options are reasonably practicable
- > which option manages the risk SFAIRP

The conceptual process of options analysis is shown diagrammatically in Figure 22, moving from a collection of credible/practicable options to those that are reasonably practicable, to the SFAIRP option.

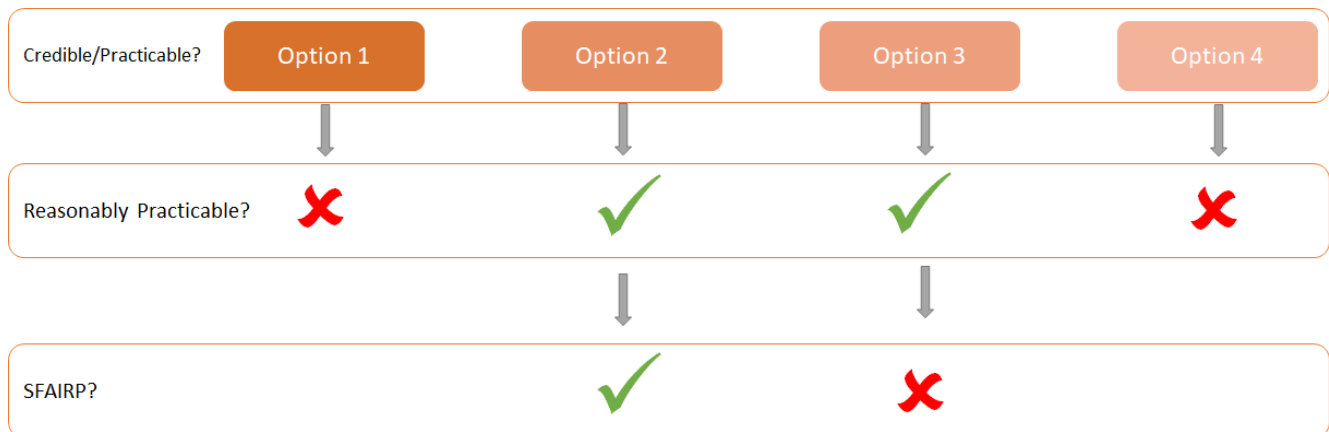


Figure 22 Process of Options Analysis

Reasonably Practicable Options

The purpose of this step is to rule out options that fail the definition of **reasonable** practicability in an absolute sense because they:

- > are not of themselves:
 - **necessary**: to meet a defined strategic or AM objective/target (including any associated risk target e.g. to maintain or reduce risk by a defined amount – see Section 2.3.2), *or*
 - **prudent**: by reference to requirements of relevant legislation, standards or codes, established industry good practice, a formal review, investigation or audit, or to satisfy engineering judgement; alternatively, because they introduce unacceptable risks, risk increases, risk trade-offs or impacts e.g. to other existing controls, *and*
 - **efficient**: as evidenced from cost-benefit analysis
- > are not strategically aligned or in the long-term interests of customers
- > are not affordable in a constrained environment, including in terms of time, trouble or money.

COMMERCIAL-IN-CONFIDENCE

Options identified from discretionary requirements of standards or codes¹⁹ or from industry good practice, must be considered in the context of costs to Essential Energy, which may legitimately be higher than industry average, due to the nature of the network or operating environment – thereby ruling them out as not reasonably practicable for us, even if others implement them.

The limit of (gross) disproportion for use in any monetised cost-benefit analysis is defined for different risk types by the associated Disproportion Factors. Using this approach, the mathematical condition for (gross) disproportion is defined as:

$$\frac{\text{Costs}}{\sum \text{Benefits} \times \text{DF}} > 1$$

Where:

- > Costs = the cost of the risk reduction measure
- > Benefit = the monetised risk reduction benefit
- > DF = the relevant disproportion factor for a particular risk type

Detail of current disproportion factors is provided in the Value Framework.

In practice, when the Cost/Benefit ratio is *close to* 1, or the Value is *close to* 0, (either above or below in both cases), the decision taker will need to consider the level of confidence in the risk, benefit and cost estimates when deciding whether an option is reasonably practicable. Care is needed to avoid assigning spurious accuracy to quantitative estimates, purely because they can technically be calculated more specifically e.g. with multiple decimal places.

As noted in Section 2.6.2 **affordability is not a defensible consideration for WHS controls**.

The SFAIRP Option

This step compares the various reasonably practicable options from the previous step to determine the option that manages risk so far as is reasonably practicable i.e. the most reasonably practicable option.

This is essentially a trade-off between the benefits and costs of the range of reasonably practicable options through consideration of qualitative and/or quantitative measures of:

- > Total benefits/risk reduction
- > Safety benefits/risk reduction
- > Any risk increases or trade-offs (shifting risk from one group to another, or from one risk type to another— including in the context of any related risk or performance objectives or risk appetite)
- > ‘Hard’ \$ costs of controls
- > Any ‘time’ or ‘trouble’ costs to implement
- > Any opportunity costs to implement (identifying if the incremental cost of a particular option could deliver more collective risk reduction if allocated elsewhere)

Specific considerations for demonstrating that safety risks are managed SFAIRP are guided by advice from Safe Work Australia²⁰. This states that, “*reasonably practicable means that which is, or was at a particular time, reasonably able to be done to ensure the health and safety, considering 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*

¹⁹ Recognises that not all requirements from standards are compulsory; some are subject to ‘best endeavours’ or limited by what is ‘reasonably practicable’

²⁰ Safe Work Australia, Interpretive Guideline – Model Work Health and Safety Act, The Meaning of ‘Reasonably Practicable’. Available at:

COMMERCIAL-IN-CONFIDENCE

- 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, Essential Energy must meet the standard of behaviour expected of a reasonable organisation in a similar position, that is required to comply with the same requirements.

AS5577 sets out an alternative explanation of these requirements:

This means that safety hazards and their associated risks, including risks to the community shall be eliminated as the first preference. Where it is not reasonably practicable to eliminate the risk, the treatments or controls shall be applied to reduce the risk to as low as reasonably practicable.

Control is achieved by the application of multiple independent protective measures. Where treatments or controls are applied, physical/engineering controls should be used in preference to procedural/managerial controls. Controls are considered effective when the residual risks associated with that hazard have been reduced to as low as reasonably practicable (ALARP) at that location.

The risk assessment should identify opportunities for further safety improvement, even if risks have been assessed as being ALARP, where determining if the risk from a specific threat has been reduced to ALARP involves an assessment of the risk to be avoided, the cost (in money, time and trouble) involved in avoiding the risk and a comparison of the two. Determining ALARP is in effect a cost benefit analysis. The measure of whether ALARP has been achieved is if the cost of reducing the risk is grossly disproportionate to the benefit gained. The reduction in risk must be insignificant when compared to the cost required.

The concept of ALARP contains an implicit assumption that there are alternative designs or measures that can reduce the risk but that some of these alternatives may not be ‘practicable’. (There is always at least one alternative—abandon the project or network). Any attempt to demonstrate ALARP that does not consider any alternatives, or at least search for them, is not convincing. An important part of the process of demonstrating ALARP is the identification and evaluation of alternative designs that offer lower risk. The following two questions illustrate the process:

(a) *What else could we do to reduce risk?*

(b) *Why have we not done it?*

*ALARP has been demonstrated when the answer to the second question, for each physically possible alternative, is ‘**because the cost is grossly disproportionate**’.*

The level of analysis required in establishing the relevant costs and safety benefits depends on the severity of the consequences. 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.

Where there could be multiple fatalities, a numeric risk assessment may be necessary to determine the risk reductions achieved by alternative designs. In all other cases, there should be at least a listing of all alternatives considered and the reasons for their rejection, including basic cost estimates. The analysis demonstrating ALARP must be documented in full.

AS5577 also states that treatments for safety risks must be applied in accordance with the hierarchy of control.

This does not require selection of the option with the lowest safety risk or that achieves SFAIRP for safety in preference or to the detriment of other risk objectives, provided this decision is substantiated through consideration of the various factors listed above.

The relative contributions of different factors or measures of benefits, risks and costs considered in the SFAIRP decision is informed by the middle section of the UKOOA framework (see below).

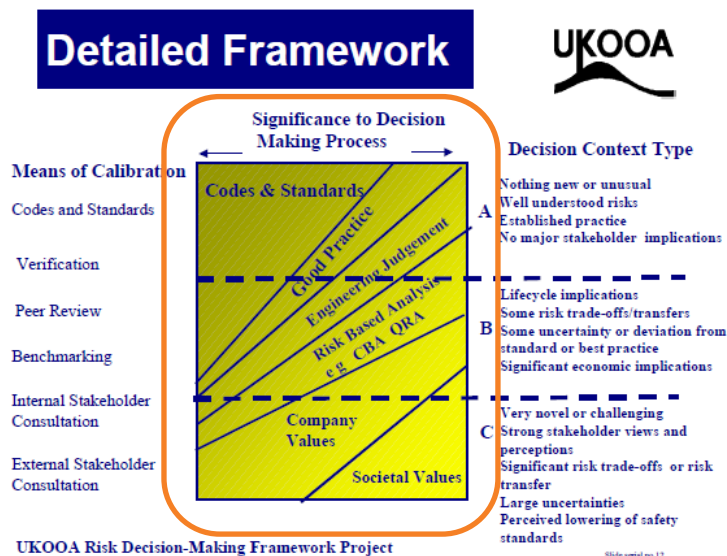


Figure 23: UKOOA risk-based decision framework

A worked example of this aspect of the UKOOA framework is provided in Section 4.4.6.

In practice, options should be ranked in the order of the safety Hierarchy of Control in the first instance. This is important to meet requirements to eliminate safety risk if reasonably practicable. If this is not reasonably practicable then progress to the next option on the hierarchy to assess if that is reasonably practicable and so on. This approach results in progressive analysis through the hierarchy of control. The analysis must demonstrate that options from higher up the hierarchy are grossly disproportionate (including for reasons other than safety) before selecting a SFAIRP option from a lower level of the hierarchy.

Where options are from the same level of the hierarchy of control, they should be ranked in order of the total benefits or risk reduction, starting with highest first. Safety benefits or risk reduction must also be stated alongside the total benefits/risk reduction so that these remain visible. Where safety is a particular concern or focus of the risk assessment, a calculation of individual or societal risk of fatality associated with each option may be made.

However, these can be complex calculations and so should only be included where they add material value to the decision-making process.

The SFAIRP option is the one that delivers the optimal risk-reduction/cost trade-off; to do more than this option to manage the risk would be disproportionate (in general) or grossly disproportionate (for safety) compared with the associated costs. In circumstances where all costs and benefits are monetised, this may be represented by the option with the highest benefit:cost ratio; in other circumstances a more qualitative or nuanced argument may need to be developed.

When comparing options through a cost-benefit analysis lens and using discounted costs and benefits, care is needed to understand the relative profiles of costs and benefits over time, and how these may differ across alternate options. For example, if one option delivers a lower overall cost-benefit, but delivers increased benefit in the short-term – is this more desirable than an alternative that delivers higher overall cost-benefit, but where most of the benefit occurs 15 years into the future? There is not a one-size-fits-all answer to this question. These types of factors therefore need to be understood in the context of specific risk assessments and appropriate ‘rules’ agreed and documented, along with the supporting rationale.

The risk assessment must capture the rationale for the SFAIRP decision in a clear and concise statement or artefact. Guidance on techniques for doing this is provided in Section 9.11.

Options analysis should also consider the need to undertake sensitivity analysis on any key assumptions, particularly if there are material uncertainties in any models or information underpinning the calculation and if results are close to any quantitative criteria (e.g. for tolerability or (gross) disproportion). This analysis should also take due account of any material human factors associated with the options.

4.4.4 Verification, Calibration and Validation

Verification, calibration and validation are critical steps to the close-out for any risk assessment, to:

- > **verify** that the risk assessment process has been applied appropriately, including appropriate quality checks on any quantitative models or tools developed to support the risk assessment,
- > **calibrate** the results against any existing or 'parent' risk assessments or performance data, and
- > **validate** results with key stakeholders and against any external sources.

This final check is guided by the left-hand section of the UKOOA framework shown in Figure 24 below. It provides a final check on the risk assessment results, prior to action planning and approval.

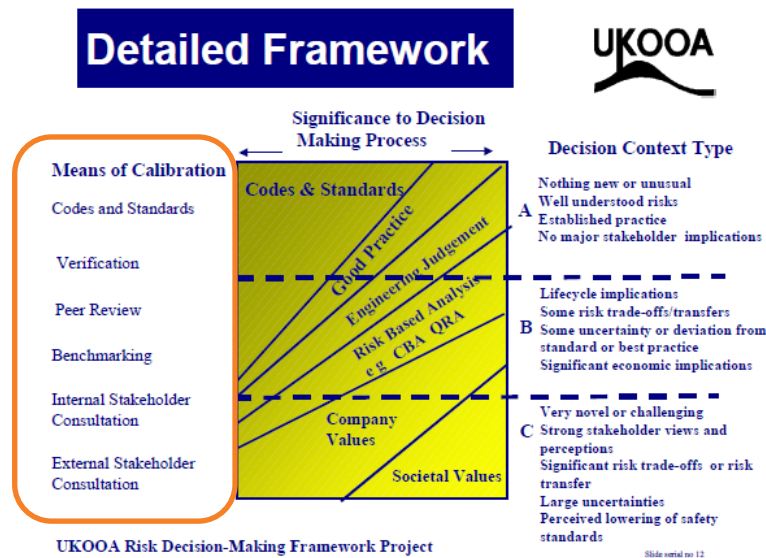


Figure 24: Final checks in UKOOA framework

4.4.5 Action Planning and Approval

Nothing happens to manage risk purely because of completing a risk assessment. As such, action planning is a key step to:

- > Agree actions with the Risk and Control Owners, including the need for any ongoing independent verification activity (to verify that controls are performing as expected)
- > Develop/update any existing Risk Management Plan(s)
- > Develop an Implementation Plan, including any communication, change control or change management (as required)
- > Secure appropriate approvals for the risk assessment, risk management plan and implementation plan

The remainder of this section sets out the requirements for each of these activities.

Agree Actions

The Risk Facilitator should agree relevant actions with the Risk and Control Owners. They should also lead a discussion around the need for any ongoing independent verification of controls. **This is a requirement for all critical controls;** independent verification may also be provided for other controls, by exception and on the request of the Risk Owner. Further guidance on the role of the Verification Owner is provided in Section 10.1.

Develop/Update the Risk Management Plan

Outputs from the risk assessment should be formally incorporated into relevant existing risk management plans e.g. incorporate any changes to bushfire risk controls into the Bushfire Formal Safety Assessment and Bushfire

COMMERCIAL-IN-CONFIDENCE

Risk Management Plan. Changes affecting risks captured within the Corporate or Network Risk Registers should also be reflected in those artefacts.

If a Risk Management Plan does not already exist, then one should be created. This should be as simple and succinct as possible to capture:

- > the understanding of the risks derived from the risk assessment
- > details of the existing risk controls
- > details of any identified critical controls (see Section 9.2)
- > details of any agreed risk treatments
- > details of any agreed control verification activities

Develop Implementation Plan

The Implementation Plan should include necessary activities for communication, developing and deploying any required changes to existing controls or to introduce new treatments, change control and change management.

Outcomes from the risk assessment must be communicated to key stakeholders. Information that needs to be communicated includes:

- > residual risk ratings
- > the work that is needed to manage risk (key controls and treatments).
- > key residual uncertainties and critical assumptions underpinning the risk assessment.

It is important that those impacted by the risk assessment understand the limits of its applicability or validity and can recognise when the risk environment is departing from what was assumed in the original risk assessment.

Appropriate change control must be applied wherever the risk assessment requires changes to assets, the Asset Management System, or other Asset Management controls (see CEOP5047 – AM Change Control). This ensures that any changes to current network risk controls are made in a controlled manner.

Change management ensures any changes are successfully implemented and sustained within the business. Visit the EPMO Hub for further information on change management and access to templates on the Change Management Plan.

Approval

Approval authority for risks depends on:

- > Whether the risk is already captured within an existing approved corporate or network risk,
- > The residual risk level, and
- > The corporate risk appetite for different types of risk

The same variables also define the requirements for initial and ongoing reporting and risk reviews.

Advice on the appropriate approval authority for risk assessments should be sought from the Network Risk and Performance Team.

4.4.6 Worked Example

This worked example considers the situation where a type fault of a piece of asset equipment has been identified, with safety risks for workers in the event of a need to operate, and bushfire risk in the event of maloperation. The risk has been assessed as an Extreme/High safety risk and a High bushfire risk using the Network Risk Matrix; it has also been assessed as an having an unacceptable individual risk of fatality from quantitative analysis.

These residual risk levels require additional treatment to be considered (Ex/H residual risk).

The individual safety risk also requires immediate action to bring the risk into the tolerable region.

Assuming that the unacceptable individual risk has been sufficiently mitigated for the period necessary to implement longer term treatments, options have been identified as:

- > Option 1 – eliminate the risk through proactive replacement of existing assets with an alternative technology, as identified through an engineering study

COMMERCIAL-IN-CONFIDENCE

- > Option 2 – reduce the risk through engineering adaptation of the current assets, based on an existing industry practice solution
- > Option 3 – reduce the risk as per Option 2 plus provide additional training for field personnel, to enable them to better identify the fault in the field – noting that this would be required to be delivered before the upcoming bushfire season to be effective
- > Option 4 – reduce the risk as per Option 2 plus introduce a new work procedure, as recommended by an investigation
- > Option 5 – reduce the risk through the new work procedure referred to in Option 4 (but without the engineering adaptation)
- > Option 6 – introduce additional PPE, based on industry practice for dealing with the hazard now presented by this type of fault

From a UKOOA perspective, this is novel situation, with high risks. However, there is no indication of any risk trade-offs and economic implications are not significant. As such, it is categorised as a low-level 'Type B' decision:

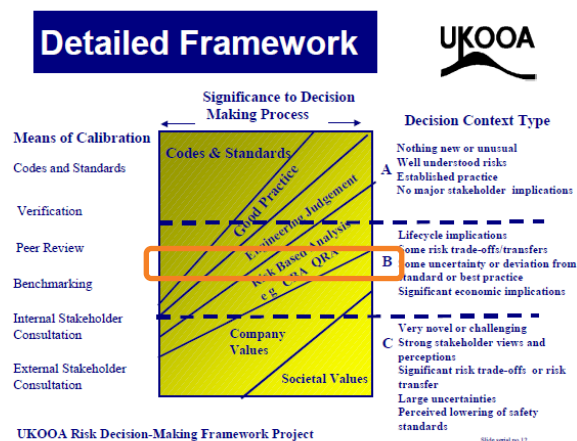


Figure 25: Type B decision in UKOOA framework

Table 13 shows the resultant options analysis. This demonstrates:

- > Progressive analysis of options through consideration of the hierarchy of control
- > Consideration of safety alongside other risks/objectives
- > Application of cost benefit analysis, using Disproportion Factors as a basis for assessment of reasonable practicability
- > Use of qualitative 'time and trouble' dimensions alongside quantitative costs in the cost-benefit analysis

From the options analysis, Option 4 is recommended, through comparison with industry practice, findings from investigations and cost-benefit analysis.

The next step is to verify, validate and calibrate this result, including:

- > verify correct application of the risk assessment process with the local Network Risk Champion (for Type B)
- > validate key sensitivities and uncertainties, particularly in the feasibility, assumed effectiveness, reliability and costs of the engineering solution
- > calibrate the forecast risk reduction and forecast improvement in control effectiveness through comparison with existing assets risk models, risk assessments and risk registers

If this confirms the results, next steps are as follows:

- > Risk Facilitator to obtain 'in principle' agreement of actions with relevant Treatment Owners
- > Risk Facilitator to update/create the Risk Management Plan
- > Risk Facilitator to develop an Implementation Plan – including communication, activities to develop and deploy any changes to existing controls or any new treatments, change control and change management (as required)

- > Risk Owner to review the above and send details of the risk assessment to the Network Risk and Performance Team for endorsement and advice on approvals, reporting and review requirements
- > Upon receipt of advice from the Network Risk and Performance Team, the Risk Owner obtains the appropriate approvals, then actions the recording, reporting, monitoring and review, as per the agreed Risk Management/Implementation Plan.

Toolkit

- Options Identification Checklist
- SFAIRP Checklist
- Implementation Plan Template

COMMERCIAL-IN-CONFIDENCE

Table 13: Options analysis

Option	Description	Hierarchy of Control (Level)	Monetised total risk reduction – excluding DF (collective safety + bushfire)	Monetised safety risk reduction – exclude g DF (collective safety risk)	Residual Individual Risk	Other Benefits	Risks	Cost (Quant)	Time + Trouble Costs (Reasonably Practicable (RP)?)	Total Cost Benefit Ratio (RP?)	Safety Cost Benefit Ratio (RP?)	Notes/Basis for SFAIRP Argument
1	Eliminate risk through proactive replacement of existing assets	1	\$100k	\$45k	7.5 x 10 ⁻⁷	Addresses findings from engineering study	-	\$1m	Time – M Trouble – M (Y)	10.0 (N)	22.9 (N)	Grossly disproportionate, evidenced by cost benefit ratio
2	Reduce risk through engineering adaptation	2	\$50k	\$32k	4.0 x 10 ⁻⁵	Aligns with industry practice	Engineering adaptation may shorten the life of connected components	\$100k	Time – M Trouble – L (Y)	2.0 (Y)	3.1 (Y)	Introduces industry standard engineering control which is reasonably practicable from cost benefit analysis; but lower risk, reasonably practicable options are available so not SFAIRP
3	Reduce risk through Option #2 + Training	2/3	\$66k	\$35k	3.0 x 10 ⁻⁵	-	Engineering adaptation may shorten the life of connected components	\$110k	Time – H Trouble – H (N)	1.67 (Y)	3.1 (Y)	Reasonably practicable by consideration of industry practice and cost benefit analysis; also the lowest risk option for safety. However 'Time' and 'Trouble' costs are not reasonably practicable for delivery before next bushfire season, therefore ruled out.
4	Reduce risk through Option #2 + new work procedure	2/3	\$60k	\$34k	3.5 x 10 ⁻⁵	Addresses findings from formal investigation	Engineering adaptation may shorten the life of connected components	\$105k	Time – M Trouble – L (Y)	1.75 (Y)	3.1 (Y)	Reasonably practicable by consideration of industry practice plus SME judgement. Incremental costs over Option 2 are also supported by cost benefit analysis. Considered SFAIRP option. Recommended.
5	Reduce risk through new work procedure	3	\$25k	\$23k	7.2 x 10 ⁻⁵	-	-	\$5k	Time – L Trouble – L (Y)	0.2 (Y)	0.2 (Y)	Reasonably practicable control, identified through SME consultation, that reduces risk below tolerable limit. However, other reasonably practicable controls are available from higher up the Hierarchy of Control, therefore not selected.

27 July 2022 – Original Issue

Approved By: Manager Network Risk & Performance

Next review date: July 2025

Page 55 of 77

COMMERCIAL-IN-CONFIDENCE**UNCONTROLLED COPY IF PRINTED**

COMMERCIAL-IN-CONFIDENCE

6	Reduce risk through additional PPE	3	\$16k	\$16k	9.5 x 10-5	Aligns with industry practice	-	\$6,500	Time – L Trouble – L (Y)	0.4 (Y)	0.4 (Y)	Lowest cost option to get risk below safety tolerability threshold and introduces an industry practice control. However, reasonably practicable controls are available from higher up the Hierarchy of Control, therefore not selected as SFAIRP solution. Will be implemented as immediate measure to manage risk until permanent solution is in place.
---	------------------------------------	---	-------	-------	------------	-------------------------------	---	---------	--------------------------------	------------	------------	--

5. Recording, Communicating and Reporting

Details of the risk assessment must be recorded, then communicated to key stakeholders. Risks must also be formally reported, including to ensure visibility of the ongoing status and delivery of agreed controls and treatments.

5.1 Records

Evidence of the work done to assess risks and identify and implement controls and treatments must be recorded.

Key information that should be captured includes:

- > Context for the risk assessment
- > Workshops completed and people who were involved, including their role
- > Methods used and why they were considered appropriate (including detailed documentation supporting any quantitative risk models developed to support the risk assessment)
- > Basis for the risk rating (e.g. choice of likelihood, consequence ratings)
- > Controls assumed plus their effectiveness (plus the basis for this rating)
- > Treatment options considered along with the supporting rationale for any treatments selected/discounted
- > Residual risk rating (if no additional or alternative treatments are identified)
- > Forecast risk rating (if additional or alternative treatments are identified)
- > Demonstration that residual/forecast risk is acceptable
- > Key underpinning information and data sources
- > Key assumptions, limitations, uncertainties and sensitivities
- > Clear identification of Risk and Control Owners
- > Evidence of agreed monitoring and review activities

Risks may be recorded in a [risk register](#), or in the [risk assessment template](#). All approved risk assessments should be submitted to the Network Risk and Performance Team by emailing them to networkrisk@essentialenergy.com.au.

5.2 Communication

The findings/outputs from risk assessments should be communicated to relevant stakeholders to ensure full transparency regarding risk exposure. This could include information about:

- > the residual risk level, including any critical risks
- > the effectiveness of current controls
- > key controls and treatments going forward, including any identified as critical
- > any limits, beyond which the risk assessment is no longer valid
- > any forecast risk or control effectiveness ratings and the expected timings for these e.g. identified controls/treatments are expected to maintain or reduce the current risk rating over the next 2 years.

Where a risk assessment relates to the scope of an existing FSA, the findings must also be communicated to the appropriate FSA owner.

Information regarding residual (critical) risks, required (critical) controls and treatments and key assumptions or factors affecting the validity of the risk assessment must be communicated through asset lifecycle stages of planning, design, construction, operation, maintenance and disposal.

5.3 Reporting

Reporting is a formal activity that provides visibility of risk exposure including through the delivery of agreed controls/treatments as per the agreed risk management plan. It helps answer the questions: *Are we doing what we said? Is it working? Has anything new come to light that changes the risk exposure?*

Reporting should be tailored to the audience, including:

- > Senior or line management
- > Other Risk or Control Owners

Risk information must also be reported to the Network Risk and Performance Team, who are responsible for centralised risk reporting. As a minimum, it is expected that reporting will include the findings from monitoring activity that indicates:

- > Risk status
- > Control status
- > Treatment status
- > Changes to the risk environment that affect the validity of the risk assessment

The Risk Owner must also report the completion of any risk reviews, as per agreed triggers.

Toolkit

- [Reporting Form](#)
- [NRM Guide: Communicating, monitoring and reporting risks](#)

6. Implementation of Risk Controls and Treatments

Actions described in the risk management plan must be implemented in line with agreed timeframes (see Section 4.4.5). The Risk Owner should maintain oversight of the implementation status of the risk management plan and act if they identify material deviation from the plan. This could include formal review and/or change control of the plan (subject to further risk assessment), or actions to correct deviations from the original plan.

7. Monitor and Review

The outcomes of a risk assessment require ongoing monitoring, review and adjustment to respond to changes and continuously improve the risk and control environment. This section focuses on approaches for performing ongoing monitoring and review activities.

Table 14 summarises the actions required by a Risk Owner based on the outcomes of a risk assessment, which should be defined as part of agreeing risk management plans (see Section 4.4.5). Function owners (or Level 3 managers reporting to the Chief Operating Officer) require visibility of key risk and control information including the implementation status of actions agreed as part of risk management plans.

Table 14: Risk Owner Actions following a Risk Assessment

IF the Residual Risk is	AND the Board Risk appetite is	THEN, the Risk Owner		
		Reviews	Escalates	Monitors and Reports
Extreme	Any	Review and endorse the adequacy of current controls and oversee implementation of interim controls or treatments.	Immediate escalation of critical and non-critical risks to the Function Owner and Executive.	Actions should be monitored and reported to the Function Owner and Executive. Reassess at least six monthly.

High	Any	Review the adequacy of current controls and consider any interim controls or treatments required.	Routine escalation of critical and non-critical risks to the Function Owner.	Any actions should be monitored and reported to the Function Owner. Reassess at least annually.
Medium	Low or Very Low ¹	Review the adequacy of current controls and consider any interim controls or treatments required.	Routine escalation of critical risks to the Function Owner.	Any actions should be monitored and reported to the Function Owner.
	Moderate	Note any new/escalating risks and provide feedback or insights as appropriate.	Optional escalation of risks that are new and/or changing fast/unexpectedly.	Reassess at least every two years.
Low	Low or Very Low ¹	Nil.	No requirement to escalate.	Reassess at least every three years.
	Moderate	Nil.	No requirement to escalate.	

¹Per CECP0002.03 Board Risk Policy; Safety, Bushfire, Environment, Compliance, Reputation and People.

Ongoing monitoring and review activities must include re-assessing the risks (in accordance with the frequency outlined in Table 14) and verifying the effectiveness of **critical** controls (in accordance with the frequency determined by the critical control owner, see NRM Guide – Critical Risks and Controls).

7.1 Environmental Scanning

Environment scanning is a technique for detecting early signs of threats and opportunities, including emerging technologies. The Risk Owner should periodically (annually for FSA owners) monitor the internal and external risk and control environment for changes that may impact the validity of the risk assessment outcomes. An environmental scan may consider several time horizons, including within the year, 1-5 years and 6-10 years.

Reviewing the internal risk and control environment may include coverage of:

- > Adequacy of risk management methods used to understand the risk and design the system of control
- > Deficiencies, or potential improvements in local practices
- > Interdependencies and goal conflicts; including controls that may be working in conflict with each other
- > New or emerging risks and / or treatment options
- > Relevant findings from internal reviews, risk assessments and investigations
- > Loss event or near miss data

Reviewing the external risk and control environment may be performed in accordance with the PESTLE (Political, Economic, Social, Technological, Legal/Regulatory and Environmental) framework (see Section 2.4).

A summary of the outcomes should be recorded, including any actions arising from the environmental scan. Where material changes are identified, timely notification should be provided to line management and the Network Risk and Performance team.

Toolkit

- [PESTLE Template](#)
- [NRM Guide: Critical risks and controls](#)
- [NRM Guide: Communicating, monitoring and reporting risks](#)
- [Network Critical Control Verification Tool](#)

8. Specific Requirements for Formal Safety Assessment

All decisions that materially affect the safety of the network (or safety risks arising from the network) must be supported by an FSA that complies with Section 4.3.2 and Appendix A of AS5577.

AS5577 specifically requires an FSA for activities related to:

- > Network planning
- > Network safety management, including decisions taken around the management of:
 - Network structural integrity
 - External interference management
 - Fault condition monitoring and response
 - Changes of operating conditions and remaining asset life review
- > Site safety management
- > Substation operation and maintenance
- > Emergency response

Other specific requirements include:

- > **Risk identification:** As a minimum, FSAs need to consider:
 - External hazards and natural disasters
 - Intentional and unintentional human activities
 - Safety related aspects of loss of supply
 - Electrical work on or near network assets
 - Other activities that may involve electrical hazards, including work being carried out in the vicinity of electrical assets
 - The design of network assets and the condition and operating methodologies for electricity network assets
 - Single and multiple failure modes, including knock-on effects as appropriate
- > **Risk analysis:** An FSA must analyse the risks associated with all identified hazards, taking due account of relevant electricity industry data and evidence as well as the following requirements:
 - Specifically consider consequences to the network workforce, the public, other stakeholders, and safety related environmental impacts. This must include consideration of consequences that are reasonably foreseeable as well as those that have occurred in previous known events.
 - Likelihood of defined consequences to be analysed regarding the Network Operator's and electricity industry's relevant information on historical fault frequencies and the level of exposure of persons to the hazard

AS5577 specifically requires an estimation of the residual risks associated with a hazard.

- > **Risk evaluation:** Where an evaluation of risks against safety risk acceptance criteria identifies that a residual risk is not acceptable, an FSA must apply treatment or controls, which may include redesign or relocation of network assets, until an acceptable risk level is achieved.
- > **Risk treatment:** Requirement to eliminate SFAIRP or where elimination is not reasonably practicable, to reduce ALARP. Requirement to demonstrate an exhaustive search for practicable control/treatment options and record all treatment options, even if the risk is SFAIRP. Controls and/or treatments must be considered in accordance with the hierarchy of control. Control measures must be incorporated into appropriate procedures.

9. Key Concepts

9.1 Information Sources to Support Network Risk Management

Information to support risk management comes primarily from two source types:

- > **Data** – including internal and external sources e.g. written reports of events, research, forecasts etc
- > **SME judgement** – including via formal expert elicitation techniques

Either source can be used to feed into the direct estimation of specific parameters (e.g. frequency of a defined loss of control event per annum, with the current system of control in place), or into models (including engineering failure models, event trees).

For safety risk, it is a requirement to consider relevant industry data and evidence, relating to:

- > the possible consequences of a hazard, 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 those that have occurred in previous known events.
- > the likelihood of these consequences occurring, having regard to relevant industry information on historical fault frequencies and the level of exposure of persons to the hazard.

Whichever information source is used, it is important that information sources are appropriate and formal, including corporate/validated datasets and suitably qualified and experienced SMEs. Further detail on current formal data sources is provided via the [Network Risk Management SharePoint site](#).

When sourcing data, care is needed to ensure sufficient history to identify or avoid anomalies e.g. driven by different risk controls or due to known external factors such as extreme weather conditions in a certain year.

Expert elicitation techniques must also make reasonable efforts to avoid foreseeable heuristics and biases (see Section 9.13)

In situations where directly relevant data is not available and/or SMEs are not confident that they can make a sufficiently accurate estimate for specific risk parameters, hypothetical values reflecting what various parameters would need to be to support a particular outcome can be estimated. Appropriate SMEs can then be asked whether these estimates (or simultaneous combinations of estimates) are credible, or under what circumstances they might become credible, to substantiate a particular decision.

Several general guidance tools are provided in Appendices A, C and D for:

- > Estimating the subjective probability or chance of a condition or risk event occurring, based on SME judgement (Appendix A)
- > Estimating population characteristics from statistical samples (Appendix C)
- > Estimating the likelihood of failures or consequences when zero events have been observed to date (Appendix D)

9.2 Critical Controls

Section 2.3.4.5 of the Corporate Risk Management Procedure defines a critical control as a control that plays a significant role in preventing or mitigating a critical risk (which is defined as any risk event with a residual consequence rating of severe). The following are *indicators* that a control may be a critical control. This is not an absolute (yes/no) standard. All items are indicators of criticality, the more present, the higher the indication.

- > The control is crucial to preventing or mitigating one or more severe consequence events.
- > The control's absence or failure would significantly increase the likelihood of one or more severe consequence events occurring, despite the existence of other controls.
- > The control's absence or failure would result in the residual risk rating being outside the Board's risk appetite.

9.3 Consequence Scenarios

There are countless ways in which risks can materialise. To make risk assessments manageable, they are often structured around a limited set of consequence scenarios:

- > **Most likely foreseeable** – the most likely or most frequent consequence rating e.g. if the defined risk event occurred 100 times, what would be the most frequent outcome?
- > **Plausible worst case** – the highest severity (but still credible) consequence rating for the defined risk event
- > **Expected value** – considers a range of possible outcomes, with appropriate likelihoods attached to each e.g. 10% chance of insignificant consequence, 20% of minor, 40% chance of moderate, 25% chance of major, 5% chance of severe.

Wherever practicable, qualitative risk assessments should consider the ‘most likely foreseeable’ and ‘plausible worst case’ consequences. This is because the higher likelihood of the most likely foreseeable consequence can result in a higher risk rating than for the lower likelihood plausible worst-case consequence.

The ‘expected value’ method is generally only practical when undertaking quantitative risk analysis. For simplicity, this method may also be applied using a subset of consequence ratings e.g. considering only the likelihood of a severe, moderate or insignificant consequence.

9.4 Network Fatal Risks and Operational Safety Risks

The Essential Energy HSE Risk Management Manual defines a suite of Network Fatal Risks and Operational Risks. Network Fatal Risks are risks that have the potential to result in loss of life or life changing injury. Operational Safety Risks are risks that are not considered fatal but expose workers to injury or expose the environment to potential impact.

While Network Fatal Risks and Operational Risks are defined for Essential Energy workers, the generic risk events that they describe can also be considered for members of the public.

The list of Network Fatal Risks can be accessed via the following link to the Safety SharePoint Site: [Network Fatal Risks - Rules We Live By](#).

9.5 Units/Measures of Safety Risk

Measures of safety risk include:

- > Individual Risk (individual risk of fatality per annum)
- > Collective Risk (statistical total number of fatalities and/or injuries over a period - usually per annum)
- > Societal Risk (risk of multiple fatalities per annum)

Individual risk is calculated with reference to the ‘hypothetical most exposed person’. It is the frequency or probability of a specific individual being killed per annum, because of a specific hazard, activity or facility. This is the measure of safety risk required for comparison with the safety tolerability criteria defined in Section 2.6.3.

This can be a complex calculation. It is a mature concept that is not required to be used in every risk assessment but will be important wherever a quantitative sense check or demonstration of safety risk tolerability is required.

Detailed guidance on the [Network Risk Management SharePoint site](#) will include guidance on calculating the individual risk value from first principles, as well as simplifying generic assumptions for use when calculating with respect to linear or point assets.

The **collective risk** calculation is a measure of the total risk posed to a defined population exposed to a specific hazard, activity or facility e.g. 0.78 fatalities per annum.

The calculation of collective can make use of the concept of ‘Fatalities and Weighted Injuries’, wherein injuries can be considered as a statistical proportion of a fatality to feed into risk aggregation calculations. Table 15 sets out the definition of Fatalities and Weighted Injuries, based on the Essential Energy Corporate Risk Matrix and monetisation principles set out in the Value Framework:

Table 15: Fatalities and Weighted Injuries

Category	Insignificant	Minor	Moderate	Major	Severe
Description	Injury or symptoms with reversible effects, requiring first aid only.	Injury or illness with reversible effects, requiring medical treatment or ongoing medical monitoring.	Injury or illness with reversible effects, requiring hospitalisation, or resulting in inability to work for multiple days (for more than one full shift).	Permanent injury, illness or impairment (other than total and permanent disability or fatality).	Total and permanent disability or fatality.
Suggested number of injuries equivalent to a fatality	7,000	1,000	200	10	1

Societal risk is the measure used to describe risk events that could result in multiple fatalities. While not widely used in the context of electricity networks, they are described here for background understanding. Indicative criteria are available from NSW Government in form of risk criteria for land use planning²¹. These are provided in Section 2.6.4 for reference.

9.6 Societal Concern

The concept of societal concern deals with factors that influence the perception of risk, which can then impact society's tolerance for a particular risk, as well as expectations around the level of effort expended to manage that risk.

Factors affecting societal concern can include the:

- > Level of knowledge of the risk (by those exposed and by science as a whole).
- > Voluntariness and equity of exposure to the risk
- > Immediacy of the effects; likelihood of chronic-catastrophic consequences and/or 'dread' factor e.g. related to the risk of cancer
- > Level of trust in those responsible for controlling the risk

An understanding of societal concern should sit alongside the statistical evidence describing a particular risk e.g. from the combination of the likelihood and consequences of the risk, to also consider the response in terms of the nature of the risk.

Societal concern should be considered when setting the tolerability limits for a risk (see Section 2.6.3).

The impact of societal concern on the 'level of effort expended to manage a risk' is addressed through application of the Disproportion Factors set out in the Value Framework. In instances where the Value Framework is not applied, societal concern should be considered qualitatively within the Risk Evaluation and Treatment step of the risk assessment (see Section 4.4).

9.7 Risk Monetisation

Consequences of risk events can be monetised using the Network Value Framework (CECG1140). This uses money as a common unit of risk, to enable logical aggregation of risks as well as direct comparisons and trade-offs across different risk types.

²¹ <https://www.planning.nsw.gov.au/-/media/Files/DPE/Other/hazardous-industry-planning-advisory-paper-no-4-risk-criteria-for-land-use-safety-planning-2011-01.pdf?la=en>

Communication or reporting of monetised risk should generally include any relevant Disproportion Factors from the Value Framework. This is to ensure that reported levels of monetised risk reflect the full 'value' that is placed on that risk, including from Essential Energy as well as from society and other key stakeholders.

9.8 Dynamic Risk Assessment

Most concepts described in this document are intended to be applied in a planned situation, over a period of days, if not weeks. However, there will be occasions when a risk assessment is required in a very short amount of time, either on-the-spot, or within a few hours.

In these situations, a 'dynamic' risk assessment approach should be used as follows:

- > Gather the minimum people necessary to identify the material risks, controls and treatment options
- > Allocate a facilitator to run the session
- > Run through an accelerated version of the risk assessment process, identifying the context, material risks to be managed, controls and control weaknesses and/or options for additional or alternative treatments
- > Explicitly pose the question: what more could we do and why wouldn't we do it?
- > Consider qualitative (at least) benefits, risk and costs of the different options
- > Document the discussion and rationale for the final decision

The target duration for this activity should be around two hours. The Network Risk and Performance team will be available to assist and facilitate this process.

If the resultant solution is permanent or required for the long term, or relates to a material risk, the outputs should be validated as soon as practicable and controls/treatments adjusted as required, based on the findings from the validation exercise.

9.9 SFAIRP and ALARP

Section 4.4.3 includes content taken directly from AS5577 that refers to the concept of reducing risks 'as low as reasonably practicable' (ALARP).

Whilst some sources assert that the requirements of SFAIRP and ALARP are fundamentally different, within Essential Energy they are considered equivalent, in that they both establish requirements to implement risk controls or treatments to the extent that doing more to manage a risk would not be reasonably practicable.

This is deemed appropriate on the basis that:

1. The UK Health and Safety Executive (HSE) explicitly addresses this point in their "*ALARP at a glance*"²² guidance. This states that: "*ALARP*" is short "or "as low as reasonably practicable". "*SFAIRP*" is short for "so far as is reasonably practicable". **The two terms mean essentially the same thing and at their core is the concept of "reasonably practicable"; this involves weighing a risk against the trouble, time and money needed to control it.**" The only exception to this, where the two terms cannot be used interchangeably, is when referring to the concept in the context of a specific requirement of an Act, Regulation or other formal requirement. For example, when formally demonstrating that a specific requirement of a Regulation or standard has been met, then the same term (SFAIRP or ALARP) must be used.
2. The UK HSE are considered an authoritative source in this matter as they were instrumental in developing guidance around the detail and application of the SFAIRP and ALARP concepts
3. The UK context is deemed relevant by reference to discussion of the origins and application of the ALARP concept in Appendix B of AS5577
4. There is no equivalent authoritative advice on the subject from Australian regulators.

²² Available at:

<https://www.hse.gov.uk/managing/theory/alarplance.htm#:~:text=%22ALARP%22%20is%20short%20for%20%22,money%20needed%20to%20control%20it.>

9.10 Removing or Relaxing Current Risk Controls

Removing or relaxing current risk controls is both allowable and necessary in certain circumstances to ensure that risks are managed SFAIRP. This is sometimes referred to as 'reverse ALARP' when used in a safety context.

Removing or relaxing safety controls should only be considered when the baseline risk is low and:

- > there is updated risk information or understanding that demonstrates the risk is lower than originally thought and controls are now demonstrably grossly disproportionate, or
- > other layers of control have been introduced, reducing the need for or effectiveness of certain controls, or
- > equipment or parts have become obsolete or too expensive/difficult to obtain, such that they are no longer reasonably practicable, or
- > multiple controls have been identified as a source of 'safety clutter' that is having a detrimental effect e.g. due to complexity or confusion, as identified through formal investigation methods.

In addition to the above conditions, care must be taken when removing or relaxing any existing controls to understand any associated risk transfer. Safety risks must not be transferred from an exposed group with lower risk to a group experiencing higher risk.

A further consideration in removing or relaxing any existing risk controls is to ensure that this does not adversely affect any controls relating to compliance or cyber security requirements.

Any decision to remove or scale back an existing safety control must be subject to comprehensive risk assessment before the change takes place.

Controls may only be removed or reduced following consultation with impacted stakeholders, including the Risk and Control owners and an appropriate risk assessment completed and approved.

9.11 Documenting the SFAIRP Demonstration

The SFAIRP demonstration is a critical artefact that needs to provide a succinct and clear argument as to why the proposed risk controls and/or treatments are deemed sufficient to manage risk so far as is reasonably practicable. For safety risks, this must clearly answer the questions:

- > What more could we have done?
- > Why haven't we done it?

The SFAIRP demonstration must then clearly substantiate the claim that to do 'more' would be grossly disproportionate.

This should be a clearly labelled and stand-alone section of the final risk assessment.

Complex risk assessments may choose to document the SFAIRP demonstration using Goal Structuring Notation (GSN). This is a graphical method more commonly used to support safety cases and to demonstrate how safety or broader performance or risk management goals will be achieved. Further guidance on the [GSN technique](#) is available on the [Network Risk Management SharePoint site](#).

9.12 Taking Account of Uncertainty and Limitations in Available Information

When undertaking risk assessment it is important to take appropriate account of uncertainty and limitations in the underpinning data, information and assumptions.

Uncertainty and sensitivity analysis techniques can be used to obtain confidence estimates for measures of risk and to identify key parameters that have a significant influence over results.

As a simple approach, input variables can be systematically varied by a set amount e.g. +/-10% or 20%, to understand the effect on the risk estimate or final decision.

Alternatively, probabilistic simulation methods can be used e.g. Monte Carlo Analysis, to define a probability estimate for the risk estimate, including the P10, P50 and/or P90 estimates (showing the outcomes with a 10%, 50% and 90% likelihood of occurrence, respectively).

COMMERCIAL-IN-CONFIDENCE

Where sensitivity analysis indicates that results are particularly sensitive to a parameter that is known to be highly uncertain, this can be used to indicate the need to reduce the uncertainty in that variable. Alternatively, it could be used to accept the current uncertainty in a variable that has very little impact on the results of the analysis.

In addition, it is important that results from any risk analysis or risk assessment are presented and used appropriately. For example:

- > present uncertain results as rounded figures, or as falling within a band instead of to 4 decimal places, where underpinning data does not support this level of accuracy (spurious accuracy)
- > do not rule out an option that has a cost-benefit ratio of 1.01 where there are known uncertainties in the underpinning data that is likely to limit the accuracy of the cost and benefit estimates to +/- 10%

9.13 Human and Cultural Factors

Human and cultural factors are systemic issues that will affect the effectiveness of risk controls or treatments, typically through the physical or behavioural interactions between human beings and the control, treatment or risk.

For purpose of network risk management, key considerations include:

- > taking account of **heuristics and biases** that affect SME estimates for risk parameters.
- > consideration of **human error and usability** in the design of risk controls e.g. using techniques such as the HEART method and Usability Mapping
- > understanding and accounting for the impacts of **human behaviour** on the effectiveness of risk treatments (including new or altered controls); anticipating how people will respond once new controls are implemented, including members of the public.

The purpose of including consideration of human and cultural factors is to optimise the overall performance of the 'system of control' associated with a particular risk.

9.14 Opportunities

A key part of asset management and network risk management is managing opportunities. While not explicitly defined in the Essential Energy corporate or network risk frameworks, if required, opportunities should be assessed using a conceptual mirror-image of corporate/network risk matrices.

9.15 Escalators

Escalators are factors that affect:

- > the likelihood of a risk event occurring e.g. a particularly bad fire or storm season, with more extreme/frequent fire or storm conditions.
- > the likelihood of a high-consequence scenario following a risk event e.g. occurrence of concurrent or widespread risk events that have a material effect on any incident response, either by Essential Energy, or by external agencies.

Escalators can be driven by internal or external factors; they may also be short-term and long-term in nature.

Climate change is a key escalator that needs to be considered within any long-term risk assessment. A generalised approach to climate change modelling has yet to be defined by the business. Until this is developed, any risk assessments linked to long term decisions that may be affected by climate change should involve the Network Risk and Performance team, to ensure that latest available methods or assumptions for climate change impacts are incorporated.

10. Authorities, Responsibilities and Resources

Management and reporting of network risk is the responsibility of **everyone**. This includes all Essential Energy staff plus contractors working on behalf of Essential Energy. It is everyone's responsibility to participate in the identification, assessment, treatment and monitoring, review and communication of risks, including current and new/emerging risks to and from the network. No one person can know everything about a risk; risk management is a team effort, requiring regular and open communication and feedback to make the best use of the collective knowledge of the organisation and key stakeholders.

10.1 Authorities and Responsibilities

Table 20 includes authorities and responsibilities for the management of risks which may be delegated as required:

Table 16: Authorities and Responsibilities

Position / Title	Responsibility
Manager Network Risk and Performance	<ul style="list-style-type: none"> • Maintenance of CEOP1141 and supporting artefacts • SME support to implement CEOP1141 • Govern and assure the appropriate implementation of CEOP1141 • Periodic formal review and improvement of CEOP1141 • Advice of approval requirements for risk assessments
All Managers	<ul style="list-style-type: none"> • Ensure appropriate team members receive training in CEOP1141 • Ensure CEOP1141 is applied where required, and by competent persons • Ensure that they maintain oversight of the status of risks within their area(s) of accountability • Ensure that new or emerging risks identified by their teams are appropriately reported
All employees and contractors	<ul style="list-style-type: none"> • Apply this manual, as appropriate • Actively monitor/manage risks, controls and/or treatments assigned to them • Report new or emerging risks
Risk Owners	<ul style="list-style-type: none"> • Ensure risks are managed in accordance with this procedure • Co-ordinate/perform risk assessments • Endorse risk assessments, including risk events, risk ratings, SFAIRP status, control/treatment actions and key risk indicators • Maintain oversight of the delivery status of the risk management plan; take action to correct any material deviations from the agreed plan • Escalate any issues that have the potential to invalidate the risk assessment • For persistent risks, undertake regular scanning of the risk environment to identify any changes that could trigger a formal risk review
Risk Facilitators	<ul style="list-style-type: none"> • Confirm the nature/category of the risk assessment to be undertaken • Facilitate risk assessments that fall within their level of training/competency • Ensure the risk assessment is appropriately recorded
Control Owners	<ul style="list-style-type: none"> • Ensure the control is designed, implemented and operated effectively • Ensure treatment action plans are implemented as planned • For critical controls, assign a Verification Owner and ensure this person undertakes Verification activities – see below. • Review assessment provided by Verification Owner and in the event of a discrepancy, see Risk Owner.
Verification Owner	<ul style="list-style-type: none"> • Independent assessment of the design, implementation and operating effectiveness of critical controls (plus other controls as required) • Submit verification summary report to the Control Owner and Risk Owner

COMMERCIAL-IN-CONFIDENCE

(Required for all critical controls, plus other controls by exception)	
Risk Champions	<ul style="list-style-type: none"> • Facilitate complex risk assessments • Ensure the risk assessment is appropriately recorded • Advice and support to implement network risk management process

10.2 Resources

Key resources supporting the implementation of this manual include:

- > key contacts in the Network Risk and Performance Team,
- > a network of Risk Champions,
- > training and awareness resources, and
- > various tools and templates, as listed in the various 'Toolkit' sections of this manual.

The details on how to access these resources are provided via the [Network Risk Management SharePoint site](#).

11. Manual Implementation, Review and Improvement

This manual applies from the date of publication. It is not to be applied retrospectively to any risk assessments completed prior to the publication date.

The manual will be reviewed every 3 years, or sooner if required by changes to the Corporate Risk Management Policy or Framework, or from some other event e.g. a formal audit or investigation.

Any opportunities for improvement to this manual should be submitted to the Network Risk and Performance Team via the [Network Risk Management SharePoint site](#).

12. Additional Guidance

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

- Appendix A – Subjective Probability Estimates
- Appendix B – Generalised Asset Failure Curves
- Appendix C – Statistical Confidence and Sample Sizes
- Appendix D – Approach When Zero Events Have Been Observed
- Appendix E – Common Assumptions For Use in Quantitative Risk Analysis
- Appendix F – Useful References
- Appendix G – Glossary of Terms

Appendix A – Subjective Probability Estimates

When data is not available, or a specific risk assessment does not require or allow time for extensive data extraction, probability estimates may be sourced from suitably competent SMEs. This includes appropriately qualified and experienced SMEs relevant to the subject of the risk assessment.

The following guide can be used to aid with this process, ensuring a consistent approach to estimating subjective probabilities.

Table 17: Subjective probability estimates

Description of Condition or Event	Order of Magnitude Probability (or Chance) Assigned
The condition or event is virtually certain to occur due to known physical processes and conditions that can be described and specified with almost complete confidence	0.99 (or 99%, or 99/100)
The condition or event is considered very likely to occur, although not completely certain	0.9 (or 90%, or 9/10)
The condition or event is considered equally likely; there is no reason to believe that occurrence is more or less likely than not	0.5 (50%, or 1/2)
Occurrences of the condition or event are observed in the available database	0.1 (or 10%, or 1/10)
The occurrence of the condition or event is not observed or is observed in one isolated instance in the available database. However, several potential failure scenarios can be identified.	0.01 (or 1%, or 1/100)
The occurrence of the condition or event is not observed in the available database. It is difficult to think about any plausible failure scenario. However, a single scenario could be identified after considerable effort.	0.001 (or 0.1%, or 1/1,000)
The condition or event has not been observed and no plausible scenario could be identified, even after considerable effort	0.0001 (or 0.01%, or 1/10,000)

These definitions should be used as a guide only; probability estimates can be interpolated between descriptions provided in the table.

Appendix B – Generalised Asset Failure Curves

Future probabilities of asset failures can be estimated using a curve which relates probability of failure to age or condition. Figure 26 sets out several 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

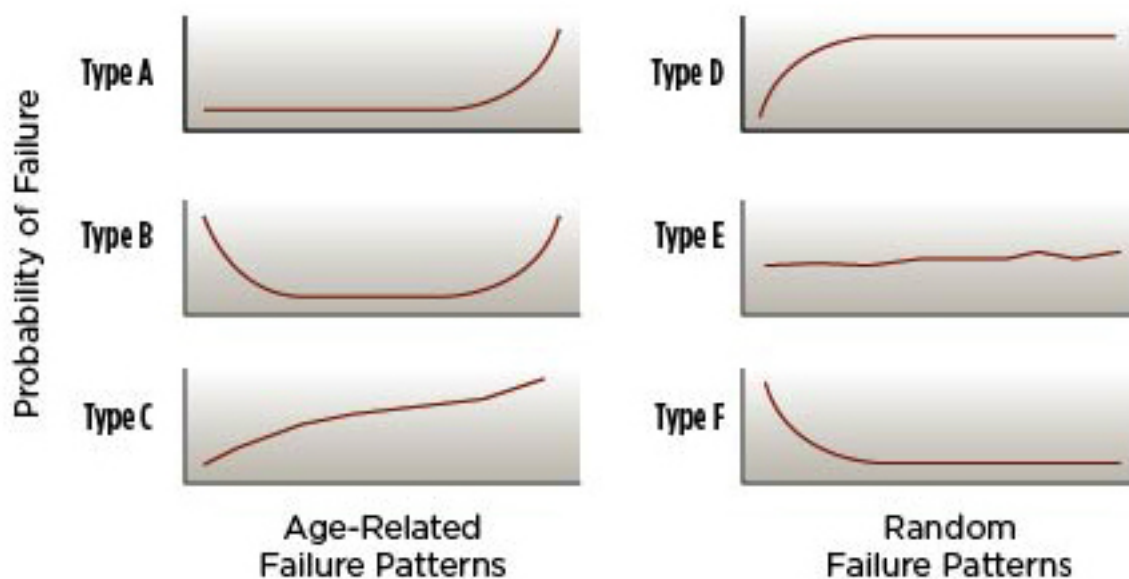


Figure 26: Asset failure patterns²³

²³ <http://www.plantservices.com/articles/2011/09-asset-manager-understanding-asset-failure/>

Appendix C – Statistical Confidence and Sample Sizes

Making risk management 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 required confidence in the resulting estimates. Sample-size calculators can be readily sourced from the internet. An example published by the Australian Bureau of Statistics can be found at: <https://www.abs.gov.au/websitedbs/d3310114.nsf/home/sample+size+calculator>

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 were 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 were 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 Three²⁴

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 × 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:

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

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

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

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

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

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.

²⁴ Evidence-Based Diagnosis, Thomas B. Newman, Michael A. Kohn

Appendix E – Common Assumptions For Use in Quantitative Risk Analysis

This appendix lists a range of common assumptions required to undertake quantitative risk analysis. Where relevant to a specific risk analysis, these should be used to ensure a consistent approach across the business.

Table 18: Common assumptions for quantitative risk analysis

Assumption	Value	Basis
Average walking speed	1.4 m/s	Preferred walking speed of normal-weight adults ²⁵
Hours of network exposure per day	14 hrs	6 am – 8pm
Average people entering asset exposure radius (urban)	2 pp / hr	Equivalent to 112 pp / square km spending 2 hrs outside / day
Average people entering asset exposure radius (rural)	0.1 pp / hr	Equivalent to 2 pp / square km 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

²⁵ 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 – CECF0002

Board Policy (Governance) – Compliance – CECF0002.02

Board Policy (Governance) - Risk Management - CECF0002.03

Company Procedure (Governance) - Risk Management - CEOP0002.21

Annexure A – Board Charter and Board Committee Charters – Board Policy (Governance) – Governance – CECF0002

Health Safety and Environmental Manual Risk Management - CECM1000.02

Network Value Framework – CECG1140

External

AS / NZS / ISO 31000 – 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 Electricity 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

Reducing Risks, Protecting People [<https://www.hse.gov.uk/managing/theory/r2p2.pdf>]

Appendix G – Glossary of Terms

Where applicable, definitions are consistent with AS/ NZS / ISO 31000:2018 – 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 effects²⁶.

Control

Measures that modify risk. Controls may 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.

Escalator

Escalators are factors that affect the likelihood of a risk event occurring, or the likelihood of a high-consequence scenario following a risk event.

Forecast Risk

A ‘forecast’ risk level is the risk level that is expected to be reached once a defined treatment is implemented.

Hazard

Something with the potential to cause harm (i.e. loss or damage).

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.

²⁶ ISO Guide 73:2009 - Risk Management vocabulary

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 period)²⁷.

Operational risk

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

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.

Opportunity

An uncertain event that, if it occurs, would have a positive effect on achievement of objectives

Residual risk

The risk remaining after the present level of risk treatment, considering 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 event

An event or occurrence that could give risk to one or more consequences

Risk management

Coordinated activities to direct and control the company regarding risk.

Risk source

An element with the potential to give rise to a risk

Threat

An uncertain event that, if it occurs, would have a negative effect on achievement of objectives

Treatment

The development and implementation of additional or alternative measures to modify risk

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

²⁷ ISO Guide 73:2009 - Risk Management vocabulary

COMMERCIAL-IN-CONFIDENCE

(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.

Value

Defined as the net benefit of risk controls/treatments, minus the cost of those measures. Define in the Value Framework as:

Value =	Net Benefit							minus	Cost
	Advantage			less	Disadvantage				Direct Costs
	Direct Benefits	plus	Risk Mitigation		Direct Detriment	plus	Introduced Risk		CAPEX and OPEX