TasNetworks Framework

RISK MANAGEMENT FRAMEWORK

Version 1.0

March 2015

Framework Overview

This framework provides an overview of the TasNetworks approach to risk management.

The framework contains two primary components – the strategic framework elements and the risk management process (or model).

Framework Ownership

Name	Position	Contact
Paul McTaggart	Team Leader – Compliance & Risk	paul.mctaggart@tasnetworks.com.au (03) 62716210

Framework Authorisation

Approval Date	Approval	Review Cycle	Next Review
26 March 2015	TasNetworks Board	Annual	30 June 2016

Framework Version Control

Version	Issue Date	Overview of Change(s)
1.0	26 March 2015	Initial framework development/approval. Endorsement by the TasNetworks Leadership Team and approval by the TasNetworks Board.

TABLE OF CONTENTS

1. Introduction

The effective management of risk is central to the core business and efficient management of TasNetworks.

Our approach to risk management involves managing to achieve an appropriate balance between realising opportunities for gains while minimising adverse impacts. Risk management is viewed as an integral part of good management practice and an essential element of good corporate governance.

An integral part of how TasNetworks operates is the identification and treatment of risk, so all our stakeholders prosper. Our ability to deliver electricity and telecommunications network services and create value for our customers, owners and our community is significantly influenced by the effectiveness of our management of risk.

Our risk management effectiveness is influenced by the level of integration with the way we operate and our business practices and processes.

TasNetworks aims for risk management to become part of the culture, embedded into our operating philosophy, business practices and processes.

1.1. Purpose

The purpose of this framework is to:

- Demonstrate the commitment and approach to the management of risk – how it is integrated with existing business practices and processes and ensure risk management is not viewed or practiced as an isolated activity;
- Set a consistent and structured approach for the management of all types of risk; and
- Provide an overview on how to apply the risk management process.

1.2. Scope and Approach

The TasNetworks Risk Management Policy requires the management of all risks using a consistent framework and structured processes.

To comply with the approved Risk Management Policy, TasNetworks adopts a structured approach utilising consistent methods for the assessment and treatment of all types of risk, at all organisational levels and for all activities.

Risk management is not viewed or practiced as an isolated activity.

We aim to embed risk management into all business processes, so we identify and manage risks in a consistent and proactive way before they can affect the achievement of our objectives.

After significant events, changes and decisions, we apply systematic processes to learn any lessons from our failures and successes.

We maintain contemporary processes for control assurance, focussed on key controls, to improve our ability to continuously manage risks.

Embedding risk management in this way leads to everyone at TasNetworks becoming involved in the management of our risks, and facilitates a culture of continuous improvement. This embedded approach assists TasNetworks to act on opportunities to gain competitive advantage, achieve sustainable growth and further enhance shareholder value.

Responsibility for the management of risk rests with all employees. Those responsible for the management of risks are also responsible for the continued adequacy and effectiveness of controls.

The Board and Leadership Team ensures that the necessary resources are available to enable the effective management of risk in accordance with this framework.

1.3. Corporate Governance Requirements

The TasNetworks approach to risk management has been designed to achieve, at a minimum, the following policy and corporate governance requirements:

SOURCE	REQUIREMENTS
TasNetworks Risk Management Policy	• TasNetworks intend to adopt best practice risk management policies and approaches. • TasNetworks will align its underlying risk principles to *AS/NZS ISO31000:2009 Risk Management – Principles and Guidelines.*
Tasmanian Government Corporate Governance Principles - Guidelines for Tasmanian Government Businesses *Recognise and Manage Risk*	• Companies should establish a sound system of risk oversight and management and internal control.
ASX Corporate Governance Council Principles (Principle 7) - *Recognise and Manage Risk*	• An entity should establish a sound risk management framework and periodically review the effectiveness of that framework.

1.4. Adherence to Standards

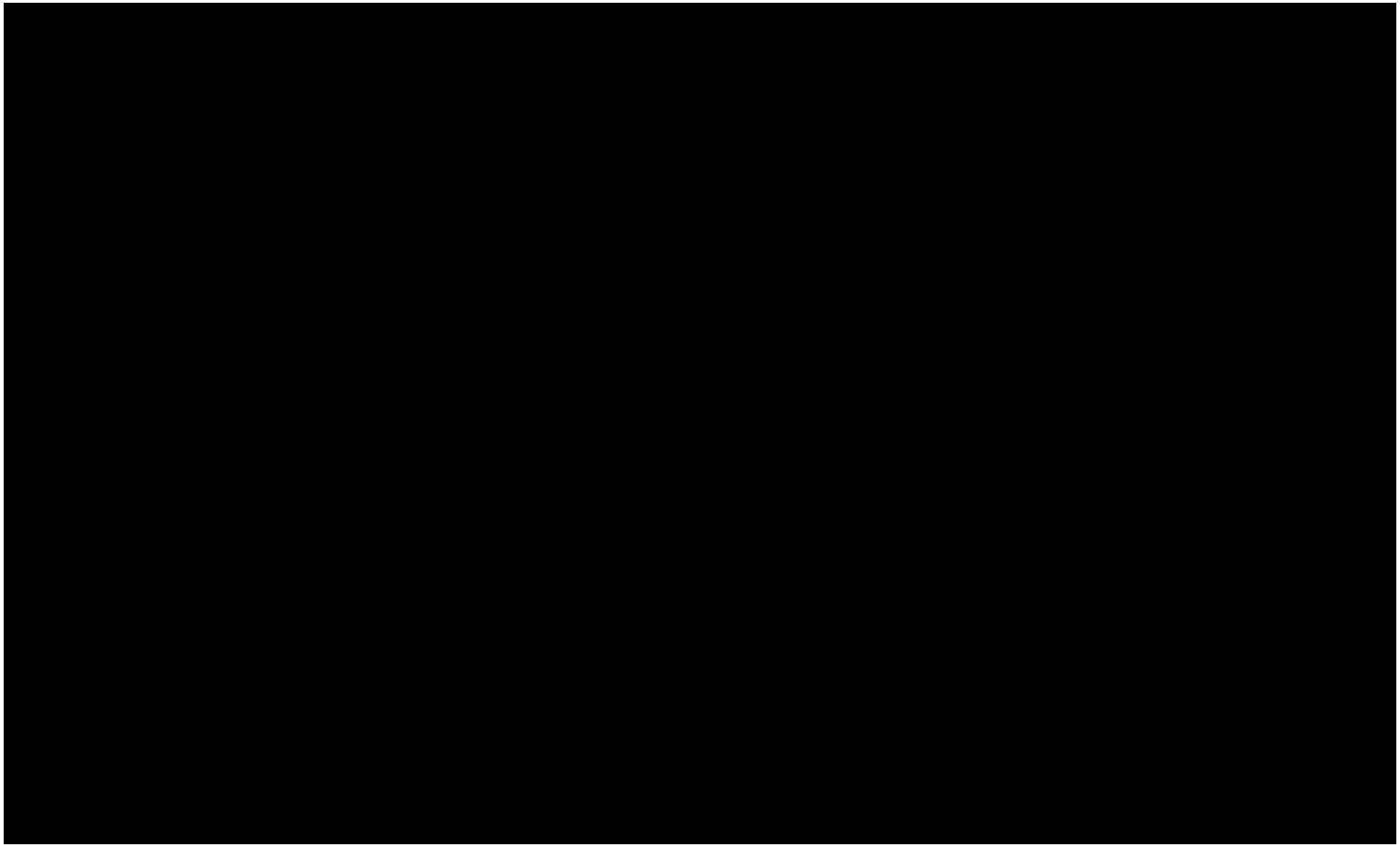
The following standards form the basis for the TasNetworks approach to risk management:

COMPONENT	STANDARD
Risk management framework	• Developed in accordance with *AS/NZS ISO 31000:2009 – Risk Management - Principles and Guidelines.*
Risk assessment techniques	• Guided by *ISO 31010 – Risk Management – Risk Assessment Techniques.*
Integration of risk management and assurance	• Based on *HB 158:2010 – Delivering Assurance based on ISO 31000:2009 – Risk Management Principles and Guidelines.*

2. Framework Components

The risk management framework encompasses two related components - the strategic component and the tactical component:

Framework for Risk Management



COMPONENT	OVERVIEW
STRATEGIC	• The ability of TasNetworks to effectively manage risk in accordance with our risk appetite statement depends on our risk management intentions and our capacity to achieve these intentions – this is the *risk management framework* (which is a component of the broader TasNetworks system of governance). • These overarching components provide the foundations to enable, support and govern risk management, so the operational risk management process can occur effectively across TasNetworks. • The implementation and evolution of these framework components (the intent, capability, accountability and continual improvement) are addressed via the risk management plan. • The TasNetworks risk management plan details how TasNetworks will implement, maintain and enhance our approach to risk management.
TACTICAL (OPERATIONAL)	• The tactical risk management process (or the risk management model) is the operational process applied in the identification, analysis, evaluation and treatment of risk. • This is 'how' the risk management process is applied across TasNetworks. • This risk management process has been developed in accordance with *AS/NZS ISO 31000:2009 – Risk Management - Principles and Guidelines*, and is designed to be applied to all types of risk across all levels of TasNetworks.

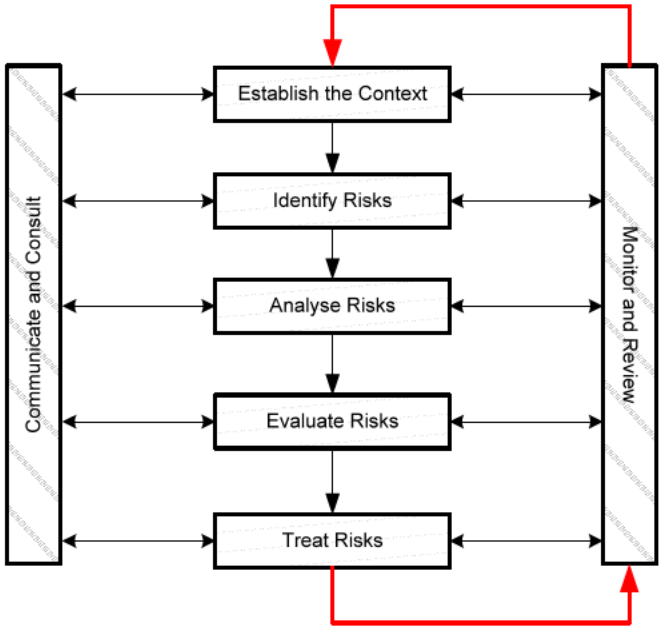
2.1. Risk Management Integration

TasNetworks focuses on three primary processes to effectively embed risk management into our existing business practices:

PERSPECTIVE	TASNETWORKS APPROACH
ROOT CAUSE ANALYSIS	• After any significant failure or success we conduct suitable root cause analysis to learn lessons from these failures and successes – aiming to drive a culture of continuous improvement. • Suitable root cause analysis is transparent and collaborative, involves stakeholders, records lessons learnt and implements actions to treat the causes. The rigour of the root cause analysis is determined by the complexity of the issue. • The lessons are recorded and actions taken to ensure that the causes are treated to prevent subsequent failures and repeat successes.
CONTROL ASSURANCE	**Controls which are business critical will be allocated to named control owners for checking and assurance:** • Key control owners are responsible for ensuring there is a process in place for their key controls to be periodically checked and assured, to verify they are adequate and effective. • Control assurance is a planned and deliberate activity, with the design of new risk controls encompassing when, by what means, and by whom, control assurance takes place. **Control assurance encompasses:** • Specific day-to-day control checks, preferably built into systems and procedures. • Periodic reviews by the control owner using control self-assessments. • Occasional verification by internal and external audit staff, who are independent of line management.
RISK ASSESSMENT	• Suitable risk assessments are conducted as part of the development of all strategic plans, business plans and project business cases. • These risk assessments are used to identify significant risks that could affect the achievement of the relevant plan or business case objectives. • Before any significant change, decision or event occurs, or when a significant external change or event is detected, a suitable risk assessment is conducted to determine the appropriate risk treatment. • The rigour of these risk assessments is determined by the severity of the potential consequences (higher potential consequences generally equals a higher level of rigour).

3. Risk Management Process

The TasNetworks operational process for the management of risk is illustrated below:



The following sections provide guidance for the operational risk management process (from establishing the context through to risk treatment).

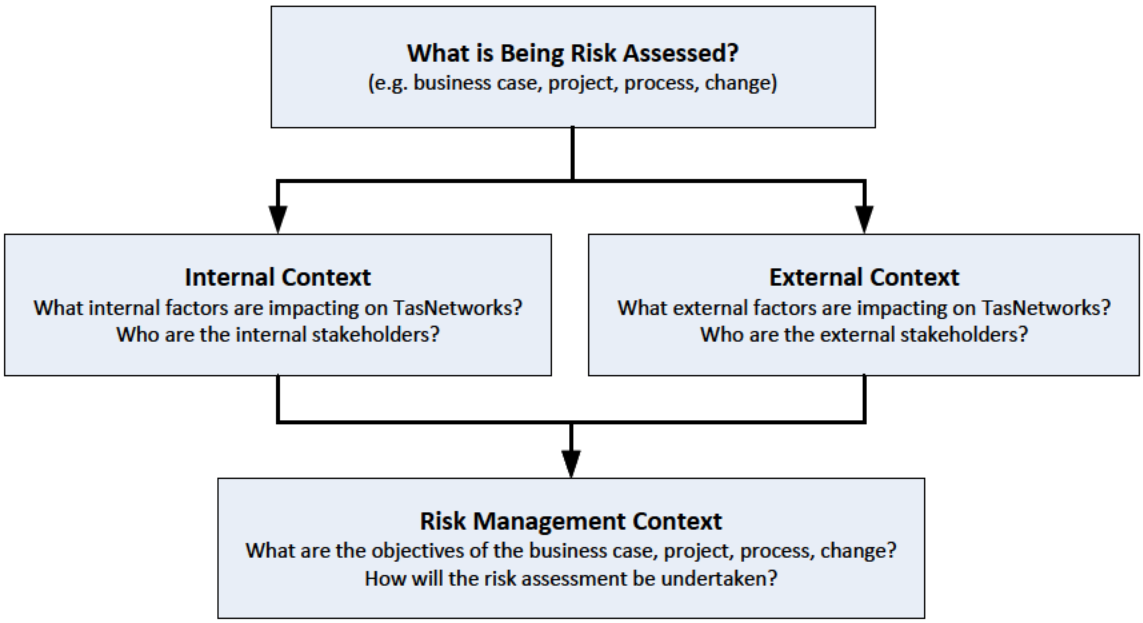
3.1. Establish the Context

Before any risk identification exercise is undertaken, a process is undertaken to establish the context.

Establishing the context identifies and documents the parameters within which risks will be managed and sets the scope, boundaries and methods to be used for the risk management process.

A key aim of the establish the context step is to identify the TasNetworks objectives and those internal and external factors that could be a source of uncertainty, to assist in the identification of potential risks.

Three contexts are established prior to undertaking a risk assessment:



3.1.1. Internal Context

Establishing the internal context is about understanding the internal characteristics of TasNetworks and identifying anything that may influence the way in which TasNetworks can and will manage risk.

INTERNAL CONTEXT	Internal stakeholders (e.g. Board, TLT, staff).
	Organisational (or divisional) structure and culture.
	Capabilities - e.g. people, competencies, systems, processes.
	TasNetworks goals, objectives and critical success factors – including the strategies in place to achieve these.

3.1.2. External Context

Establishing the external context is about understanding the relationship between TasNetworks and our external environment.

EXTERNAL CONTEXT	External stakeholders (including their objectives and how they measure TasNetworks success).
	Regulatory, social, cultural, financial, political and competitive environments.
	Strengths, weaknesses, opportunities and threats.
	Key business drivers.

- It is particularly important to take into account the objectives of external stakeholders to ensure their objectives are considered in the risk management process.
- To gain this understanding, consultation with the stakeholder is generally undertaken to fully understand their objectives and concerns.

3.1.3. Risk Management Context

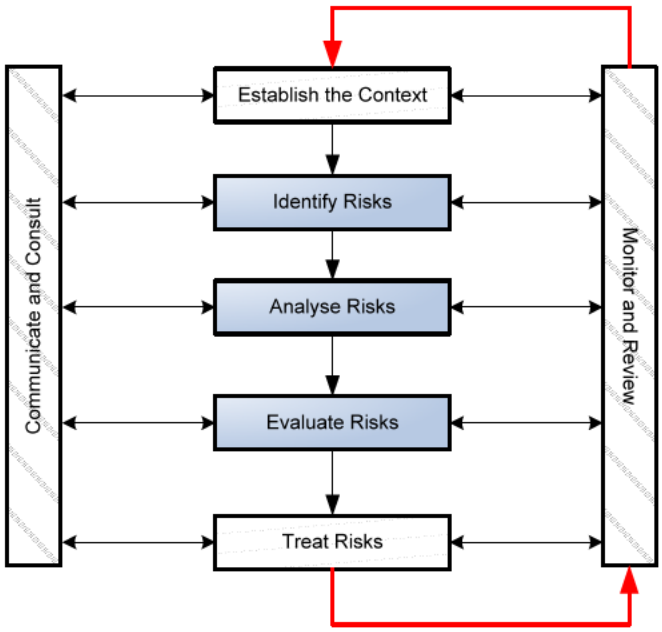
Establishing the risk management context sets the scope, boundaries and approach for the risk management activity, and provides an overview for how the risk management process will be applied.

RISK MANAGEMENT CONTEXT	Clear definition of the project, process, change or decision that is to be subject to the risk management process: • Objectives. • Success criteria (how success will be measured and achieved). • Timeframe and location of the activity.
	Detailing the nature of the decisions that have to be made based on the risk assessment results (for example whether or not to proceed with a change or the approval of proposed capital expenditure).
	Defining the breadth, depth and rigour of the risk assessment - including any specific inclusions and exclusions.

3.2. Risk Assessment

Risk assessment encompasses three steps in the risk management process:

1. Risk identification.
2. Risk analysis.
3. Risk evaluation.



3.2.1. Identify Risks

This involves the identification of what, why, where, when and how events could either harm or enhance the achievement of the TasNetworks objectives.

This step seeks to identify the risks to be managed:

- Comprehensive identification using a well-structured systematic process is critical, because risks not identified at this stage are excluded from further analysis and treatment.
- Identification should include all risks – including those that are not under the control of TasNetworks.

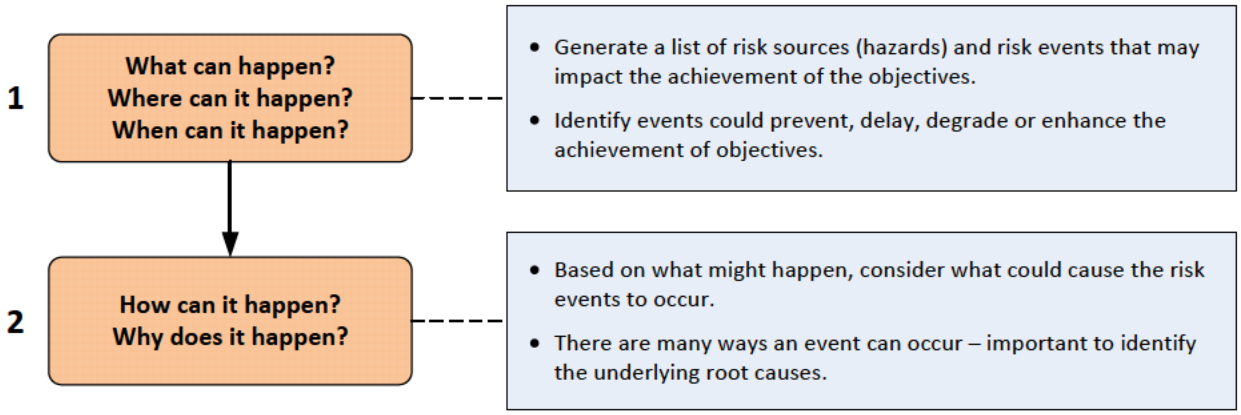
TasNetworks utilises multiple methods for risk identification:

- These range from quite detailed and rigorous techniques such as a hazard and operability studies (HAZOP), failure modes and effects and critically analysis (FMECA) and reliability centred maintenance (RCM), to softer less rigorous approaches like brainstorming and checklists.
- The structure and rigour of the risk identification process adopted reflects the complexity of the problem/issue and the severity of the potential consequences.

The selection of the appropriate risk identification technique is guided by *ISO 31010 – Risk Management – Risk Assessment Techniques.*

3.2.1.1. Risk Identification Steps

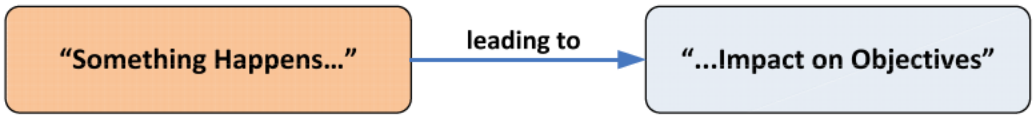
The risk identification process has two primary steps to identify potential risk events and the underlying causes of these events:



It is important to regularly confirm the currency of the risks identified, particularly when there are material changes in the external or internal environments or changes in the expectations of stakeholders.

3.2.1.2. Risk Expression

Risks are expressed in the following format:



Risk statements always contain a link back to one or more of the relevant objectives.

3.2.2. Analyse Risks

A qualitative method of risk analysis is employed at TasNetworks to prioritise risks for attention.

Risk analysis provides a detailed understanding of the identified risk and provides an input for decisions on whether risks need additional control and, if so, the most appropriate and cost effective approach:

- Involves consideration of the sources of risk, their positive and negative consequences and the likelihood that those consequences may occur.
- Risk is analysed by combining the consequence and likelihood, taking into account existing control measures.

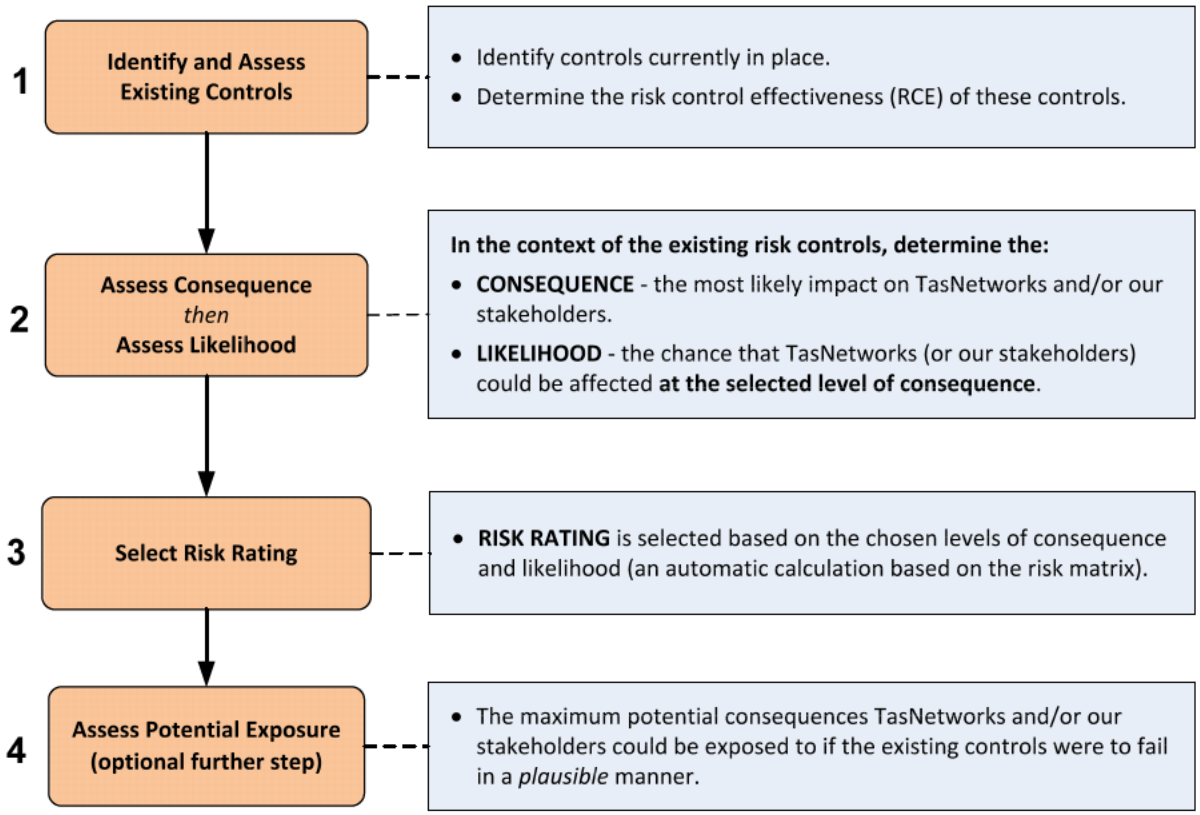
Risk analysis is always undertaken in the context of the existing controls and their effectiveness (commonly referred to as the residual risk).

3.2.2.1. Risk Analysis Steps

Risk analysis is undertaken as a sequential process:

1. Identification and assessment of the effectiveness of the existing controls.
2. Taking into account the effectiveness of these controls, determining the potential consequences that could result from the risk event, and the likelihood of these consequences occurring (to arrive at the level of risk).

The sequential risk analysis process is presented graphically below:



3.2.2.2. Risk Control Effectiveness

The first step in the risk analysis process is the identification and assessment of the existing risk controls.

TasNetworks defines a control as any measure that modifies a risk.

Risk control effectiveness (RCE) measures the strength of the existing controls, relative to the level that is *reasonably achievable* for a particular risk:

- Rating ranges from **FULLY EFFECTIVE** to **NONE** (refer to section 3.2.2.3).
- The assessment is relative to the level of control effectiveness TasNetworks could realistically achieve (it is not an assessment against a theoretical state of perfect control).
- Used as an indicator of whether TasNetworks is doing all that it could or should to manage a particular risk.
- Assessed based on the suite of controls related to a risk, not for each individual control.
- Assessment is undertaken before, and then included in, the assessment of consequences and their associated likelihoods.

Risk control effectiveness is assessed using a consistent rating scale for all risk controls across TasNetworks and has two components to the assessment:

CONTROL ADEQUACY	• How well are the controls designed with reference to the underlying risk causes? • Do the risk controls match the risk causes?
OPERATING EFFECTIVENESS	• Assessment of the operating effectiveness of the controls. • Are the controls operating as intended? (e.g. are the asset inspections actually performed within the defined timeframes?)

3.2.2.3. Risk Control Effectiveness Ratings

RATING	GUIDE
FULLY EFFECTIVE	**Nothing more to be done except review and monitor the existing controls:** • Controls are well designed for the risk, are largely preventative, address the root causes of the risk and management believes they are reliable and effective at all times. • Reactive controls only support preventative controls.
PARTIALLY EFFECTIVE	**Most controls are designed correctly and are in place and effective:** • Some more work can be done to improve the operating effectiveness; or • Management has doubts about their operational effectiveness and reliability.
INEFFECTIVE	**While the design of controls may be largely correct, in that they treat most of the root causes of the risk, they are not currently very effective:** • There may be an over-reliance on reactive controls. • Some of the controls do not seem correctly designed (they do not treat root causes). • Those that are correctly designed are operating effectively.
TOTALLY INEFFECTIVE	**Significant control gaps:** • The controls do not treat root causes or they do not operate at all effectively; or • Controls, if they exist, are only reactive (where preventative controls could be implemented).
NONE	**Virtually no credible control:** • Management has no confidence that any degree of control is being achieved, due to poor control design and/or very limited operational effectiveness.

3.2.2.7. Potential Exposure

In addition to the residual risk measure, the level of risk taking into account the strength of existing controls, TasNetworks also calculates the potential exposure for a risk.

The potential exposure measures the maximum potential consequences if the existing controls were to fail *in a plausible manner.*

The potential exposure measure achieves the same outcomes as the inherent risk measure, the identification of key controls, without the complexity and ambiguity in determining the level of inherent risk (the risk level assuming there are no controls).

Determining the potential exposure is generally the last step in the risk analysis process and assists in the identification of risks that have key controls.

Key controls indicate that a risk is being controlled to an acceptable level due to the strength of the controls. These key controls maintain an otherwise intolerable risk to a tolerable level, which for TasNetworks is generally determined by the risk appetite statement.

If these key controls were to deteriorate or fail, it is likely that the consequences TasNetworks and/or our stakeholders would be exposed to would be intolerable.

Risks that are identified with key controls become the focus of the control assurance processes (e.g. monitoring of controls by control owners, independent reviews and internal audit).

Following the calculation of the potential exposure, TasNetworks prioritises the implementation of control assurance mechanisms for risks with the following properties:

- Risk level is assessed as **LOW** or **MEDIUM**.
- Control strength is determined to be **FULLY EFFECTIVE** or **PARTIALLY EFFECTIVE**.
- Potential exposure is determined to be **SEVERE** or **MAJOR.**

These qualities indicate that the risk is currently being controlled to an acceptable level due to the strength of the existing controls – a strong indicator that key controls are present.

How TasNetworks Assesses Potential Exposure

Based on the risk controls identified and assessed, credible and plausible scenarios are considered in relation to if and how the risk controls could fail:

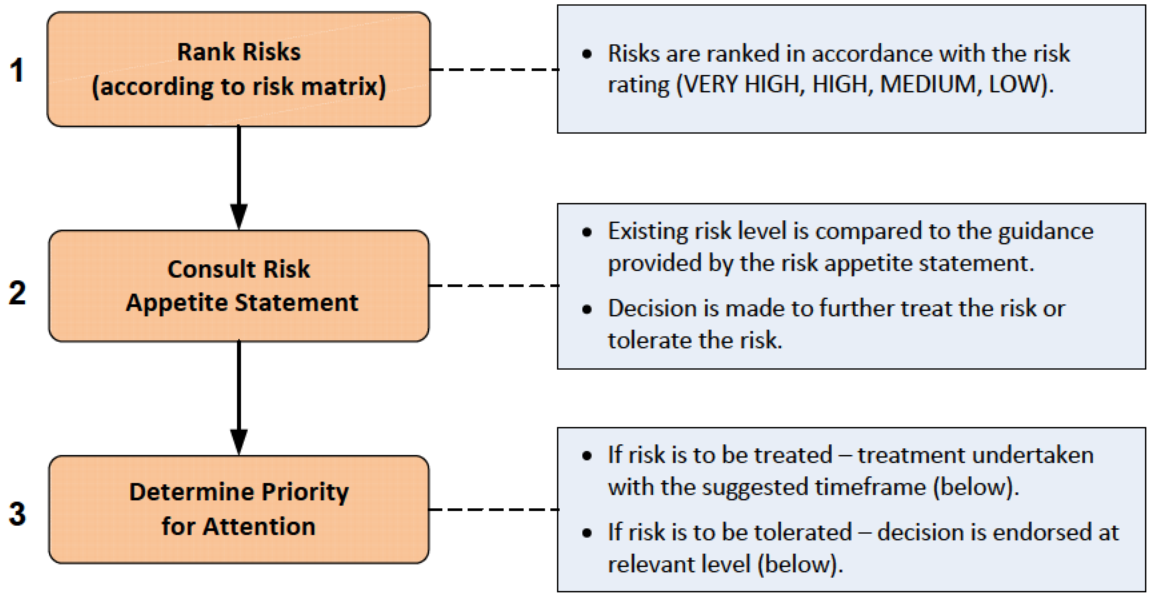
1. If the controls could fail in a realistic manner, the consequences TasNetworks and/or our stakeholders could subsequently be exposed to from the control failure are determined (from the TasNetworks consequence table).
2. The potential exposure rating is recorded with the other risk components (the risk control effectiveness, consequence, likelihood and risk level).

3.2.3. Evaluate Risks

Risk evaluation makes decisions based on the outcomes from the risk analysis phase about which risks require treatment and which risks can or will be tolerated.

For those risks that will be treated, the risk evaluation phase determines which risks will receive priority for treatment.

3.2.3.1. Risk Evaluation Steps



The primary consideration is whether the risk can be further treated in a way that is cost effective.

In general, the following factors are considered:

1. Whether the risk being controlled to a level that aligns with the TasNetworks risk appetite;
2. Whether it would be cost effective to further control risk; and
3. The willingness to continue tolerating risk(s) that exceed the TasNetworks risk appetite.

The level of risk alone does not necessarily indicate a need for further risk treatment:

- Risk treatment is not automatically undertaken because the current level of risk is on the higher end of the risk rating scale.
- Further risk treatment is only undertaken if the benefits from the risk treatment exceed the costs of the risk treatment – both financial or non-financial and tangible or intangible benefits are included.
- The exception to the cost benefit test is where legislative or regulatory requirements require adherence to certain standards for residual risk levels - for example as low as reasonably practicable (ALARP) required by the *Work Health and Safety Act*.

3.2.3.2. Applying the Risk Appetite Statement

In the evaluation of a risk, following the completion of the risk analysis, the TasNetworks risk appetite statement provides guidance in the risk treatment vs. risk toleration decision.

The purpose of the risk appetite statement is to:

- Assist in determining whether a risk can be tolerated at the current level, or if risk treatments should be implemented.
- Target risk treatment at those risks that exceed the stated risk appetite.
- Ensure risks are not tolerated outside the risk appetite where cost effective treatment can occur.
- Ensure risks that can continue to be tolerated are not subjected to further excessive risk treatment.

3.2.3.3. Continued Toleration of Risk

If a risk exceeds the desired level in the risk appetite statement, the business can continue to tolerate this risk provided there is an explicit decision to do so at the appropriate level of the organisation (refer to the authority for continued toleration below).

In the absence of any legislative, regulatory or internal policy requirements, continued risk toleration of this nature is generally undertaken on cost benefit grounds.

3.3. Treat Risks

Formulating and selecting risk treatment actions is a key component in delivering tangible results from the risk management process.

Risk treatment is undertaken to modify a risk, typically resulting in the enhancement of existing risk controls or the implementation of new risk controls.

If it is determined that a risk should be treated, it is usually not be desirable or cost effective to implement all possible risk treatments. It is necessary to choose, prioritise and implement the most appropriate combination of risk treatments.

Risk treatment options, or more usually the combination of options, are selected by considering:

- Target (post-treatment) risk levels.
- Costs and benefits of further risk treatment.
- External and/or internal criteria relevant to TasNetworks (for example treating the risk to the point where the costs are disproportionate to the benefits – the as low as reasonably practicable level).

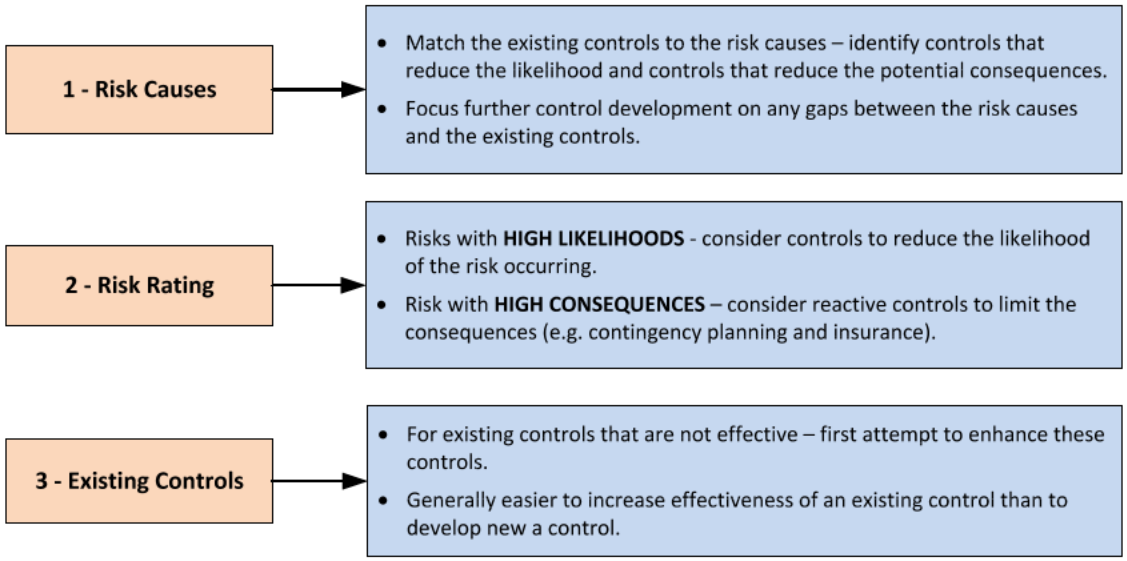
3.3.1. Developing a Treatment Strategy

Treatment of individual risks does not usually occur in isolation and is part of an overall treatment strategy:

- TasNetworks consults broadly about risk treatment with the relevant stakeholders, peers and specialists – for risk treatments are to be effective and sustainable they need to be acceptable to stakeholders and those responsible for implementing and maintaining the controls.
- An understanding of a complete treatment strategy is obtained to ensure that dependencies and linkages are not compromised, and the implementation of new risk treatments does not generate additional risks for the business.

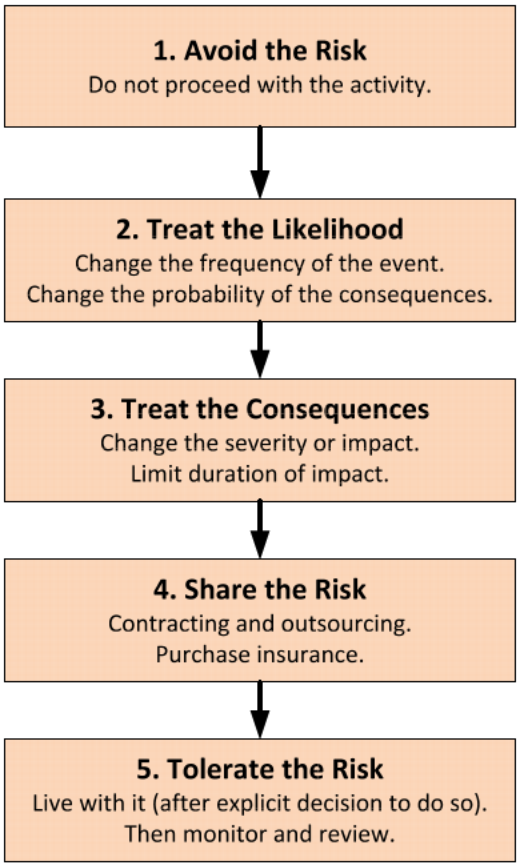
3.3.2. Developing Effective Risk Treatments

The development of effective risk treatments considers three pieces of information generated during the risk assessment process:



3.3.3. Risk Treatment Hierarchy

The general approach to risk treatment across TasNetworks is in accordance with the risk treatment hierarchy:



There are three general principles that support the risk treatment hierarchy:

1. Attempt to treat the likelihood first then the consequences.
2. Identify risk treatment synergies – can a number of risks be treated with one control? can an existing control be enhanced to treat a new risk? (rather than implementing a new control).
3. Careful consideration of rare (but severe) risks:
    - These risks may warrant treatment actions that are not justifiable on cost benefit grounds alone.
    - Reputational, legal, community and shareholder requirements may override cost benefit analysis.

The generic risk treatment hierarchy is applied in the absence of any existing guidelines for risk treatment – for example the existing hierarchy of control contained in the TasNetworks *HSEQ Risk Management Procedures*.

4. Risk Management Process – Supporting Guidance/Templates

COMPONENT	DOCUMENT	PURPOSE	TASNETWORKS ZONE LINK
Communicate and Consult	Guidance – communication and consultation	• Guidance on how to communicate and consult on risk with internal and external stakeholders.	<insert Zone link>
Establish the Context	Template – context establishment	• Template to assist in the context establishment process (prior to a risk identification process commencing).	<insert Zone link>
Identify Risks	Template – risk register	• Simple and advanced risk register templates to capture the outputs from the risk management process.	<insert Zone link>
	Risk assessment techniques (ISO 31010)	• The 'toolkit' of risk assessment techniques that can be employed. • Selected based on the importance/complexity of the subject of the risk assessment.	<insert Zone link>
Analyse Risks	Guidance - bow-tie analysis Template - bow-tie analysis	• Guidance and template for undertaking bow-tie analysis. • Tool for assessing the effectiveness of risk controls.	<insert Zone link>
	Guidance – root-cause analysis Template – root-cause analysis	• Guidance and template for undertaking basic root-cause analysis • To determine the underlying causes for a business failure.	<insert Zone link>
	Guidance – determining potential exposure	• Guidance for determining the potential exposure from a risk.	<insert Zone link>
Evaluate Risks	Guidance - risk appetite statement	• Guidance for applying the Board-approved risk appetite statement.	<insert Zone link>
Treat Risks	Guidance - control design and control improvement	• Guidance on how to design and improve risk controls.	<insert Zone link>
	Template - risk treatment plan	• Template for developing/documenting a risk treatment plan.	
Monitor and Review	Guidance - risk-based assurance planning	• Guidance for linking the assurance process to the risk management process (to ensure assurance activities are risk-based and focussed on the key controls).	<insert Zone link>