



Part of Energy Queensland

Network Risk Framework

CONTENTS

1	PURPOSE AND SCOPE.....	4
2	DEFINITIONS, ABBREVIATIONS AND ACRONYMS	5
2.1	Definitions	5
3	REFERENCES	11
3.1	Legislation, regulations, rules, and codes.....	11
3.2	Energy Queensland controlled documents.....	11
3.3	Other sources	11
4	ENQUIRIES REGARDING THIS DOCUMENT	12
5	FRAMEWORK HIERARCHY	12
5.1	Network Risk Framework	12
5.2	Network Risk Evaluation Matrices	13
6	APPLICATION	14
7	ALIGNMENT TO AS ISO 31000.....	15
8	CONDUCTING A NETWORK RISK ASSESSMENT	16
9	ESTABLISHING THE CONTEXT	17
10	RISK ASSESSMENT	17
10.1	Qualitative.....	17
10.2	Semi-Quantitative	18
10.3	Quantitative.....	18
11	RISK IDENTIFICATION.....	19
11.1	Choosing a consequence.....	19
12	RISK ANALYSIS	19
12.1	Develop Risk Scenario.....	19
12.2	Assessing Likelihood.....	22
12.3	Risk Analysis and Impact of Controls	22
12.4	Control Effectiveness	23
13	RISK EVALUATION (INCLUDING RISK TOLERABILITY)	24
14	RISK TREATMENT	25
15	COMMUNICATION AND CONSULTATION	27
15.1	Roles and Responsibilities	27
16	RISK RECORDING, MONITORING AND REVIEW	28
16.1	Required Documentation	28
16.2	Measurement	29
16.3	Periodic Review	29

Network Risk Framework



Annex A	NETWORK RISK EVALUATION MATRICES	30
A.1	Legislated Requirements.....	30
A.2	Customer Impact	31
A.3	Business Impact	32
A.4	Network Risk Likelihood Scale	34
A.5	Safety Consequence Scale	35
A.6	Safety Likelihood Scale	36
A.7	Environment Consequence Scale	37
A.8	Environment Likelihood Scale	40
Annex B	NETWORK RISK PROCESS FLOWCHART	42
Annex C	NETWORK RISK EVENT TREE EXAMPLES	43
Annex D	SAMPLE BOW TIE/ THREAT BARRIER DIAGRAM	45
Annex E	RISK ASSESSMENT RECORD (SEMI-QUANTITATIVE)	46
Annex F	SIMPLE RISK ASSESSMENT TEMPLATE	47
Appendix A	48
Document History	48
A.1	Revision History	48
A.2	Document Approvals	49

FIGURES

Figure 1: EQL Enterprise Risk Management	12
Figure 2: EQL Enterprise Risk Categories	13
Figure 3: Risk Management Process	15
Figure 4: Structure of an Event Tree	20
Figure 5: Example Fault Tree Structure	21
Figure 6: Risk Assessment Multiplication Matrix	23
Figure 7: A Risk Tolerability Scale for evaluating Semi-Quantitative risk scores	24
Figure 8: Risk Treatment and Control Hierarchy	26

TABLES

Table 1: Risk Treatment Hierarchy by order of most preferred (based on WH&S approach).....	23
Table 2: Record Repositories.....	29

EQUATIONS

Equation 1: Semi-Quantitative Risk.....	18
Equation 2: Quantitative Risk Cost.....	18
Equation 3: Semi Quantitative Risk	23

1 PURPOSE AND SCOPE

The purpose of this Network Risk Framework is to supplement Energy Queensland's enterprise risk management approach by providing additional guidance when undertaking specialised/ technical risk assessments.

It seeks to:

- explain the process of conducting a network risk assessment
- ensure consistency of application of the network risk assessment process
- enable network risks to be considered and addressed on a priority basis.

This framework supports the overarching principles of effective risk management whereby it:

- facilitates continual improvement
- is systematic, dynamic, and responsive to change
- explicitly addresses uncertainty
- provides a rigorous basis for decision making leading to pro-active rather than re-active decisions
- provides better identification of opportunities and the associated risks
- leads to more effective allocation and use of resources.

This *Network Risk Framework* applies to all staff that are required to assess a risk or limitation associated with the Ergon Energy or Energex networks within the Energy Queensland Group. This includes safety and environment incidents or concerns, and risks associated with network projects and programs.

This framework presents a risk management approach using the standard *AS ISO 31000:2018 Risk Management – Guidelines*. It aligns to the EQL corporate risk management framework and should be used in conjunction with the principles described in those documents

This framework comprises the agreed approach to the practical assessment and management of network risk within the Engineering division. It provides a summary of tools and processes that facilitate this function including the suite of risk evaluation matrices that provide context around the assessment of network risk.

Note: This does not preclude engineering professional services required under *EQL's Professional Engineering Policy P057* and the requirements of an RPEQ.

2 DEFINITIONS, ABBREVIATIONS AND ACRONYMS

2.1 Definitions

For the purposes of this standard, the following definitions apply.

Term	Definition
AER	Australian Energy Regulator.
ALARP	As Low as Reasonably Practicable. An established principle in risk management that is detailed in Standards legislation. Under the ALARP principle, risks in the broadly acceptable region may be regarded as insignificant and adequately controlled. ALARP is generally the target for risk reduction of operational (network capability and reliability) risks.
AMS	Asset Management System
Appetite	Amount and type risk that EQL is willing to pursue or retain to achieve objectives. EQL articulates risk appetite in a series of statements.
Attitude	Organisation's approach to assessing and eventually pursuing, retaining, taking, or turning away from risk.
Context	The operating environment and conditions in which an organisation operates. It includes internal and external factors relevant to organisation's regulatory environment, strategy, objectives, and risk management process.
BAU	Business as Usual – resources and effort are focused on the planned and budgeted work required to operate and maintain electricity infrastructure, its operational functions, and capabilities.
Consequence/ Impact	Outcome of an event affecting objectives. Can have a positive or negative, direct, or indirect effects on objectives. Can be expressed qualitatively or quantitatively.
Control	Measure that maintains or modifies risk. Includes but not limited to any process, policy, device, practice, or other conditions and/or actions which maintain and/or modify risk. An act, object (engineered) or system (combinations of act and object) intended to prevent or mitigate a risk or unwanted event.
Control Owner	Individuals with the accountability and authority for ensuring a control is in place and working as designed.
Corrective Control	Reduces the impact after the event has occurred or addresses flow-on effects.
Current/ Existing Control	A control which is in place and effectively modifying risk to the current level of risk (along with all other current controls).
Deep Dive	The process of conducting a thorough and detailed identification, analysis, and evaluation of business critical and strategic risks to enable discussion and risk oversight by the Executive, Risk and Compliance Committee (RCC) and Board.
Detective Control	May determine if the impact has occurred or if another control has failed but does not address the risk in the absence of further action.

Network Risk Framework



Term	Definition
DNSP	Distribution Network Service Providers i.e., Energex and Ergon Energy etc.
ENSMS	Electricity Network Safety Management Systems
Escalators	A scenario that increases the risk likelihood, including: <ul style="list-style-type: none"> Loss of control escalators increase the likelihood of a hazardous event occurring. Consequence escalators increase the likelihood of a high-consequence scenario following a hazardous event.
Event	Occurrence or change of a particular set of circumstances. Can be something that is expected which does happen or something that is not expected which does happen.
Finding	A factual outcome of an audit or investigation.
FSA	Formal Safety Assessment (As per AS5577)
GRC	Governance, Risk and Compliance (GRC) known as the SAP GRC Enterprise Tool for Energy Queensland. Risk information is stored in the Risk Module of GRC.
Hazard	Source of potential harm. Can be a risk source. i.e., something that may pose a threat to a person's safety.
Hazardous Event	Where one or more precautions fail contributing to a loss of control where someone is exposed to a safety risk resulting in consequences.
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 (in order): elimination, substitution, isolation, engineering controls, administrative controls and finally use of personal protective equipment.
Key Control	Controls that provide the most defence against a particular risk. One that is crucial to preventing the event or mitigating the consequences of the event. Its absence or failure would significantly increase the risk despite other controls.
Key Control, Performance and Risk Indicators	
Key Control Indicators (KCIs)	Metrics tied to controls. KCIs are used to define the company wide controls to and monitor the achievement of the set objectives. Managers define the related desired tolerances for controls before measuring
Key Performance Indicators (KPIs)	A measurement with a defined set of goals and tolerances that gauges the performance of an important business activity.
Key Risk Indicators (KRIs)	A proactive measurement for future and emerging risks that indicates the possibility of an event that adversely affects business activities.

Network Risk Framework



Term	Definition
Level of Risk Inherent Risk (Inherent Level of Risk / Untreated) Residual Current Risk (Current Level of Risk) Residual Planned Risk (Target Level of Risk)	Magnitude of a risk or combination of risks, expressed in terms of the combination of consequence and likelihood assessed in line with the Risk Evaluation Matrix. Initial assessment of risk where there are no existing controls or where the controls are assumed to fail to take effect during a risk event. Takes into consideration existing controls at their actual level of effectiveness. Expected level of risk following the completion of all (current and planned) risk treatment actions.
Likelihood	Chance of something happening (ISO31000:2018 section 3.7).
Mitigative Control	Reduces the consequence/ impact of an event.
Monitoring & Review	Monitoring involves continual checking, supervising, critically observing or determining the status to identify change from the performance level required or expected. Reviewing involves activities undertaken to determine the suitability, adequacy, and effectiveness of the subject matter to achieve established objectives. Monitoring and reviewing can be applied to risk management framework, process, risk, or risk control.
Network Risk	For the purposes of this document, Network Risks are those risks that: <ul style="list-style-type: none"> • are associated with monitoring, maintaining, and improving or extending the Ergon Energy and Energex distribution networks • include risks to; people, assets, the environment, the distribution organisations and Energy Queensland Limited, that arise from the above activities • are monitored and managed by the Engineering Division.
NREM	Network Risk Evaluation Matrices are used to evaluate network risks. They are a subset of the EQL Risk Evaluation Matrix that provide additional granularity for evaluation of operational and investment risk in the Engineering Division.
Opportunity	Combination or circumstances expected to be favourable to objectives. A positive situation in which gain is likely and over which one has a fair level of control. An opportunity to one party may pose a threat to another. Taking or not taking an opportunity are both sources of risk.
PoW or Program of Work	The suite of network projects and programs that will be undertaken utilising capital (Capex) and operational (Opex) budgets for a given expenditure period. The Capex PoW generally includes augmentation, replacement, and connections work. The Opex PoW generally includes routine maintenance activities.
Preventative Control	Attempts to prevent the consequence/ impact from occurring in most circumstances by reducing the likelihood. Work to address the Drivers to the risk by preventing or reducing the likelihood of the risk event occurring.

Network Risk Framework



Term	Definition
RCC	Risk and Compliance Committee.
Reasonably Foreseeable	Risk scenarios that can be anticipated; that a reasonable person in the same situation could anticipate in the circumstances. Sufficiently likely to occur such that a person of ordinary prudence would take into account in reaching a decision.
RPEQ	Registered Professional Engineer of Queensland
REM	Risk Evaluation Matrix – EREM generally refers to the EQL corporate matrix R056 whereas NREM is used to denote the Network matrices provided in the Network Risk Framework
Response	A Response is any action proposed to modify a risk by preventing, detecting, or correcting issues caused by unwanted events. The Response once completed may become a control.
Response Owner	Individuals with the accountability and authority to complete the required activity.
Risk	Effect of uncertainty on objectives. It can be positive, negative or both and can address, create, or result in opportunities and threats. Objectives can have different aspects and categories and can be applied at different levels.
Risk Analysis	The process of comprehending the nature of risk and to determine the level of risk. Provides the basis for risk evaluation and to decisions about risk treatment.
Risk Appetite/ Risk Appetite Statement	Risk appetite refers to the amount, type, and level of risk that EQL is willing to take, pursue or accept in order to achieve its objectives. Refer to the EQL Risk Appetite Statement (RAS).
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Evaluation	Process of comparing the results of risk analysis with risk criteria to determine whether the risk is acceptable or tolerable. Assists in the decision about risk treatment.
Risk Expert	Subject matter experts that support Risk Owners manage and respond to a risk.
Risk Identification	Process of finding, recognising and describing risks that might help or prevent an organisation achieving its objectives.
Risk Management	Activities (communicating, consulting, including educating, establishing the context, and identifying, analysing, evaluating, treating, monitoring, and reviewing of risks) to enable informed decision making in relation to risk.
Risk Management Framework	The set of foundation documents and organisational arrangements for designing, implementing, monitoring, reviewing and continually improving risk management throughout the company.
Risk Management Plan	A document that formally collates the results of risk assessments related to a specific set of objectives. This includes the risk ratings, key risk indicators and treatment action plans for the reduction of risk to a tolerable level.

Network Risk Framework



Term	Definition
Risk Management Process	The systematic application of management policies, procedures, and practices to the activities of communicate, consulting, establishing the context, identifying, analysing, evaluating, treating, monitoring, and reviewing risk.
Risk Owner	Person or entity with the accountability and authority to manage risk. They are responsible for monitoring and managing the risk, including response planning, implementation, monitoring, review, and reporting. The owner also makes decisions on the tolerability of risk and the appropriateness of treatment plans (within EQL's overall risk context)
Risk Scenario	Risk is usually expressed in terms of risk sources, potential events, their consequences/impact, and their likelihood.
Risk Source/ Driver	<p>Risk Source: Element which alone or in combination has the potential to give rise to risk.</p> <p>Risk Driver: Factor that has a major influence on risk. A brief statement of the reason for an unwanted event (other than failure of a control).</p>
Risk Treatment	<p>Process to modify risk. Can involve:</p> <ul style="list-style-type: none"> • Avoiding the risk by deciding not to start or continue with the activity that gives risk to the risk • Taking or increasing risk to pursue an opportunity • Removing the risk source • Changing the likelihood • Changing the consequence • Sharing the risk with another party or parties (including contracts and risk financing) • Retaining the risk by informed decision

Network Risk Framework

Term	Definition
Risk Types	
Strategic	Effect of uncertainty associated with EQL's strategic vision. Can be both internal and external risks that disrupt/impact/drive strategic objectives as well as those risks that can impact the achievement of strategic objectives.
Operational	Effect of uncertainty associated with the execution of business activities. Includes asset risk management, delivery of a program, projects and change initiatives, activity, or deliverable.
Emerging	Risks that are known to some degree but are not likely to materialise or have an impact for some time. They can be difficult to quantify. May start as a trend such as a demographic shift that may not have a material impact over the next two years but may dramatically impact EQL in 10 years. Emerging risks are particularly important in the context of strategic planning.
Portfolio Risks	Portfolio Risks are an aggregated view of risks across EQL. Portfolio Risks may include strategic, operational, and emerging risks. There are currently 10 Portfolio Risk areas. Health, Safety & Wellbeing, Energy Transition, Environment & Cultural Heritage, Cybersecurity, Network Asset Safety & Reliability, Customer & Social Licence, Climate Change, Digital Evolution, Financial Sustainability, People & Culture.
SFAIRP	So Far as Is Reasonably Practicable. An established principle in risk management that is detailed in legislation and by Safe Work Australia. Under the SFAIRP principle, it is still necessary to demonstrate there is no reasonably practicable means of risk reduction for risks in this region. SFAIRP is generally the target for risk reduction of safety risks.
SRA	Simple Risk Assessment – Simple risk assessment approach template to network risk assessments. This is most commonly used for Network Investments and Defect Management Plans.
Subject matter expert (SME)/ Risk expert	An individual with in-depth knowledge of the related business process/es.
Threat	Potential source of danger, harm, or another undesirable outcome. A negative situation in which loss is unlikely and over which one has relatively little control. A threat to one party may pose an opportunity to another.
Threat Barrier (Bow Tie) Diagram Bow-Tie Methodology	Threat barrier diagrams are 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.

Term	Definition
Tolerance	Organisation's readiness to bear the residual risk to achieve its objectives. Risk Tolerance is the degree of variance from its risk appetite that EQL is willing to tolerate. It sets the acceptable minimum and maximum variation levels for EQL on a particular strategic objective, KPI, category of risk or risk for example. Risk Tolerance typically acts as a trigger for corrective action, notification, and a review of the underlying causes of the risk exposure or significant variation from expected performance.
Uncertainty	State, even partial of deficiency of information related to understanding or knowledge. Uncertainty is the root source of risk.
Vulnerability	Intrinsic properties of something resulting in susceptibility to a risk source that can lead to an event with a consequence.
WH&S / HSE	Workplace Health and Safety/ Health Safety and Environment.

3 REFERENCES

3.1 Legislation, regulations, rules, and codes

- AS ISO 31000:2018 Risk Management – Guidelines
- AS/NZS IEC 31010:2020 Risk management - Risk assessment techniques
- HB 327:2010 Communicating and consulting about risk
- HB 158-2010 Delivering assurance based on ISO 31000:2009
- IEC/ISO 55000:2014 – Asset Management Standards

3.2 Energy Queensland controlled documents

Document Number	Document Name
689958	Enterprise Risk Management Standard R271
691603	EQL Risk Appetite Q015
690750	P043 Risk Management Policy
690762	Professional Engineering Policy P057
691861	Risk Evaluation Matrix R056
9937852	Risk Management Procedure

3.3 Other sources

[Network Risk Factsheets](#)

4 ENQUIRIES REGARDING THIS DOCUMENT

This framework is owned by the EGM Engineering.

Please direct any enquiries to the Engineering Division – Manager Network Safety and Risk.

5 FRAMEWORK HIERARCHY

5.1 Network Risk Framework

The Network Risk Framework exists as a sub framework of EQL’s enterprise risk management approach. It adheres to all principles and concepts defined in the parent document suite, however, provides a more contextualised application suitable to the specific management of network risk. Figure 1 displays this relationship.

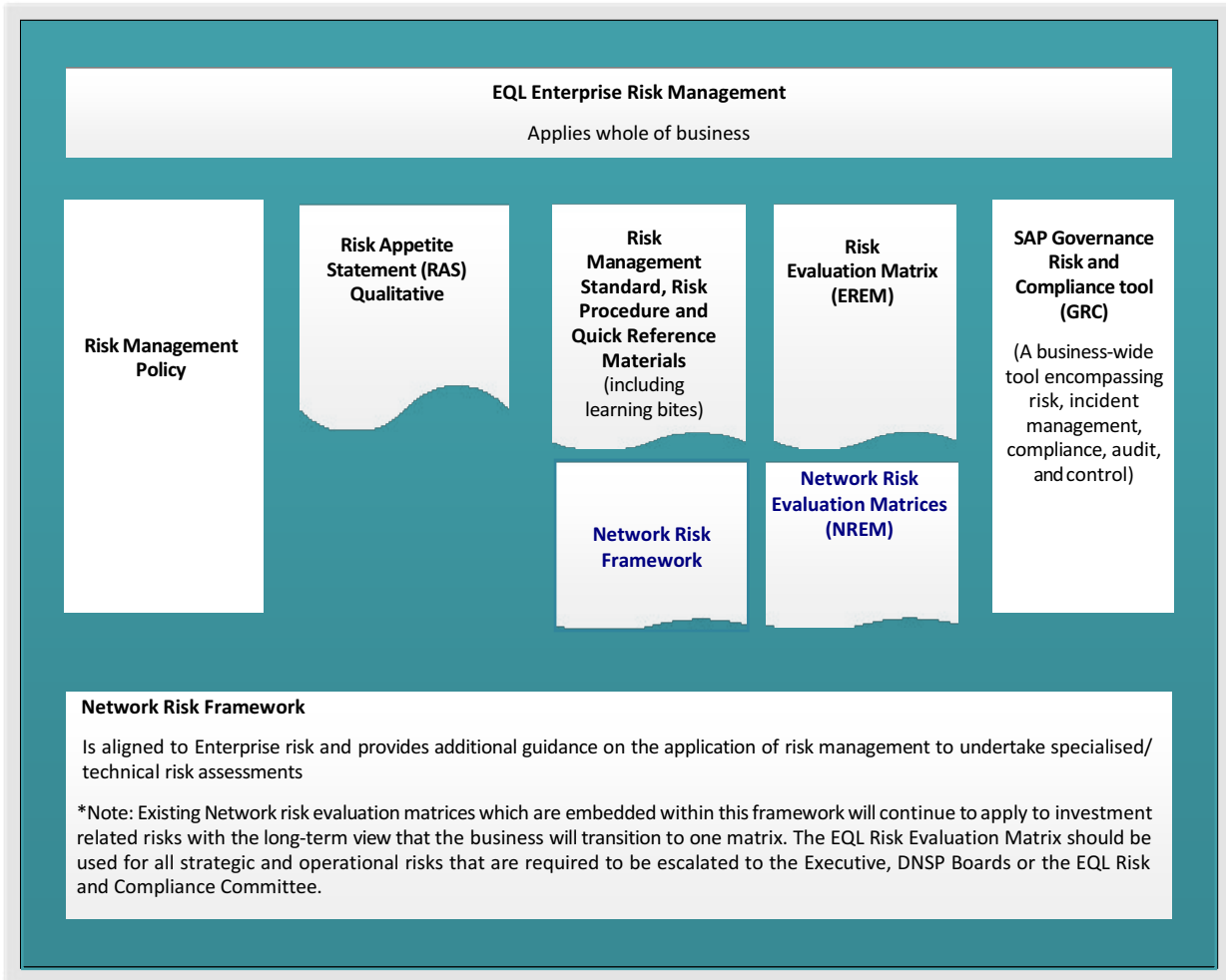


Figure 1: EQL Enterprise Risk Management

5.2 Network Risk Evaluation Matrices

The Network Risk Evaluation Matrices (sub-scales) are aligned to Risk Evaluation Matrix R056 – 691861 as detailed in Figure 2. They provide additional detail for the practical discernment of risk levels across risk categories relevant to Engineering.

There are three Network Reliability consequence frameworks in addition to the existing Safety and Environmental scales which cover the five network risk domains, as shown in Figure 2.

- **Safety**
 - **Environment**
 - **Legislated Requirements**
 - **Customer Impact**
 - **Business Impact**
- } **Jointly referred to as Network Reliability Sub-Scales**

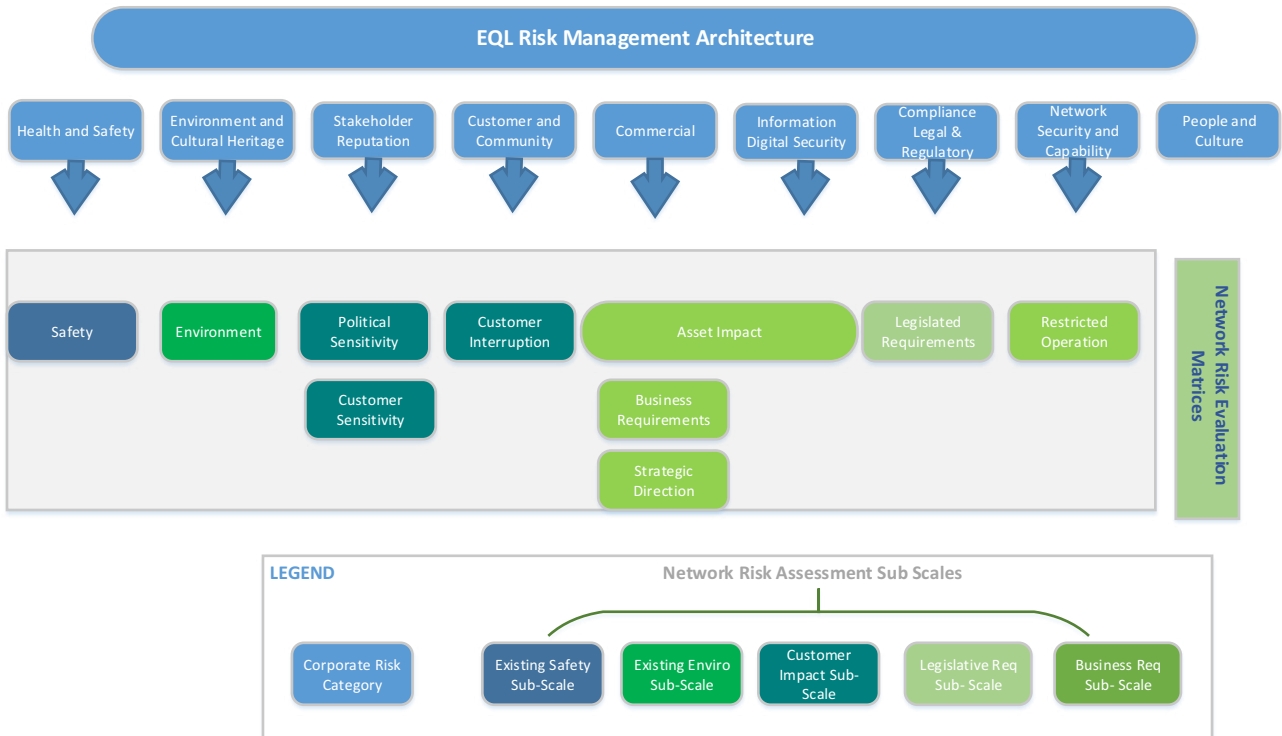


Figure 2: EQL Enterprise Risk Categories

6 APPLICATION

The Network Risk Framework and its embedded Network Risk Evaluation Matrices are to be used to conduct risk assessments on:

- all new investment proposals (business cases and project approval reports)
- investments detailed in the Program of Work
- asset assessments within forecasting tools (e.g., Copperleaf, P6).
- new operational risks identified in the field that are likely to require investment

Assessments should also be repeated regularly as part of our due diligence practices.

The Enterprise Risk framework (Risk Evaluation Consequence and Likelihood Matrix) should be used for risks that are:

- strategic in nature (i.e., they may impact the achievement of EQL's strategic objectives);
or
- non-network (i.e., not directly related to the physical distribution network e.g., cultural risks); or
- emerging where treatment through specific investment has not yet been identified
- appropriate to be escalated to the Executive, The Board and or Shareholding Minister.

These risks are managed through the Risk Module of the SAP tool.

7 ALIGNMENT TO AS ISO 31000

The network risk management approach aligns to the process stages described in AS ISO 31000. The *Enterprise Risk Management Standard R271 – 689958* details the high-level approach adopted by the Energy Queensland Group in applying this model.

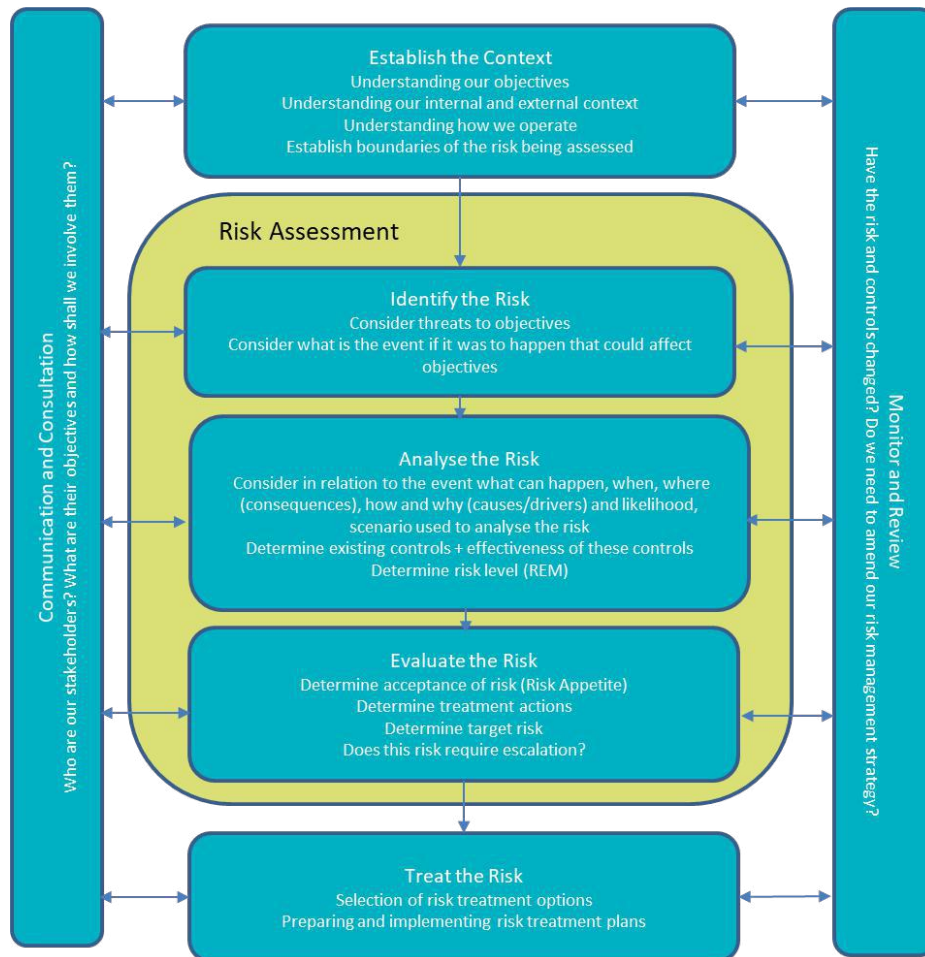


Figure 3: Risk Management Process

The following sections detail the application of this process within the Engineering division and aligned to *Enterprise Risk Management Standard R271 – 689958*.

8 CONDUCTING A NETWORK RISK ASSESSMENT

Risk assessments in Engineering are conducted in alignment with the ISO 31000 framework (above) according to the process outlined in Appendix B. Assessments should be conducted by a panel (of no less than three) whenever a threat is noted and should be repeated regularly to monitor that threat.

A variety of risk assessment templates are available on the Network Safety and Risk SharePoint site (examples are provided in Annexes C, D, E, F). Selection of the appropriate template will depend on the number of; scenarios, risk factors and controls to be considered. As a simple guide:

- Simple Risk Assessments (SRA) – may be used to assess an observed threat/hazard that may have multiple impacts
- Network Scenario Risk Assessments (M888) and Event Trees – may be used when assessors need to understand the detailed threat, progression pathway and control options for a specific sequence of events
- Bowtie or Threat Barrier Risk Assessments – may be used when there are multiple threats and multiple impacts connected via multiple pathways

Note: Other risk assessment techniques in accordance with *AS/NZS IEC/ISO 31010:2020 Risk management – Risk assessment techniques* may be used when appropriate for the specific business functions.

Outcomes (risk assessment records and action plans) are to be stored in a central location accessible to the business. In future this will be the Enterprise Content Management System ECM however, specific processes and technical functionality (workflows) have yet to be developed. Until the ECM system is established a copy of the risk assessment may be stored by the Network Safety and Risk Team.

The following sections detail the application of this process.

9 ESTABLISHING THE CONTEXT

Establishing the context and scope of the risk management process is performed by deciding upon the criteria against which risk is to be evaluated, e.g., safety, environmental criteria etc. Setting the scope should also ensure that goals or objectives are articulated along with the nature of decisions that must be made.

Internal context: Considers the current and future operating environments and should consider corporate objectives and obligations, policies, values, economic and resource factors.

External context: Considers legislative, regulatory and code requirements, perceptions, and values of external stakeholders (including customers), external influences and trends (e.g., Labour market) and their impact on the objectives of the organisation.

Regional and Isolated Network context: EQL acknowledges the regional nature of a large proportion of its geographical distribution area. When devising scenarios for risk assessment facilitators should take into consideration possibilities of incidents occurring in areas that have low population densities, and which are difficult to access. When considering remote scenarios, both consequence and likelihood scores (and suitable mitigation strategies) may differ to those devised for the urban context.

For most network concerns, the Network Risk Evaluation Matrices and Network Risk Tolerability scales will frame the assessment context. The matrices provide an agreed risk language where levels of magnitude are understood across the Engineering Division.

10 RISK ASSESSMENT

It is noted that the term “risk assessment” is commonly misused in place of “risk management”. Risk assessment, however, correctly refers to a component of the risk management process which only encompasses risk identification, risk analysis, and risk evaluation stages.

All risk assessments contain a certain level of subjectivity, which is why it is preferable to conduct risk assessments utilising more than one person. It is recommended that the minimum number of people is three, with as diverse range of knowledge and experience as possible for the relevant topic. To promote frank discussion and evaluation, individual responses may be recorded anonymously within the group.

Risk analysis may be undertaken to varying degrees of detail depending upon the risk, the purpose of the analysis, the availability of information, data, and resources. Analysis undertaken may be qualitative, semi quantitative, or quantitative, usually in that progressive order with each result needed to justify the extra time and effort to progress to the next.

10.1 Qualitative

Qualitative assessments are subjective estimates of risk used in the initial scoping stages to justify proceeding with either a semi-quantitative or full quantitative risk assessment. Their accuracy relies heavily upon accessing an appropriate range of subject matter experts with detailed knowledge and experience.

Qualitative Risk = Low, Medium or High

Qualitative risks assessments are often used to rank risks to ensure additional time and effort is spent on more detailed risk assessments for managing risks of higher importance.

10.2 Semi-Quantitative

Semi-quantitative assessments are a less subjective method of estimating risk. They involve estimating the likelihood of a consequence considering all risk factors collectively. This process also relies upon utilising an appropriate range of subject matter expertise.

Graded categories are used for both consequence and likelihood to calculate an overall risk score. In the Network Risk Evaluation Matrices both the consequence and likelihood scales range from 1 to 6 where 1 is low and 6 is high. Tables or scales of magnitude for each of consequence and likelihood have been developed for each assessment category, Safety, Environment, Legislated Requirements, Customer Impact, and Business Impact. These tables are provided in the Annex A.

$$\text{Semi-Quantitative Risk} = \text{Consequence} \times \text{Likelihood} = C \times L$$

Equation 1: Semi-Quantitative Risk

If there is wide variation of the estimated likelihood (e.g., If four persons give likelihood scores of: L=2, L=2, L=5, L=1), assessment facilitators should define the scenario in more detail such that there is common understanding of the sequence of events and the risk factors involved.

10.3 Quantitative

Quantitative risk assessment (QRA) requires accurate, readily available and quality data relevant to the risk factors under consideration. This often includes historical incident data, asset age and condition data, failure modes and failure probabilities, and consequence costings but is not limited to this. QRA assigns a measurable value to each specific consequence. When dollar figures are used, this is sometimes referred to as risk monetisation, but other scales such as time may be used. QRA then requires the likelihood of each impact event to be estimated independently as a numerical probability or frequency.

These factors are then combined logically to give the likelihood of the entire sequence of events leading to the chosen consequence occurring.

$$\text{Quantitative Risk Cost} = \text{Sum of } (\text{Probability of Failure (PoF)} \times \text{Likelihood of Consequence (LoC)} \times \text{Cost of Consequence (CoC)})$$

Equation 2: Quantitative Risk Cost

Various forms of QRA are being used throughout the Engineering Division in areas where the level of detailed data required is available. These include:

- Failure modes and effects analysis (FMEA) – used in maintenance planning
- Reliability assessment planning (RAP) – used in network planning.

Work is currently underway to establish an EQL suite of agreed methodologies (including standard and discretionary factors/constants).

AS/NZS IEC/ISO 31010:2020 Risk management – Risk assessment techniques contain a full listing of QRA methods and procedures. The AER has additionally provided an *Industry practice application Note: Asset replacement planning* to assist EQL to develop its approach.

11 RISK IDENTIFICATION

11.1 Choosing a consequence

Risk identification begins by choosing a consequence or consequences of most concern or interest. The NREM provides a framework for consequences of significance to Engineering. A chosen consequence should generally be aligned to one of these descriptors.

There are three network consequence frameworks in addition to the existing Safety and Environmental scales which cover the five network risk domains, as shown in Figure 2.

- **Safety**
 - **Environment**
 - **Legislated Requirements**
 - **Customer Impact**
 - **Business Impact**
- } **Jointly referred to as Network Reliability Sub-Scales**

A group performing a risk assessment need never argue about consequences. If more than one consequence is of concern, then each consequence is considered one at a time (each has a separate associated scenario). Where there are multiple consequences applicable, each should be considered however the overall risk level is generally reported as the highest outcome of all consequences.

12 RISK ANALYSIS

12.1 Develop Risk Scenario

A chosen risk scenario must be fully described before moving onto risk evaluation. Group brainstorming is often used. The extent and depth of the risk scenario depends on the estimated level of the risk.

To begin the scenario, it is often helpful to pose a risk question or description. For example: *What is the risk of [something/someone] suffering [this consequence] under the following circumstances?*

Scenario mapping can be used to either graphically (e.g., event tree or fault tree) or in writing capture a credible sequence of events, or the possible ways in which the chosen consequence could occur.

The circumstances or risk factors are then identified for each section of the scenario. The effectiveness and potential failure of existing risk controls are risk factors when considering the current residual risk scenario.

Relevant risk factors and existing controls for each step in the sequence should be identified, as the effectiveness and potential failure of existing risk controls are factors that could influence the outcome.

This process is repeated for each consequence of concern, with a scenario defined for each.

Important points to remember during risk identification:

- The focus should be on articulating what is uncertain about this scenario. The risk being described should be the most credible/ plausible, 'most likely' risk event, not the worst-case scenario.

- Not only the most severe (worst case) consequence needs to be considered, as there are often other consequences of interest for example, a fatality versus a broken limb, or a whole of substation outage versus an individual 11kV feeder outage. In general terms, the lower the severity of the consequence the higher the likelihood tends to be, and vice versa (e.g., there are less risk factors present or less risk controls needed to fail for a low severity consequence to occur).
- It is not correct or logical to attempt to select “a most likely consequence” because that is claiming that the likelihood is known before it is calculated.
- The same scenario cannot lead to different consequences. There will be different circumstances or different events that occur in order to lead to a different consequence. Each consequence of concern will therefore require a different scenario development.
- Even if only one event or circumstance is changed then the risk scenario and its likelihood are also changed.
- Network risk scenario/s should be sufficiently detailed to be understood and have outcomes that are repeatable by others.
- Common mistakes in defining risks include:
 - Confusing a missing, inadequate, or failed control as a risk.
 - Try to avoid risks starting with ‘Poor...’, ‘Inadequate...’ or ‘Lack of...’ as they are likely to be a statement of an ineffective control and rather than a risk.
 - Detailing just the impact.
 - Broad, non-specific statements such as “revenue loss” or “brand damage” or “non-achievement of an objective” are not helpful in understanding the risk.
 - Using jargon, acronyms or vague wording that makes it difficult to understand what the risk actually is.

Scenario Mapping Tools – Event Trees

Event trees may be used to define the scenario of a risk concern or to assess an incident that has occurred. The scenario is represented by a simple map of the sequence of events needed to lead to a specific selected consequence. Event tree analysis explores risk factors of each event, such that assessments of likelihood or probability can be made.

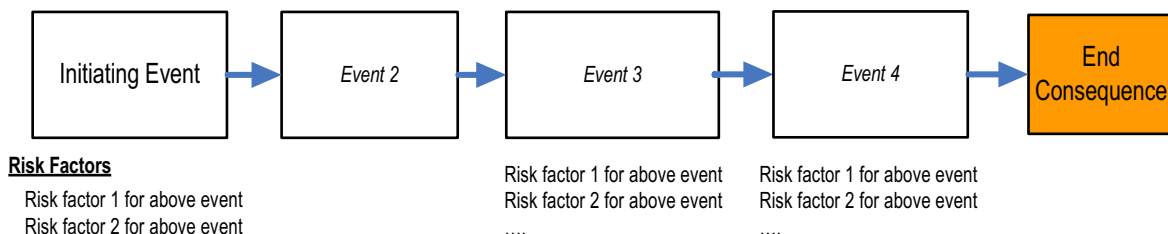


Figure 4: Structure of an Event Tree

See Annex C for worked examples of an event tree.

Scenario Mapping Tools – Fault Trees

Fault trees are graphical representations of a logical structure representing undesired events (failures) and their causes.

The structure is created by using logic gates (AND and OR gates). Reliability parameters are assigned to the basic events. In contrast to an event tree, there is no time dimension in a fault tree, only causal logic gates.

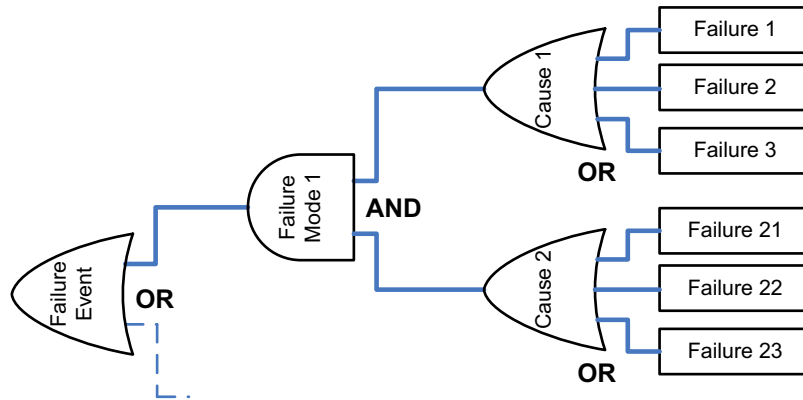


Figure 5: Example Fault Tree Structure

Scenario Mapping Tools – Bow Tie and Threat Barrier Diagrams

Bow-Tie and Threat Barrier diagrams are effective at displaying several distinct scenarios on a page. They are particularly useful when evaluating risk treatments or controls where these may be shown to act as barriers to reducing either the likelihood or consequence of a risk pathway.

See Annex D for an example of a Bowtie/ Threat Barrier Diagram

12.2 Assessing Likelihood

When estimating the likelihood, assessors should note that the likelihood of the whole scenario (all events in sequence), including the end consequence occurring, should be considered.

To perform this, assessors should choose the appropriate column(s) from the Likelihood tables in Annex A NETWORK RISK EVALUATION MATRICES. Note that:

- different columns of the table may be relevant to different identified risk scenarios. Ensure that the column for situations related to 'Generic failure of an asset type' is not confused with the column for situations pertaining to 'Single specific items', as only one should apply to the scenario being considered
- the history or past frequency of events may influence but should not solely determine the estimation of the likelihood or frequency of future events being considered. Risk factors or circumstances may be changed with respect to the past.

To address a number of commonly asked questions about estimating the likelihood of a scenario, there are some rules or assumptions presented below.

- The age and condition of plant and its location and exposure to external forces (i.e., whether a transformer has external bushings or cable boxes)
- If feeders are overhead or underground, the type of construction, condition, and terrain.
- Asset replacement and augmentation scenarios must include and detail the plant outage events and how they are caused
- Vegetation caused outages, weather events (including storms), plant or systems failure, external party damage to network, animal impact.
- The risk assessment is NOT assessing the likelihood of spare plant or resources being available.

12.3 Risk Analysis and Impact of Controls

There are three risk levels of interest that should be considered. These are:

- **Inherent risk level** – the risk that exists prior to any treatments or controls being applied or considered (including any operational solutions) or that exists in the event of failed controls.
- **Residual Current risk level** – the risk that remains with all current operational risk treatments or controls verified to be in place and effective. For a customer impact risk, for example, this may include available load shifts to restore supply.
- **Residual Planned risk level** – the desired risk level consistent with the SFAIRP/ALARP principle and achievable with the additional or changed risk controls or risk treatments in place. Again, considering an example in the customer impact risk domain, this may be after the implementation of a new capital project that permanently treats the risk of supply outage.

For each of these situations once likelihood and consequence levels have been determined, the multiplication matrix for semi quantitative risks can be used to determine the risk score.

$$\text{Semi Quantitative Risk} = \text{Consequence} \times \text{Likelihood} = C \times L$$

Equation 3: Semi Quantitative Risk



Risk Analysis 6x6 multiplication R=C x L		Consequence 					
		1	2	3	4	5	6
Likelihood 	6	6	12	18	24	30	36
	5	5	10	15	20	25	30
	4	4	8	12	16	20	24
	3	3	6	9	12	15	18
	2	2	4	6	8	10	12
	1	1	2	3	4	5	6

Figure 6: Risk Assessment Multiplication Matrix

12.4 Control Effectiveness

After each risk analysis, assess which risk factors have the greatest effect on the risk score estimate i.e., to which factors is the risk level most sensitive. Usually, some assumptions regarding risk factors are made and need to be tested by seeing how much a small change in each factor can influence the final risk level or score.

By detecting the sensitive risk factors, a better understanding of the certainty and confidence of the risk score can be made. This analysis will also reveal which risk factors will have the highest priority for risk controls. Controlling these factors will reduce the risk level the most.

Table 1 presents the risk control hierarchy based upon effectiveness of risk treatments.

Table 1: Risk Treatment Hierarchy by order of most preferred (based on WH&S approach)

Risk Treatment Hierarchy <i>By order of most preferred</i>		
Physical Engineering	1. Elimination	Avoiding or removing exposure to a hazard or event leading to the consequence under consideration.
	2. Substitution	Replacing the hazard or risk factor with another object, material, plant item, or substance that reduces the risk factors.
	3. Separation	Physical distance or barriers or time separation to reduce exposure to the risk factors, hazards, or events.
4. Administration		Ensure effective implementation of rules, policies, and procedures to reduce exposure to the consequence or the likelihood of the existing consequence being realised.
5. Behaviour related measures		Measures that encourage required behaviours.

13 RISK EVALUATION (INCLUDING RISK TOLERABILITY)

Risk Tolerability scales provide for evaluation of considered risks by the appropriate level of management. They also provide a determination of whether the risk resides in the intolerable or tolerable range and whether additional actions are warranted to further control or mitigate the risk.

The agreed Network Risk Tolerability Scales for risks evaluated according to the Network Risk Evaluation Matrices are presented in Figure 7.

Network Risk – Risk Tolerability Criteria		
Risk Score	Risk Descriptor	Risk Tolerability Criteria, Management Oversight and Action Requirements
30 - 36	Extreme Risk	Intolerable <i>(stop exposure immediately and notify management chain)</i>
24 - 29	Very High Risk	Executive Committee (ExCom)
18 - 23	High Risk	Executive General Manager (EGM)
11 - 17	Medium Risk	General Manager (GM)
6 - 10	Low Risk	Department Manager (DM) / Process Owner (or equivalent)
1 - 5	Very Low Risk	No direct approval required but evidence of ongoing monitoring and management is required

- Safety risks must be managed in line with the principles of **So Far as is Reasonably Practicable SFAIRP**
- Non-Safety risks must be managed in line with the principles of **As Low as is Reasonably Practicable ALARP**
- All identified risks are required to be periodically reviewed to monitor the ongoing risk levels, the effectiveness of new risk treatments and existing controls.

Figure 7: A Risk Tolerability Scale for evaluating Semi-Quantitative risk scores

All identified risk requires periodic review see Section 16.3.

The risk tolerability scales for Network risks are underpinned by the following directives:

1. Exposure to risks identified as intolerable must cease immediately and the risk must be clearly communicated to the business.
2. For risks identified as intolerable (risk score >29) and for which exposure is still required and necessary, proponents must maintain regular and detailed communication with the EGM to ensure that all practicable resources and effort required to bring the risk into the tolerable range are applied as a matter of priority.
3. EQL leaders have an obligation to be aware of risks and how they are being managed within their area of accountability. The tolerability table links risk levels to the appropriate level of management oversight required. The escalation of risk profiles provides leaders with the opportunity to review/endorse or otherwise intervene in risk mitigation plans, for example, decision may be made to access funding to accelerate mitigations or alternatively to determine that proposed treatments are not reasonably practicable.

4. Escalation pathways and timing will vary with risk emergence and mitigation urgency. For example, leaders at the appropriate level should be notified as soon as possible of emerging risks that require immediate responses. Lower-level emerging risks of a less urgent nature may be discussed in Team meetings and escalated via the management hierarchy to higher levels. Risks where specific investment options have been identified to treat limitations may be aggregated for approval by relevant managers as they enter the Program of Work.
5. No identified risks should be considered as “negligible”. Where the possibility of an adverse consequence exists risk exposure should be managed (for very low risks this could be as simple as a periodic review).
6. The aim is to reduce all network risks to So Far as is Reasonably Practicable (safety risks) or As Low as Reasonably Practicable (operational risks where the consequence is not safety related, for example financial impacts). ***Where there are no obligations to manage risk SFAIRP, risks are to be managed in line with the EQL Risk Appetite. EQL’s Risk Appetite Statements establishes the amount of risk EQL is willing to pursue or accept in order to achieve its objectives. The RAS should be used to inform and assist in decision-making.***
7. Risks are considered SFAIRP/ ALARP if it can be shown that further risk reduction has been considered and concluded as impracticable or requires action grossly disproportionate in time, cost, and effort to the reduction in risk achieved. For operational risks there may be pre-determined spend levels that are considered as organisationally tolerable consequences. There is no pre-determined level at which adverse safety consequences are acceptable.
8. There is no barrier to allowing a particular risk to remain above the Very Low-level range, provided it is demonstrated that current/planned controls provide the best outcome for the business, and the risk is supported by detailed assessments with the appropriate level of approval.

14 RISK TREATMENT

The goal of risk treatments or risk controls is to:

- reduce exposure to hazards; and or
- minimise or control risk factors; and or
- reduce the likelihood of the scenario eventuating; and or
- reduce the consequence of the scenario.

When choosing risk treatments or control measures, consideration must be given to the known effectiveness of various risk treatment options.

Selecting the most appropriate risk treatment involves balancing the costs and efforts of applying the treatments against the benefits achieved. The treatment should clearly identify the priority in which individual risk treatments should be implemented or staged over time.

Some risk treatment may introduce new risks that need to be identified, assessed, and monitored as part of an iterative and continuous process.

Appropriate risk management may require the choice of more than one risk treatment option.

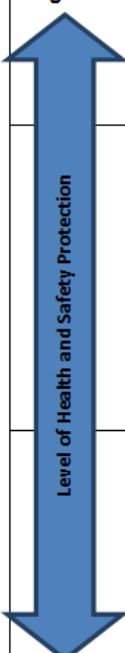
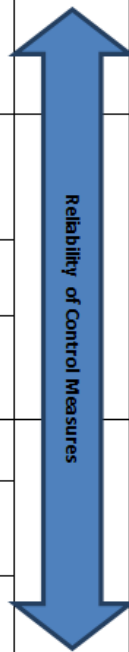
Risk Treatment / Control Hierarchy						
HARD Options - Most preferred – Consider First (less dependent on human reliability - can appear to be more costly)						
	Level	Control Hierarchy	Risk Treatment			
 Highest Least	1	Elimination / Substitution	eliminating / removing exposure to the hazardous object, material, substance, method or procedure , or replacing it with another that has a lower risk for the same exposure <i>For example, not using an EWP that has been identified as having faulty controls or using a chemical with a lower toxicity or flammability but still achieves the same function or outcome.</i>	 Most Lowest		
		2	Design		better initial design / ergonomics and reengineering / redesign which introduces new methods of physical operation, barriers , safe-guards or safety devices to reduce the risk exposure <i>For example, design an overhead network to enable de-energised work or ergonomic redesign of tools and equipment</i>	
	Separation		distance or time separation of hazards and exposed persons <i>For example, demarcation / barricading exclusion zones for fall / drop hazards</i>			
	3	Administration	improved or new rules / procedures / scheduling / maintenance / communications – better involvement of users in risk assessments / review or development of better user documents, signage, messages, notices			
		Supervisor / Enforcement	selection and preparation of personnel / behaviour reinforcement methods / fair and just culture discipline /culture			
		Checking / Assessments	Audits / Inspections / reviews / risk assessments / frequency / depth <i>For example, scheduling work on /near roadways outside of peak hours or improved checking on actual operations and activities. Better / different frequency maintenance inspections / servicing</i>			
		Behaviour-Related Measures	wearing PPE Personal protective equipment - providing protective clothing or equipment to exposed personnel – Training – all kinds, - Behaviour observation / interaction related programs. <i>For example, better Initial and refresher training for high risk activities.</i>			
	SOFT Options - Least preferred (– more dependent on human reliability - can appear to be less costly)					
	Notes 1) Always use multiple controls – never rely on only 1 - the more controls the less likely that all will fail / be ineffective at the same time 2) Always use a combination of controls from different parts of hierarchy – even HARD controls at the top of the hierarchy are not perfect 3) Always use pre-emptive controls which reduce Likelihood L as well as reactive responsive controls which primarily reduce Consequence C 4) Always consider effectiveness of control options – not just cost 5) "Better Ergonomics" means changing design and methods of use to better match human operators' capabilities and limitations					

Figure 8: Risk Treatment and Control Hierarchy

This is an iterative and continuous process. This risk assessment process, if required, follows the same steps as for an assessment of the inherent/untreated risk with the addition of now considering the new and/or changed risk treatments in place to yield either the current residual or target residual risk.

If the budget or resources for risk treatments is constrained, the treatment plan should clearly identify the priority order in which individual risk treatments should be implemented or may be staged over time. Choice of treatment options needs to involve comparative cost benefit analysis for each option, even if only qualitative, and should be documented.

15 COMMUNICATION AND CONSULTATION

Risk communication and consultation should be continuous from the beginning to the end of the risk management process, not only at the conclusion.

The consultation aspect is to ensure that the best available knowledge and experience is drawn upon for the assessment of risks and development of risk treatment plans. As stakeholders are likely to make judgements about risk based on their perceptions, it is important to involve persons with a broad a range of experience in network risk assessments.

Communication of the risks and treatment plans is an important step in informing the business of emerging or changing risks, as well as the current and (if applicable) future risk levels and risk treatment measures to be implemented.

Risk communication channels currently in use within the Energy Queensland Group include: SAP Risk Module, the Copperleaf (C55) tool, the Distribution Annual Planning Report (DAPR), the Program of Works governance process and quarterly reviews, Project Approval Reports, Investment Business Cases, and others.

15.1 Roles and Responsibilities

The following details the key roles and responsibilities during a risk management process.

Risk Owner

The risk owner is responsible for the overall management of the risk and the implementation of risk response strategy which includes ensuring controls are in place and working, in addition to actions/responses which are planned to achieve the residual risk planned outcome. Whilst the Risk Owner may delegate day-to-day operations and functions associated with the risk to a Risk Manager, the Risk Owner continues to hold overarching accountability for the risk and should be identified prior to the risk assessment.

Risk Assessment Originator

The risk assessment originator is responsible for providing all relevant context and background with regard to the risk assessment. The originator will work closely with the risk assessment facilitator to run the risk assessment workshop at a time suitable to all stakeholders. The originator is responsible for ongoing action management and is for also ensuring all risk artefacts and records are kept in accordance with EQL's records management policy and stored in a system such as ECM, SharePoint, or another appropriate tool.

Subject Matter Experts

Subject matter experts (SMEs) involved in risk assessments are individuals who have the necessary expertise or knowledge of the risk and its context to provide an objective assessment of the risk being considered and its impact on our objectives (i.e., safety of people etc). SMEs represent the forum, department, group, or division within the risk assessment. The SME is responsible for communicating the outcomes of the risk assessment and potential actions to their area of remit after the risk assessment. Communication may include informing relevant teams and management of outcomes in conjunction with the risk assessment facilitator. SMEs also represent control owners for their applicable area. The SME (together with the Risk Assessment Originator) is also responsible for communicating with control owners about any changes, improvements, or effectiveness of controls.

Note: The number of SME involved in a risk assessment may vary from time to time, where numbers exceed >10 people, groups with multiple SME's from the same group may elect one individual to participate in the risk assessment.

Risk Assessment Facilitator

This risk assessment facilitator is responsible for facilitating the risk assessment workshop following the risk management process. The facilitator will guide the risk assessment in line with the risk management process and the selection of tools/techniques. The facilitator will capture relevant information about the risk assessment to assist in the development of the risk assessment scenario, identification of risk factors, existing and new controls, and subsequent actions.

The facilitator and scribe are not responsible for ongoing active management and outcomes coordination.

At the conclusion of the risk assessment, the facilitator will send the risk assessment document to the risk owner, risk subject matter experts and originator. As part of good governance, the facilitator should not be the approver of the risk assessment. In limited circumstances where the facilitator is also the originator and risk owner, a level of independent oversight and approval is recommended. As risk assessment scribe may also be used to capture and record risk assessment information and outcomes.

16 RISK RECORDING, MONITORING AND REVIEW

16.1 Required Documentation

Regardless of the tools used, each network risk of concern or interest is to be documented with the following information:

- Scenario of concern including the chosen consequence of interest or concern
- Risk factors
- Assessed likelihood
- Risk level calculation and Tolerability outcome
- Details regarding any new or changed risk treatment measures
- Persons responsible for implementing the new or different risk controls, and when they are to be implemented
- Date on which risk assessment was completed and the timing for which the risk assessment will apply (i.e., risk assessment was documented on 01/01/2023 for a network risk that is not expected to exceed this risk level before 30/12/2025)
- Reference any supporting documents for details on monitoring and review plans, communication, and consultation strategies and/or audit schedules.

This documentation must be completed for a minimum of the current risk case, and the target risk case as relevant with the results formally recorded in the appropriate Risk Register. The most common templates for recording this information are the Risk Assessment Record-Semi-quantitative (previously M888) (see Annex E) and the Simple Risk Assessment Template (see Annex F).

Table 2: Record Repositories

Risk	Register
Emerging risks (newly identified operational or strategic risks)	<ul style="list-style-type: none"> SAP Risk Module - Governance Risk and Compliance GRC Tool
Assessed Safety risks	<ul style="list-style-type: none"> SAP HSE (where related to an incident) Network Safety and Risk Team and or Risk Owner to maintain copies in a corporate system such as ECM
Assessed Environmental risks	<ul style="list-style-type: none"> Network Safety and Risk Team and or Risk Owner to maintain copies in a corporate system such as ECM
Assessed Network risks	<ul style="list-style-type: none"> Network Safety and Risk Team and or Risk Owner to maintain copies in a corporate system such as ECM
Network related risk where a risk treatment / investment has been proposed or planned	<ul style="list-style-type: none"> Copperleaf C55 Master Projects Library – may be stand-alone or incorporated into Business cases, scope statements and/or Project Approval Reports Network Access Restriction NAR Manager Defect Management Plan Library

16.2 Measurement

The management of Network Risk is to be measured by the following:

- Assurance of network risk assessments and compliance to this procedure
- Outcomes of network risk assessments (network risk scores) used as an input into risk-based optimisation of Programs of Work
- Network risk assessment outcomes used as an input for decision making around new or emerging risks documented in the Network Risk and Safety SharePoint/Tool/Portal.

16.3 Periodic Review

Assessments should be repeated regularly at time frames relevant to the risk being assessed. The periodic review frequency needs to be set according to foreseeable changes in significant risk factors and should be recorded.

Review periods should be based on tolerability (more frequent reviews of higher risks) and should consider the effectiveness of existing controls including temporary mitigation efforts. Where deficiencies in controls have been identified, a more frequent review of the risk may be required. It is recommended that reviews of risks should not exceed 12 months.

Engineering acknowledges that there are other periodic reviews that are in place as part of existing business processes and PoW optimisations. Therefore, periodic reviews may differ between Operational and Investment Risks.

Annex A NETWORK RISK EVALUATION MATRICES

A.1 Legislated Requirements

Consequence Scale	Legislated Requirements, Regulatory Involvement
6	Administration appointed / entire or partial loss of operating works or functions Revocation of operating licence, permit or authorisation
5	Enforcement Notice issued by regulator (or equivalent) as a result of breach of Acts, Regulations, Codes or Rules
4	Improvement or Penalty Infringement Notice issued by regulator (or equivalent) as a result of breach of Acts, Regulations, Codes or Rules
3	Note 1
2	
1	
Note 1: No applicable measure for this dimension	

Network Risk Framework

A.2 Customer Impact

Consequence Scale	Interruption (>1 min)			Customer & Political Sensitivity	
	Customer No's	Duration / Time to Restore	Repeat Frequency		
6	70,000	> 1 week	Note 1	Note 1	Call for replacement of Directors and / or Executive management, Sustained or widespread levels of national attention / Extensive public outrage, Irreversible brand damage
5	50,000	> 3 days			Call for enquiry, public outrage, and sustained or widespread levels of adverse attention / negative media. Medium to long-term Brand damage. Multiple ministerial / cabinet involvement
4	15,000	> 1 day	every day in one week	Inability to meet agreed target date, or disruption to multiple large-scale businesses or essential services (e.g., Hospitals, sewage)	Adverse widespread regional media attention (e.g., Disruption to large public events). Loss of public trust
3	5,000	> 12 hours	three times in one week	Disruption to single large-scale business or essential service, or inability to meet agreed target for increased supply	Adverse local media attention. Loss of customer trust / action groups formed. Ministerial direction / approval. Short-term brand damage
2	1,000	> 3 hours	twice in one month	Disruption to small to medium business, or inability to meet agreed target for increased supply to small to medium customers / businesses	Low levels of adverse local media reporting or other negative external publicity. Multiple customer complaints. State MP concern / Ministerial request / concern
1	100	< 3 hours	once only p.a.	Customer inconvenience	Few customer complaints and or external criticism. Local government concern. Informal response from EQL may be required to resolve

Note 1: No applicable measure for this dimension

Network Risk Framework

A.3 Business Impact

Consequence Scale	Business Rules, Data management & security	Restricted network operation / loss of control, indication, protection	Strategic Direction	Asset and Commercial Impact (including Obsolescence) #
6	Note 1	Inability to remotely control majority of Energex/Ergon network, or plant operated above rating	Unable to deliver on its agreed strategic initiatives resulting in additional costs to the business or lost opportunity \$>20 million	Business impact >\$20million total impact of event - for example: cost premium on project, labour 200 000hr, reliability impact or opportunity lost
5		Inability to remotely control half of Energex/Ergon network	Unable to deliver more than half its agreed strategic initiatives, resulting in additional costs to the business or lost opportunity \$>5 million	Business impact >\$5million total impact of event - for example: labour 50 000hr, reliability impact, inability to meet strategic initiatives or opportunity lost
4	Release of non-public / sensitive information or vulnerabilities in Information Security, IT, OT, or Telco Networks	Inability to remotely control > = 2 bulk supply substations supply area	Unable to deliver an agreed strategic initiative, resulting in additional costs to the business or lost opportunity \$>1 million	Business impact >\$1million total impact of event - for example: cost premium for project, labour 10 000hr, reliability, opportunity lost
3	Compliance breach with Energex/Ergon policies Compliance breach with external standards*	Inability to remotely control an Energex/Ergon substation, or abnormal network configuration (inc. inability to detect and clear a network fault)	There is a significant cost premium (>50% of estimates) required to deliver agreed strategic initiative/s	Business impact >\$500,000 total impact of event - for example: cost premium on project, labour 5000hr, reliability impact or opportunity lost
2	Corrupting / loss of data, release of asset / plant data, intellectual property issue	Note 1	There is a cost premium (>25% of estimates) required to deliver agreed strategic initiative/s	Business impact >\$100,000 total impact of event - for example cost premium for project, reliability, opportunity lost

Network Risk Framework

Consequence Scale	Business Rules, Data management & security	Restricted network operation / loss of control, indication, protection	Strategic Direction	Asset and Commercial Impact (including Obsolescence) #
1	Compliance breach with internal guidelines or standards*		There is a cost premium (>10% of estimates) required to deliver the agreed strategic initiatives	Business cost >\$50,000 total impact of event - for example: cost premium for project, reliability, opportunity lost
<p>Note 1: No applicable measure for this dimension. *Not to be used where the external standard is a legislative compliance issue. # Includes impact on any restoration or planned works i.e., disruption to the Program of Work.</p>				

Network Risk Framework

A.4 Network Risk Likelihood Scale

LEGISLATED, CUSTOMER IMPACT & BUSINESS IMPACT LIKELIHOOD SCALE						
Likelihood Scale	Verbal Descriptors Defined Sequence or scenario is the credible combination of evens and risk factors / circumstances required to lead to the chosen Consequence	Single Specific Item e.g., Likelihood of this specific transformer failing in the way described and leading to the chosen Consequence - here and now with the existing risk factors	Past History/ Experience (refer to corporate databases and risk registers)	Probability estimates Whole scenario including the chosen Consequence could occur.... (Used in converting Reliability Assessment Planning to a semi quantitative likelihood)	Generic failure of a chosen asset type for a large population e.g., Likelihood of any RMU of this type failing? Also see past history	
6	Almost certain to occur	Almost certain the defined sequence can and does happen because ALL risk events / risk factors are almost likely to occur or be present	Extreme exposure because All risk factors are poorly controlled throughout the whole lifetime of this asset	Whole scenario including Consequence has been occurring Almost all of the time within the EQL Group or in similar organisations / industries	Approx. 1 chance in 1 or very close to eve time 100%	Could occur daily or more often Approx. 300 times per year
5	Very likely to occur	Very likely the defined sequence can and does happen because most risk events / risk factors are very likely to occur or be present	Very high exposure because most risk factors are present and are not well controlled during most of the lifetime of this asset	Whole scenario including Consequence has been occurring very regularly within the EQL Group or in similar organisations / industries	Approx. 1 chance in 10 10% of the time	Could occur as often as weekly Approx. 50 times per year
4	Likely to occur	Likely the defined sequence can and does happen because many risk events/ risk factors are likely to occur or be present	High exposure because many risk factors are present and are only partly controlled during much of the lifetime of this asset	Whole scenario including Consequence has been occurring regularly within the EQL Group or in similar organisations / industries	Approx. 1 chance in 100 1% of the time	Could occur as often as monthly Approx. 10 times per year
3	Unlikely to occur	Unlikely the defined sequence can happen because most risk events/ risk factors are unlikely to occur or be present	Moderate exposure because many risk factors are not present and are well controlled during many parts of the lifetime of this asset	Whole scenario including Consequence has been occurring now & then within the EQL Group or in similar organisations / industries	Approx. 1 chance in 1,000	Could occur as infrequently as once per year
2	Very unlikely to occur	Very unlikely the defined sequence can happen because most risk events/ risk factors are very unlikely to occur or be present	Low exposure because most risk factors are not present or are well controlled during most parts of the lifetime of this asset	Whole scenario including Consequence has been occurring rarely within the EQL Group or in similar organisations / industries	Approx. 1 chance in 10,000	Could occur as infrequently as once in 10 years
1	Almost no likelihood to occur	Almost no likelihood that the defined sequence can and does happen because almost ALL risk events/ risk factors only occur or would be present in exceptional and rare circumstances	Very low exposure because All risk factors are not present , or All are well controlled during All parts of the lifetime of this asset	Whole scenario including Consequence has been occurring Almost never within the EQL Group or in similar organisations / industries	Approx. 1 chance in 100,000 or even less	Could occur as infrequently as once in 100 years or even less

Network Risk Framework

A.5 Safety Consequence Scale

SAFETY CONSEQUENCE SCALE

Consequence Scale	Degree of Personal Harm	Examples of Types of Harm	Degree of Non-Fatal Harmful Effects Incapacity Disability Impairment	Duration of Non Fatal Harmful Effects Discomfort / Pain / Disability / Impairment	Duration of Business Effects Disabling / Reduced Productivity / Alternate Work / Lost time	Treatment Required	Required Administrative / Regulatory Response
6	Multiple Fatalities / Incurable Fatal Illnesses						
5	Single Fatality / Incurable Fatal Illness		Irreversible Total				
4	Multiple Serious Injuries / Illnesses	Quadriplegia / complete loss of vision / hearing / mobility	Irreversible partial >30%	Permanent / Indefinite / Years	Permanent / Enduring approx months	Hospitalisation - Inpatient / long term / months extensive rehabilitation	
3	Single Serious Injury / Illness	Amputation / paralysis of a limb / severe burns / loss of vision / hearing / mobility	Irreversible partial <30%	Long term / Enduring / Days	Long term / >1 day <1 week	Hospitalisation - Inpatient / short term / days some rehabilitation	External Record & Report Required
2	Minor Injury / Illness	Cuts / burns / strains / sprains	Reversible partial >30%	Short term / approx hours	Short term <1 day	Medical / Outpatient (Doctor) / limited rehabilitation	
1	Low Level Injury / Illness	Scratches / bruises	Reversible partial <30%	Temporary / approx minutes	Approx minutes	First Aid or less	Internal Record & Report Required

A.6 Safety Likelihood Scale

SAFETY LIKELIHOOD SCALE

Likelihood Scale	Verbal Descriptors - Defined sequence of scenario is the credible combination of events and risk factors / circumstances required to lead to the chosen Consequence	Past History / Experience (refer to databases and risk registers)	Exposure to Risk Factors measured in their effects and exposure time period - job duration or task time or operational time or lifetime	Likelihood Estimate can be expressed as a FREQUENCY per year / per climb / per hour / per km The whole scenario including the chosen consequence could occur.....	Likelihood Estimate can be expressed as a PROBABILITY 1 in 100 / 0.01 / 1% / 1E-02 The whole scenario including the chosen consequence could occur.....
6	ALMOST CERTAIN the defined sequence or scenario can and does happen because ALL risk events / risk factors are almost certain to occur or be present	Whole scenario <u>including consequence</u> has been occurring Almost all the time in ours or similar organisations / industries	Extreme EXPOSURE because ALL Risk factors are poorly controlled throughout the whole of the time period	at least daily - or more often ~ 500 times per year	Approx 1 chance in 1 Or very close to everytime 100%
5	VERY LIKELY the defined sequence or scenario can and does happen because most risk events / risk factors are very likely to occur or be present	Whole scenario <u>including consequence</u> has been occurring very regularly in ours or similar organisations / industries	Very high EXPOSURE because most Risk factors present and not well controlled during most of the time period	as often as weekly ~ 50 times per year	Approx 1 chance in 10 10% of the time
4	LIKELY the defined sequence or scenario can and does happen because many risk events / risk factors are likely to occur or be present	Whole scenario <u>including consequence</u> has been occurring regularly in ours or similar organisations / industries	High EXPOSURE because many Risk factors present but are only partly controlled during much of the time period	at least monthly ~ 10 times per year	Approx 1 chance in 100 1% of the time
3	UNLIKELY the defined sequence or scenario can and does happen because many risk events / risk factors are unlikely to occur or be present	Whole scenario <u>including consequence</u> has been occurring occasionally in ours or similar organisations / industries	Moderate EXPOSURE because many Risk factors are not present and are well controlled during many parts of the time period	as infrequently as once per year	Approx 1 chance in 1000
2	VERY UNLIKELY the defined sequence or scenario can and does happen because most risk events / risk factors are very unlikely to occur or be present	Whole scenario <u>including consequence</u> has been occurring rarely in ours or similar organisations / industries	Low EXPOSURE because most Risk factors are not present or are well controlled during most parts of the time period	as infrequently as once in 10 years	Approx 1 chance in 10,000
1	ALMOST NO LIKELIHOOD the defined sequence or scenario can and does happen because almost ALL risk events / risk factors only occur or be present in exceptional and rare circumstances	Whole scenario <u>including consequence</u> has been occurring almost never in ours or similar organisations / industries	Very Low EXPOSURE because ALL Risk factors are not present or ALL are well controlled during ALL of the time period	as infrequently as once in 100 years or even less	Approx 1 chance in 100,000 or even less

Network Risk Framework



Part of Energy Queensland

A.7 Environment Consequence Scale

Consequence Scale	Release / Spill / Contaminate / Pollutant Material					Biodiversity (losing)			Biosecurity (preventing)	
	Quantity	Extent	Resources Required	Degree of Toxicity	Degree of Contamination	Nature of Fauna effected	Nature of Flora effected	Duration of Disruption to Ecosystem	Nature of Fauna Effects	Nature of Flora Effects
6	>20,000 litres SF ₆ >100kg	Widespread area of contamination beyond property / worksite boundary	Emergency situation declaration	Note 1	Irreversible contamination of the environment	Species extinction	Species extinction	Total Loss	Introduction of new exotic species	Introduction of new species
5	>10,000 <20,000 litres SF ₆ ≥50 - ≤100kg	Offsite – beyond property / worksite and enters water course	Emergency services assistance required	Highly Toxic	Long-term contamination of the environment	Endangered species affected	Highly sensitive and endangered vegetation harmed	Long-term	Introduce, spread, or supply Class 1 pest	Introduce, spread, or supply Class 1 pest
4	>5,000 <10,000 litres SF ₆ ≥25 - ≤50kg	Offsite – beyond property / worksite but prevented from entering water course	Contained by with outside assistance required	Seriously Toxic	Short-term contamination of the environment	Vulnerable species affected	Highly sensitive and of concern vegetation harmed	Medium-term	Introduce, spread, or supply Class 2 pest	Introduce, spread, or supply Class 2 pest
3	>1,000 <5,000 litres SF ₆ ≥10 - ≤25kg	NOT beyond property / worksite alignment border but threatens to cross-boundary	Can be internally managed and internal resources capable of clean-up	Moderately Toxic	High level of nuisance	Threatened species affected	Not of concern remnant vegetation harmed	Short-term	Introduce, spread, or supply Class 3 pest	Introduce, spread, or supply Class 3 pest
2	>200 <1,000 litres SF ₆ ≥1.0 - ≤10kg	NOT beyond property boundary / worksite alignment border	Can be internally managed and on-site resources capable of clean-up	Slightly toxic	Some nuisances	Least concern species harmed	Low sensitivity and vulnerable environment harmed	Note 1	Note 1	Note 1

Network Risk Framework

Consequence Scale	Release / Spill / Contaminate / Pollutant Material					Biodiversity (losing)			Biosecurity (preventing)	
	Quantity	Extent	Resources Required	Degree of Toxicity	Degree of Contamination	Nature of Fauna effected	Nature of Flora effected	Duration of Disruption to Ecosystem	Nature of Fauna Effects	Nature of Flora Effects
1	<200 litres SF ₆ <1.0kg	Very localised - close to activity zone or within spill containment structure/ bunding	Can be internally managed and very little clean-up required	Not particularly toxic	Low or no nuisance	Least concern species threatened	Least concern species threatened			

Note 1: No applicable measure for this dimension.

Network Risk Framework

Consequence Scale	Regulatory			Cultural Heritage		Public Impact		
	Statutory approval required #	Regulatory Descriptors	Rectification Remediation / Clean-up Costs	Indigenous Cultural Heritage	Non-Indigenous Cultural Heritage	Carbon Cost *	Public Health Effects	Public Relations Impact
6	Activities are conducted without statutory approval/s	Note 1	Unknown & / or on-going costs of clean-up & / or management	Destruction of human remains	Note 1	Extreme	Exposure to chronic health effects	Extensive public outrage, call for replacement of Directors and / or Executive management
5	Note 1	Extensive serious environmental harm	<\$5,000,000 and >\$500,000	Disturbing human remains etc.	Destruction of registered State heritage place	Very high	Exposure to acute health effects	Public Outrage, call for enquiry, substantial negative media campaign. Brand damage
4		Serious environmental harm	<\$500,000 and >\$50,000	Destruction of artefacts, medicine, or scar trees etc.	Disturbance of registered State heritage place	High	Short-term public health impact	Adverse national media attention (e.g., disruption to large public events). Loss of public trust
3		Material environmental harm	<\$50,000 and >\$5,000	Disturbance of artefacts, medicine, or scar trees etc.	Disturbance of a place that may be eligible to be registered State heritage place	Medium	Minimal public health impact	Adverse regional media attention. Loss of customer trust / action groups formed
2		Lawful environmental harm	<\$5,000 and >\$500	Note 1	Note 1	Low	Some nuisances	Adverse local media attention or negative external publicity. Multiple customer complaints
1		Unregulated matters and environmental nuisance (complaint)	<\$500	Lack of consultation with EPA / DNR or indigenous group/s		Very Low	Low or no nuisance	Few customer complaints and or external criticism

Note 1: No applicable measure for this dimension
 * Commercial Cost may also be associated with this impact.
 # Legislative risk may also be associated with this impact

Network Risk Framework

A.8 Environment Likelihood Scale

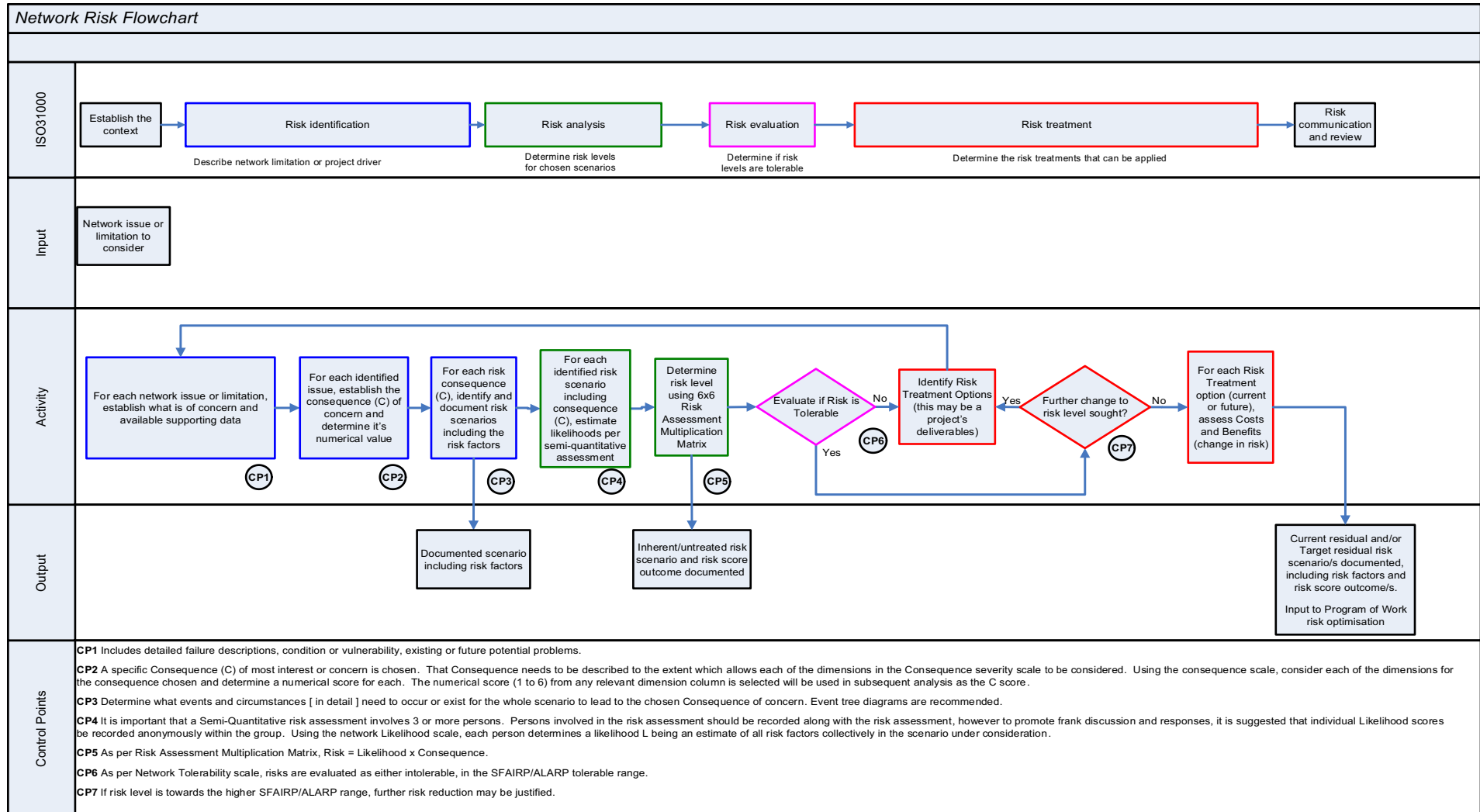
ENVIRONMENT LIKELIHOOD SCALE – use columns 2 and 3 as a minimum and all other columns where required/necessary

Likelihood Scale	Verbal Descriptors Defined sequence or scenario is the credible combination of events and risk factors / circumstances required to lead to the chosen Consequence. (Likelihood estimate must consider the whole scenario including the chosen Consequence).	Past History / Experience refer to databases and risk registers)	Exposure to Risk Factors Measured in their effects and exposure time period Job duration or task time or operational time or lifetime	Likelihood Estimate can be expressed as a FREQUENCY The whole scenario including the chosen Consequence could occur	Likelihood Estimate can be expressed as a PROBABILITY The whole scenario including the chosen Consequence could occur
6	Virtually certain the defined sequence can and will happen because ALL risk events/ risk factors are almost likely to be present.	It has been a common / very Frequent Occurrence in our organisation / industry (It = whole scenario including the Consequence).	Extreme EXPOSURE because ALL risk factors are poorly controlled throughout the whole of the time period.	At least daily - or more often than 300 times per year.	At least as often as 1 chance in 10 times or even more often (at least 10% of the times) or up to every time (1:1)
5	Very likely that the defined sequence can and will happen because most risk events/ risk factors are very likely to occur or be present.	It is known to have frequently occurred / happened in our organisation / industry (It = whole scenario including the Consequence).	Very high EXPOSURE because most risk factors present and not well controlled during most parts of the time period.	As often as weekly - 50 times per year.	Between 1 chance in 10 times and 1 chance in 100 times . Between 10% and 1% of the times.
4	Possible and likely that the defined sequence can and will happen because many risk events/ risk factors are likely to occur or be present.	Have heard of it happening regularly before in our organisation / industry (It = whole scenario including the Consequence).	High EXPOSURE because many risk factors present but are only partly controlled during much of the time period.	As often as monthly - 10 times per year.	Between 1 chance in 100 times and 1 chance in 1,000 times .
3	Possible but unlikely that the defined sequence can and will happen because many risk events/ risk factors are unlikely to occur or be present.	Have heard of it happening occasionally before in ours or similar organisations / industries (It = whole scenario including the Consequence).	Moderate EXPOSURE because many risk factors are not present and are well controlled during many parts of the time period.	As infrequently as once per year.	Between 1 chance in 1,000 times and 1 chance in 100,000 times .

Network Risk Framework

Likelihood Scale	<p>Verbal Descriptors</p> <p>Defined sequence or scenario is the credible combination of events and risk factors / circumstances required to lead to the chosen Consequence.</p> <p>(Likelihood estimate must consider the whole scenario including the chosen Consequence).</p>	<p>Past History / Experience</p> <p>refer to databases and risk registers)</p>	<p>Exposure to Risk Factors</p> <p>Measured in their effects and exposure time period Job duration or task time or operational time or lifetime</p>	<p>Likelihood Estimate can be expressed as a FREQUENCY</p> <p>The whole scenario including the chosen Consequence could occur</p>	<p>Likelihood Estimate can be expressed as a PROBABILITY</p> <p>The whole scenario including the chosen Consequence could occur</p>
2	<p>Very unlikely that the defined sequence can and will happen because most of the risk events/ risk factors are very unlikely to occur or be present.</p>	<p>Rarely heard of in ours or similar organisations / industries (It = whole scenario including the Consequence).</p>	<p>Low EXPOSURE because most risk factors are not present or are well controlled during most parts of the time period.</p>	<p>As infrequently as once in 10 years.</p>	<p>Between 1 chance in 100,000 times and 1 chance in 1,000,000 times.</p>
1	<p>Extremely unlikely that the defined sequence can and will happen because almost ALL of the risk events/ risk factors only occur or would be present in exceptional and rare circumstances.</p>	<p>Unheard of in ours or similar organisations / industries (It = whole scenario including the Consequence).</p>	<p>Very Low EXPOSURE because ALL risk factors are not present, or ALL are well controlled during ALL of the time period.</p>	<p>As infrequently as once in each 100 years or even less.</p>	<p>As little as 1 chance in 1,000,000 times or even less.</p>



Annex B NETWORK RISK PROCESS FLOWCHART



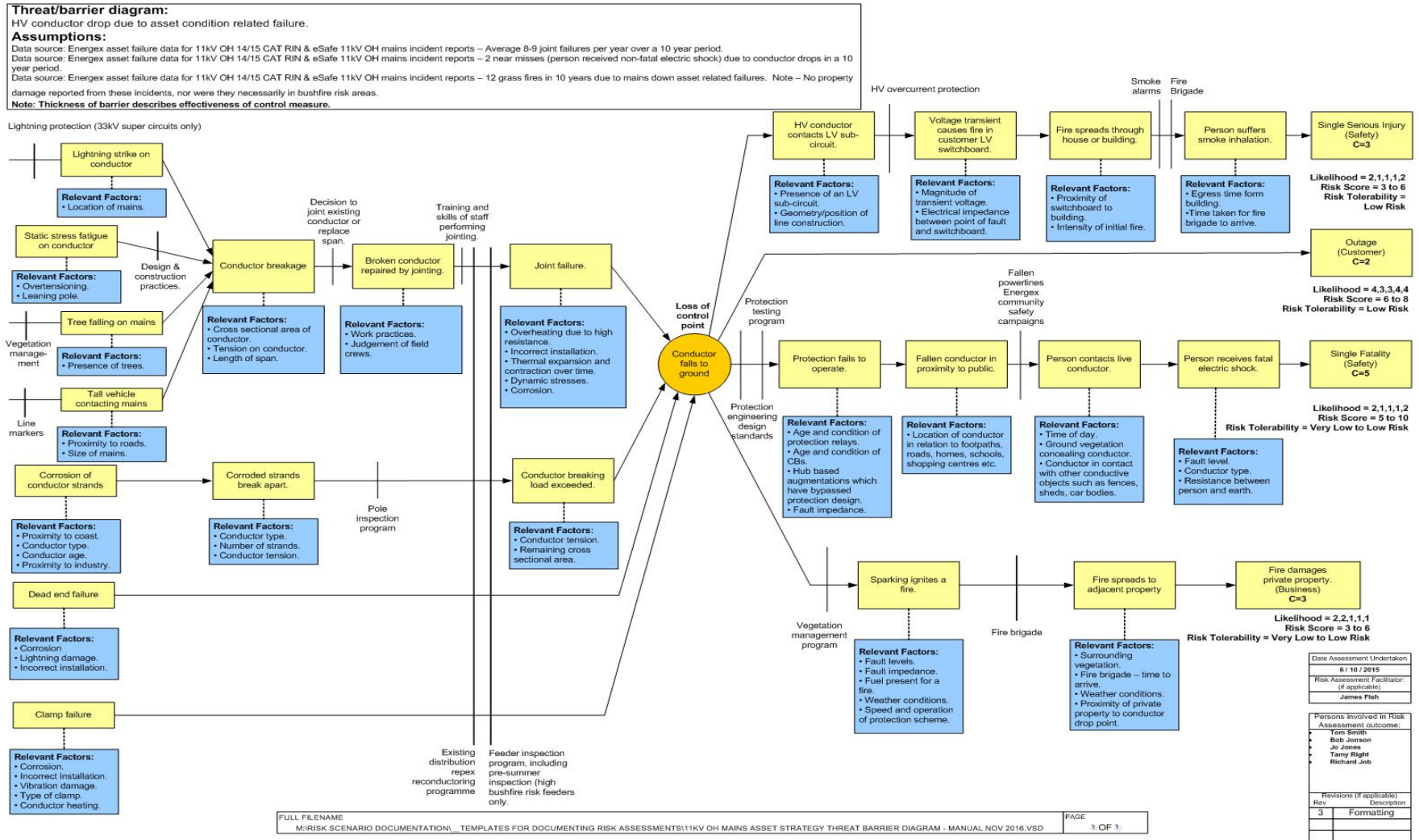
Annex C NETWORK RISK EVENT TREE EXAMPLES

<p>TITLE</p> <p style="text-align: center;">Example Safety Risk Assessment (Community Safety)</p>																					
<p>Example Scenario: Excavation in vicinity to ENERGEX Underground Cables, and person manually excavating / digging contacts mains resulting in a fatality</p>																					
<p>Current Residual Risk Level (with all risk factors in place and effective)</p>																					
<p>Person manually excavating near ENERGEX Underground Mains</p> <p>Using steel crowbar LV Mains</p>	<p>Knowledge of ENERGEX Assets in the Area</p> <p>Excavator gains access to Live U/G Cable</p> <p>Person makes contact with "Live" Mains or Excavator</p> <p>Education & Advertising</p>																				
<p>Protection does not prevent injury to Person</p> <p>Person receives Fatal Shock Current</p> <p>Person part of circuit path through direct contact</p> <p>Clothing Footwear</p>	<p style="text-align: center; background-color: orange; color: white; padding: 5px;">Single Fatality</p> <p style="text-align: center;">C = 5</p>																				
<p>Risk Factors</p> <ol style="list-style-type: none"> 1. Dial before you Dig (Accuracy of ENERGEX records) 2. Excavator Operator is trained and authorised (check if there is an Industry Authorisation scheme in place) 3. Physically locate cable by hand digging 4. ENERGEX Awareness publications / training information of steps to take before digging near U/G cables for earth moving Equipment operators. 5. Codes of Practice for excavation 6. ENERGEX Standards and methods for installation of U/G Mains (ie. Orange Plastic marker tape, clay tile, etc) 																					
<p>Qualitative Risk Assessment</p> <p>Scores = Low, Medium, Low, Low</p>																					
<p>Semi-Quantitative Risk Assessment</p> <p>Likelihood L = 2, 2, 3, 3</p> <p>R = C x L, R = 5 x 2 to 3 = 10 to 15</p>																					
<p>Risk Tolerability</p> <p>Risk score of 10 to 15 = Low to Moderate Risk</p>																					
<p>For Text in Red – Maintaining or increasing focus in these areas could improve the risk outcome</p>																					
<p>FULL FILENAME</p> <p style="text-align: center;">VISIODOCUMENT</p>	<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2">Date Assessment Undertaken</td> </tr> <tr> <td colspan="2" style="text-align: center;">28/05/2008</td> </tr> <tr> <td colspan="2">Risk Assessment Facilitator: (if applicable)</td> </tr> <tr> <td colspan="2"> </td> </tr> <tr> <td colspan="2">Persons involved in Risk Assessment outcome: 4 persons</td> </tr> <tr> <td colspan="2"> </td> </tr> <tr> <td colspan="2">Revisions (if applicable)</td> </tr> <tr> <td style="width: 10%;">Rev</td> <td>Description</td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </table>	Date Assessment Undertaken		28/05/2008		Risk Assessment Facilitator: (if applicable)				Persons involved in Risk Assessment outcome: 4 persons				Revisions (if applicable)		Rev	Description				
Date Assessment Undertaken																					
28/05/2008																					
Risk Assessment Facilitator: (if applicable)																					
Persons involved in Risk Assessment outcome: 4 persons																					
Revisions (if applicable)																					
Rev	Description																				
<p>PAGE</p> <p style="text-align: center;">1 OF 1</p>	<p> </p>																				

Network Risk Framework

TITLE: Environment Risk Assessment – Example Scenario only																					
Example Scenario only: Transformer tank failure at SSSDM Somerset Dam substation leading to leak of transformer oil into the nearby waterway																					
Inherent/Untreated Risk (semi-quantitative)																					
																					
<p>Risk Factors</p> <ol style="list-style-type: none"> 1. Age of transformer (65 years) 2. Transformer oil contains (4.76 ppm) PCB 3. Total transformer oil volume approx. 3200L 4. No transformer oil bunding or containment (but temporary oil socks present) 5. Substation located on river bank in close proximity to Somerset Dam causeway 6. Through fault on transformer 7. Condition of transformer and seals 8. Vandalism - substation fence not current standard 	<p>Risk Assessment Likelihood L = 4 (High exposure as many risk factors are present and only partly controlled)</p> <p>$R = C \times L, R = 5 \times 4 = 20$</p> <p>Risk Tolerability Risk score of 20 = High Risk</p>																				
Target Residual Risk (semi-quantitative) after completion of network project WR131604 – 2nd TR and oil containment																					
																					
<p>Risk Factors</p> <ol style="list-style-type: none"> 1. Age of transformer (65 years) 2. Transformer oil contains (4.76 ppm) PCB 3. Total transformer oil volume approx. 3200L <li style="color: red;">4. Substation oil containment installed 5. Substation located on river bank in close proximity to Somerset Dam causeway 6. Through fault on transformer 7. Condition of transformer and seals 8. Vandalism - substation fence upgraded to current standard (electric fence) 	<p>Risk Assessment Likelihood L = 1</p> <p>$R = C \times L, R = 5 \times 1 = 5$</p> <p>Risk Tolerability Risk score of 5 = Very Low Risk</p>																				
For Text in Red – Maintaining or increasing focus in these areas could improve the risk outcome																					
FULL FILENAME: VISIODOCUMENT	PAGE: 1 OF 1																				
<table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td colspan="2">Date Assessment Undertaken</td> </tr> <tr> <td colspan="2" style="text-align: center;">/ /</td> </tr> <tr> <td colspan="2">Risk Assessment Facilitator: (if applicable)</td> </tr> <tr> <td colspan="2"> </td> </tr> <tr> <td colspan="2">Persons involved in Risk Assessment outcome:</td> </tr> <tr> <td colspan="2"> </td> </tr> <tr> <td colspan="2">Revisions (if applicable)</td> </tr> <tr> <td style="font-size: small;">Rev</td> <td style="font-size: small;">Description</td> </tr> <tr> <td> </td> <td> </td> </tr> <tr> <td> </td> <td> </td> </tr> </table>		Date Assessment Undertaken		/ /		Risk Assessment Facilitator: (if applicable)				Persons involved in Risk Assessment outcome:				Revisions (if applicable)		Rev	Description				
Date Assessment Undertaken																					
/ /																					
Risk Assessment Facilitator: (if applicable)																					
Persons involved in Risk Assessment outcome:																					
Revisions (if applicable)																					
Rev	Description																				

Annex D SAMPLE BOW TIE/ THREAT BARRIER DIAGRAM



Network Risk Framework

Annex E RISK ASSESSMENT RECORD (SEMI-QUANTITATIVE)

[\(Tools and Templates link\)](#)

Risk Assessment									
Risk Assessment Title									
Task									
Risk Scenario									
Scenario Sequence	Consider below for each event in the scenario sequence: - Risk Factors - Hazards - Missing or Ineffective controls - System Factors for each Event	>		>		>		>	Chosen Consequence 3 - Single Serious Injury/Illness
Risk Factors	Risk Factors: List the risk factors which could influence the likelihood/chances of each event occurring								
Existing Controls	Existing Controls: List the existing controls currently in place								
New Controls	Controls: List the proposed or new controls to be implemented								
Inherent Risk / Existing Controls					Residual Risk (New Controls)				Notes: (Include any actions required as follow up to risk assessment)
Name	Consequence	Likelihood	Total	Tolerable Yes or No	SOFAIRP (Yes or No)	L/hood with additional controls	New Total	SOFAIRP (Yes or No)	
1	6.00	0	0.00			0.00	0.00		
1		0	0.00			0.00	0.00		
1		0	0.00			0.00	0.00		
1		0	0.00			0.00	0.00		
1		0	0.00			0.00	0.00		
1		0	0.00			0.00	0.00		
1		0	0.00			0.00	0.00		
1		0	0.00			0.00	0.00		
1		0	0.00			0.00	0.00		
1		0	0.00			0.00	0.00		
Total People	6.00	0.00	0.00			0.00	0.00		
Result	10	6.00	0.00	0		0	0.00		
Risk Assessment number:									
Risk assessment requested by:									
Risk assessment facilitated by: XXX									
Facilitation Date: XX/XX/XXXX									
Risk assessment approved by:									
Comments:									

Annex F SIMPLE RISK ASSESSMENT TEMPLATE

[\(Tools and Templates link\)](#)

Simple Network Risk Assessment Template



***** All items highlighted in yellow need to be updated/removed in this template*****

Risk Title/Name								
Include a short description to explain the risk being assessed.								
Risk Context and Background								
What is the actual issue and background and what uncertainty do we need to address? Outline how the issue was identified. Outlined why we're worried about it (e.g. "There is a risk of catastrophic failure of the circuit breaker") Work Order/Work Request Details: XX Compliance/RBD Date: XX Defect Classification: XX Planned Construction/Rectification Dates: XX								
Considerations and Issues				Risk Factors				
<ul style="list-style-type: none"> Consider things that may influence what we do or can impact what we can do Consider our existing controls and how effective they are SME's involved to date: <ul style="list-style-type: none"> X 				Risk Increasing Factors <ul style="list-style-type: none"> <Insert things that make the risk worse> Risk Reduction Factors <ul style="list-style-type: none"> <Insert things that make the risk better> 				
Risk Category	Risk Scenario	Current Residual Risk Score			Current Controls / Mitigations	Residual Planned Risk (Target) Scores		Additional Planned Controls / Mitigations (Immediate controls to minimise the risk and be on track for the target to be achieved i.e. project delivery)
		C	L	Score		L	Score	
Safety	Catastrophic failure of X results in a EQL worker being struck by debris and sustaining a single serious injury.	3	4	12 Moderate	<ul style="list-style-type: none"> Worksite Hazard Management Personal Protective Equipment 	2	6 - Low	Immediate / Temporary Controls <ul style="list-style-type: none"> Update / New Work Practice 1234 Widget / Barrier Network Access Restriction / Safety Alert

Appendix A

Document History

A.1 Revision History

Revision date	Version number	Author	Description of change/revision
02/10/2018	5		Initial release of the joint Network Risk Framework for Ergon Energy and update for Energex in corporate document management system. This document replaces the (2008) Network Risk Framework Manual and Network Risk Framework Procedure. It reflects the incorporation of existing network risk management practices shared across Energex and Ergon Energy as an aligned sub-framework of the EQL Enterprise Risk Architecture.
04/05/2021	6		Updates to legislative references, organisational names, and software systems.
24/09/2021	7		Update to: <ul style="list-style-type: none"> Recording and storage of risk assessment records Risk Tolerability table- approvals and actions Legislative risk consequence level 4 and 5 Updates to document links
20/07/2022	8		Update to: <ul style="list-style-type: none"> Definitions as provided by Enterprise Risk team ECM Document links Qualitative Risk Assessment descriptor
09/11/2022	9		Republishing in ECM
21/07/2023	10		Update to: <ul style="list-style-type: none"> Definition changes as per Based on ISO 31073: 2022 Risk management – Vocabulary.

Network Risk Framework

Revision date	Version number	Author	Description of change/revision
			<ul style="list-style-type: none">• Linkages to EQL Risk Standard and Manuals• NREM – spelling/wording change and Updates to Environment including SF6, Customer and Political Sensitivity to Align to EQL REM, Addition of Commercial Cost to Asset Impact, Wording alignment to Legislative and EQL REM. Updated Examples.

A.2 Document Approvals

Name	Position title	Signature	Date
Ingrid Fuentes	Manager Network Safety and Risk		
Sharyn Scriven	General Manager Grid Investment		