

Application of Risk Management

RSK-WI-001

Applicability

ARTC Network Wide	SMS
-------------------	-----

Publication Requirement

Internal / External

Primary Source

RMWI1 Risk Assessment Process V1.0
RMWI2 Conduct Risk Assessment Workshop V1.1

Document Status

Version #	Date Reviewed	Prepared by	Reviewed by	Endorsed	Approved
1.3	23 November 2018	Corporate Risk Manager	GM Risk, Safety & Environment	GM Risk, Safety & Environment	Group Executive Corporate Services & Safety

Amendment Record

Amendment Version #	Date Reviewed	Clause	Description of Amendment
1.0	26 May 2016	All	Rebranded and assigned new document number. Document references updated and new documents included. Amendments to incorporate Risk Management Information System. Roles and responsibilities updated. Inclusion of contemporary flowcharts. Reordering and rewording for improved document flow and readability. Removal of duplicated information. Inclusion of Project Risk Management requirements, tiered risk structure, inherent risk and risk ownership. Amendments to endorsement & approval process.
1.1	19 December 2017	Various	Removal of RMIS and HP Trim references and inclusion of Central Risk Register. Consistent use of terminology for treatment. Update to reflect current project management practices.

© Australian Rail Track Corporation Limited (ARTC)

Disclaimer

This document has been prepared by ARTC for internal use and may not be relied on by any other party without ARTC's prior written consent. Use of this document shall be subject to the terms of the relevant contract with ARTC.

ARTC and its employees shall have no liability to unauthorised users of the information for any loss, damage, cost or expense incurred or arising by reason of an unauthorised user using or relying upon the information in this document, whether caused by error, negligence, omission or misrepresentation in this document.

This document is uncontrolled when printed.

Authorised users of this document should visit ARTC's intranet or extranet (www.artc.com.au) to access the latest version of this document.

1.2	19 February 2018	Various	Change of title for Executive roles. Change Division/ Business Unit.
1.3	23 November 2018	Various	Incorporation of references to ARTC's new Enterprise Risk Management System, and terminology and process changes arising from the system implementation including transitional arrangements. Renaming of document. Consolidation of RSK-WI-002, RSK-WI-003 and RSK-WI-004 into this document.

Table of Contents

Table of Contents3

1 INTRODUCTION5

1.1 Purpose5

1.2 Scope5

1.3 Document Owner5

1.4 Responsibilities5

1.5 Parent Procedure7

1.6 Subordinate Documents.....7

1.7 Reference Documents7

1.8 Definitions.....8

2 OVERVIEW & GENERAL PRINCIPLES12

2.1 Risk Management Process12

 2.1.1 Default methodology – Bow Tie Analysis..... 13

2.2 Communication & Consultation.....14

2.3 Risk Registers14

2.4 Determining and Allocating Risk Ownership.....14

3 IDENTIFYING RISK15

3.1 Components of risk15

3.2 Risk Identification15

 3.2.1 Determining Areas of Focus..... 15

 3.2.2 Methods of Risk Identification..... 16

3.3 Causes and Contributory Factors16

3.4 Identification of Consequences.....16

3.5 Identification of Controls.....16

 3.5.1 Hierarchy of Controls..... 17

3.6 Determining Control Effectiveness.....17

 3.6.1 Determining Adequacy of the Control..... 18

 3.6.2 Considering Human Fallibility 18

 3.6.3 Control Effectiveness Criteria 18

4 ANALYSING RISK.....19

4.1 Determining risk level.....19

4.2 Analysing risk23

5	EVALUATING RISK.....	23
5.1	ARTC Risk Management and SFAIRP	24
5.2	Evaluation and control for Non-SFAIRP risk assessment	24
6	TREATING RISK.....	25
6.1	Proposed Treatments.....	25
6.1.1	<i>Suitability of Proposed Treatments</i>	26
6.1.2	<i>Implications of Proposed Treatments</i>	26
6.2	Rejecting a Proposed Treatment	27
6.3	Determining Target Risk Level.....	27
6.3.1	<i>Setting the Target Date for Risk Reduction</i>	27
7	REMOVING A CONTROL (REVERSE SFAIRP)	28
8	MONITORING AND REVIEWING RISK.....	29
8.1	Preparing for the Review.....	29
8.2	Conducting the Review	30
8.3	Unscheduled Risk Review	31
8.4	Reviewing a Control	31
8.4.1	<i>Monitoring and Validating Controls</i>	32
8.5	Determining Next Review.....	32
9	CONDUCTING WORKSHOPS	33
9.1	Allocate Responsibility	33
9.2	Identify Key Stakeholders	33
9.3	Organise Risk Workshop	34
9.4	Establish the Objectives, Context and Scope	34
9.4.1	<i>Establish the Context</i>	35
9.4.2	<i>Determine the Scope</i>	36
9.4.3	<i>Additional Information</i>	36
9.5	Distribute Pre-Workshop Reading.....	36
9.6	Conduct Risk Workshop.....	37
	APPENDIX 1 – RISK IDENTIFICATION METHODS.....	38
	<i>General Methods of Risk Identification & Assessment</i>	38
	<i>Additional Specific Methods of Risk Identification & Assessment</i>	39

1 INTRODUCTION

1.1 Purpose

This work instruction provides general guidelines for the practical application of risk management.

1.2 Scope

This work instruction is applicable to all ARTC workers and contractors undertaking risk management activities.

This work instruction is consistent with *ISO 31000:2018 Risk Management – Guidelines*.

1.3 Document Owner

The ARTC Corporate Risk Manager is the coordinator of this work instruction and is the initial point of contact for all inquiries relating to its application across the organisation.

1.4 Responsibilities

Group Executive Corporate Services & Safety is responsible for:

- The development, review and analysis of policies and practices to identify, assess and manage risk in accordance with the ARTC Risk Appetite Statement, and to ensure compliance with So Far As Is Reasonably Practicable (SFAIRP) principles.

ARTC Executive are responsible for:

- Ensuring appropriate resources are available to conduct risk assessments relevant to their area of responsibility;
- Ensuring appropriate assessments of risk are conducted for notifiable changes to ARTC infrastructure or the Safety Management System.

ARTC Corporate Risk Manager is responsible for:

- Providing advice and reasonable assistance to Executive and Senior Managers, Risk Owners, Risk Managers, Workshop Facilitators, other workers and relevant external stakeholders on their risk management obligations;
- Providing training, mentoring and advice to workshop facilitators on the facilitation of risk assessment and risk review workshops and utilisation of tools referenced in this work instruction;
- Implementing mechanisms to ensure risks are being managed in accordance with the risk management framework.
- Documenting and communicating this work instruction to all relevant internal and external stakeholders; and
- Managing information within the ARTC Enterprise Control Library, ARTC Enterprise Cause Library and ARTC Enterprise Consequence Library.

Risk Owners are responsible for:

- Ensuring that risks within their area of responsibility are identified, assessed and managed utilising ARTC's Enterprise Risk Management System (ERMS);
- Ensuring that they have appropriate oversight for the risks that they own, and that those risks are being managed in accordance with the ARTC Risk Appetite Statement;
- If appropriate, assigning a suitable Risk Manager to manage further detailed activity for the risks that they own;
- Ensuring appropriate controls are in place to manage safety risks, in accordance with SFAIRP principles;
- Providing information regarding any identified deficiencies of controls to Control Owners.
- Providing the Corporate Risk Manager with updates for controls within the ARTC Enterprise Control Library, as appropriate;
- Ensuring that appropriate Proposed Treatments are in place and being actioned for the risks that they own;
- Ensuring that periodic reviews of the risks that they own are conducted, including the effectiveness of their existing controls;
- Reporting information on risks in accordance with escalation requirements and governance arrangements.

Risk Managers are responsible for:

- Ensuring that the risks that they manage, including their Controls and Proposed Treatments, are entered into an appropriate risk register within ARTC's Enterprise Risk Management System and appropriately documented and updated;
- Ensuring that periodic reviews of the risks that they manage are conducted, including the effectiveness of their existing Controls, and appropriate records of review and updates made within the Enterprise Risk Management System; and
- Ensuring that appropriate Proposed Treatments are identified and being actioned for the risks that they manage.

Control Owners are responsible for:

- Taking remedial action to address identified deficiencies of controls, as agreed with Risk Owners and/or Risk Managers.

Workshop Convenors are responsible for:

- Providing oversight and guidance for risk workshops;
- Assigning a suitable Facilitator for workshops;
- Ensuring that appropriate resources are available to conduct workshops;
- Ensuring that outcomes of risk workshops are documented in ARTC's Enterprise Risk Management System in a manner that is consistent with the requirements of RSK-PR-001 Risk Management, this work instruction, and other related risk management documents.

Note: The Workshop Convenor may, or may not be, a Risk Owner

Workshop Facilitators are responsible for:

- Preparation activities for a risk workshop, including identification of key stakeholders, preparation and collation of pre-workshop reading material, organising required facilities and distributing pre-workshop reading material;
- Documenting the Objectives, Background and Context and Scope of the risk workshop in the Enterprise Risk Management System in accordance with this work instruction and other related risk management documents;
- Facilitating the collection of risk and control information at the risk workshop, in accordance with RSK-PR-001 Risk Management, this work instruction, and other related risk management documents;
- Ensuring appropriate consultation and documenting finalised risk and control information in the appropriate register within ARTC's Enterprise Risk Management System;
- Initiating the approval process for new and/or updated risk entries.

Note: The Workshop Facilitator may, or may not be, a Risk Manager

Managers and Supervisors are responsible for:

- Identifying where risk assessment or review activity may be required to be undertaken, and providing relevant information and input in risk assessment and review activity, where requested; and
- Reviewing and updating the progress of Actions and Proposed Treatments for which they are responsible in ARTC's Enterprise Risk Management System.

Workers are responsible for:

- Identifying and communicating local worksite hazards and their controls to all personnel at that particular worksite, and reporting risks to their supervisor; and
- Providing relevant information and input in risk assessments, where requested.

1.5 Parent Procedure

RSK-PR-001 Risk Management is the Parent Procedure for this work instruction.

1.6 Subordinate Documents

There are no documents subordinate to this work instruction.

1.7 Reference Documents

The following documents are related to this guideline:

- COR-PO-006 Risk Management Policy
- RSK-WI-005 Project Risk Management
- RSK-GL-001 Risk Management Terms and Data Guideline
- RSK-GL-003 Risk Management Overview
- RSK-GL-005 Project Risk Management Overview

The following documents were referenced in this procedure:

- ISO 31000:2018 Risk Management – guidelines
- Rail Safety legislation (various)
- Commonwealth Work Health and Safety legislation
- Environment legislation (various)

1.8 Definitions

The following terms and acronyms are used within this document:

Term or acronym	Description
Causal & Contributing Factor	<p>A condition or set of conditions leading to a risk. It is often used to describe “what could go wrong”. Used in this document to describe the cause contributing to a risk.</p> <p>A causal factor is a factor which may alone cause the risk to eventuate. A contributing factor, is a factor which, when combined with other factors could cause the risk to eventuate.</p>
CGR Foundation	<p>The name of the proprietary governance, risk and assurance software developed by Corporate Governance Risk Pty Ltd and utilised by ARTC as its Enterprise Risk Management System. Its use to document and manage risks is mandated.</p>
Consequence	<p>Outcome of an event affecting objectives.</p> <p>An event can lead to a range of consequences. A consequence can be certain or uncertain and can have positive or negative effects on objectives. Consequences can be expressed qualitatively or quantitatively.</p> <p>A consequence may also be referred to as an impact.</p>
Context	<p>The set of circumstances or facts that surround a particular event or situation, and/or, a clearly defined set of parameters that enable focussed risk assessment.</p>
Contractor	<p>An entity performing work under contract to ARTC. For the purpose of this work instruction, contractor includes entities performing work under sub-contractor arrangements.</p>
Control	<p>A measure that modifies risk by either preventing the risk or mitigating the consequences of the risk. Controls may include any process, policy, device, practice or other action which modifies risk.</p>
Control Owner	<p>The person with the responsibility, authority and accountability to manage a control of a specific risk/s.</p>
Control Effectiveness	<p>A term that addresses the question of whether the controls are adequate and operating as intended.</p>
Control Effectiveness Criteria	<p>Specific criteria that describes the attributes for each of the levels of Control Effectiveness.</p>
Critical Control	<p>Means that if the control was absent or failed, the risk would eventuate.</p>
Current Control	<p>A control that is currently in place that prevents or mitigates a risk.</p>
Current Risk Level	<p>The risk level, given the effectiveness of controls currently in place. Also known as residual risk level.</p>

Term or acronym	Description
Enterprise Risk Management System (ERMS)	A system that is utilised to record and manage risks, controls, treatments and actions across the whole of the organisation, including projects. CGR Foundation is ARTC's mandated Enterprise Risk Management System.
Hazard	A source of potential harm e.g. in terms of human injury, damage to property or other loss. A hazard can be a risk source.
Hierarchy of Controls	<p>A sequence of options which offer you a number of ways to approach the control of hazards. The hierarchy is arranged in order of implementation preference.</p> <ul style="list-style-type: none"> • Elimination • Substitution • Isolation • Engineering controls • Administrative controls • Personal Protective Equipment (PPE)
Human Factors	<p>A discipline concerned with the interactions between humans and other elements of a system, where theory, principles, data, and methods to design are applied to optimise human well-being and system performance.</p> <p>Also known as ergonomics</p>
Inherent Risk Level	The risk level without any controls in place, also known as "untreated risk".
Level of Risk	Magnitude of a risk or combination of risks, expressed in terms of the combination of consequences and their likelihood.
Likelihood	A qualitative description of the chance of something happening.
Objectives	Organisational and/or project deliverables.
Proposed Treatment	A control that is not yet implemented.
Qualitative Assessment	Method of risk analysis used to describe the level of risk considering scaled consequences and likelihood, utilising the ARTC Risk Matrix.
Quantitative Assessment	Method of risk analysis used to numerically assess the nature, sources, and impact of a risk, and assess and quantify the overall impact of uncertainties.
Review	Activity undertaken to determine the suitability, adequacy and effectiveness of the subject matter to achieve established objectives. Review can be applied to a risk management framework, risk management process, risk or control.
Risk	Effect of uncertainty on objectives. An effect is a deviation from the expected. Objectives can have different aspects (such as financial, rail safety, WHS and operation goals) and can apply at different levels (such as strategic, organizational, project and process).
Risk Appetite	<p>The amount of risk an entity is willing to accept or retain in order to achieve its objectives.</p> <p>The appetite for risk and opportunity can vary between, and within, risk impact categories depending on the type of risk and the potential for adverse events and positive rewards.</p>
Risk Appetite Statement	A formal statement that describes ARTC's attitude towards risk taking.
Risk Assessment	The process of identifying, analysing and evaluating risk.

Term or acronym	Description
Risk Identification	<p>Process of finding, recognizing and describing risks.</p> <p>Risk identification involves the identification of risk sources, events, their causes and their potential consequences. Risk identification can involve historical data, theoretical analysis, informed and expert opinions, and stakeholder's needs.</p>
Risk Impact Categories	<p>ARTC's six identified organisational areas of risk focus; SAFERR. In the context of project risk, ARTC recognises a seventh area of risk focus – Schedule.</p>
Risk Management Process	<p>The systematic application of management policies, procedures & practices to the tasks of:</p> <ul style="list-style-type: none"> • Establishing the context of the risk • Identifying the risk • Analysing the risk • Evaluating the risk • Controlling the risk • Monitoring and reviewing the risk • Communicating the risk
Risk Manager	<p>The person appointed by a Risk Owner to conduct the detailed activity on a risk on their behalf. Nomination of a Risk Manager is not mandatory, and is only undertaken in circumstances where the Risk Owner is not undertaking detailed activity themselves.</p>
Risk Owner	<p>Person with the responsibility, authority and accountability to manage a risk.</p>
Risk Register	<p>A collation of risk information that provides a record of identified risks relating to the objectives of the organisation, business unit or project. They provide assurance on the range of control measures and plans in place to address identified risks.</p>
Risk Tolerance	<p>The specific level of risk taking that is acceptable in order to achieve a specific objective or manage a category of risk.</p>
Safety Impact	<p>An impact to workers and/or the public incorporating impacts to:</p> <ul style="list-style-type: none"> • Physical safety (e.g., from hazards such as machinery and plant); • Health and wellbeing; • Psychological health; • System and process safety (e.g. assets); or • Operational safety (e.g. railway operations).
SFAIRP	<p>So Far As Is Reasonably Practicable – The likelihood and consequences of a risk must be weighed against the availability, effectiveness and cost of measures to eliminate or reduce the risk.</p>
Stakeholder	<p>Person or organisation that can affect, be affected by, or perceive themselves to be affected by a decision or activity. A decision maker can be a stakeholder.</p>
Target Risk Level	<p>The risk that is expected to remain after implementation of Proposed Treatments.</p>
Workshop Convenor	<p>The person with the responsibility, authority and accountability for ensuring that a risk assessment workshop is conducted appropriately</p>

Term or acronym	Description
Workshop Facilitator	<p>A person with sufficient training and/or experience to conduct a risk workshop. Sufficient training and/or experience includes:</p> <ul style="list-style-type: none"> • The ARTC Risk Workshop Facilitator training course; and/or • External training course based on AS/NZS ISO 31000; and/or formal recognised qualifications that include risk management; and/or • Experience in the facilitation of previous risk assessments using Bow Tie methodology or quantitative risk analysis – whichever is relevant.

2 OVERVIEW & GENERAL PRINCIPLES

2.1 Risk Management Process

Risks may be identified that are either new (or previously unidentified) risks, or changes or implications to current risks may be identified. Where impacts or variations to existing risks have been identified, these are to be communicated to the relevant Risk Owner and Risk Manager for review and update of the relevant risk entry (refer Figure 1).

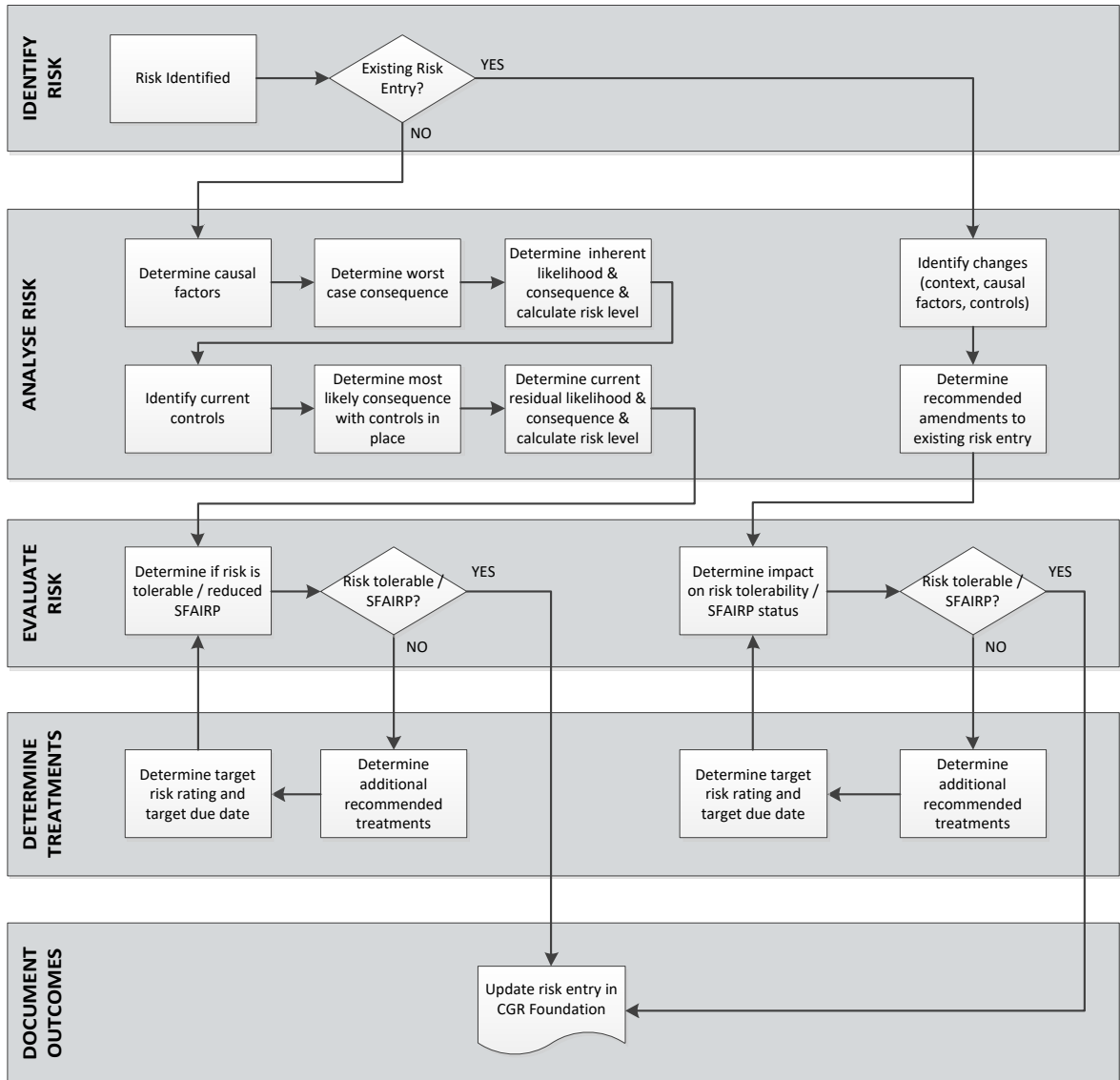


Figure 1: Risk Identification, Analysis and Evaluation Overview

2.1.1 Default methodology – Bow Tie Analysis

Bow Tie Analysis is a method of pictorially depicting a risk and its causes, consequences and controls, and that provides an effective method of determining and demonstrating that identified causal and contributory factors have associated controls in place. Bow Tie Analysis is the default methodology to be utilised for qualitative risk assessment.

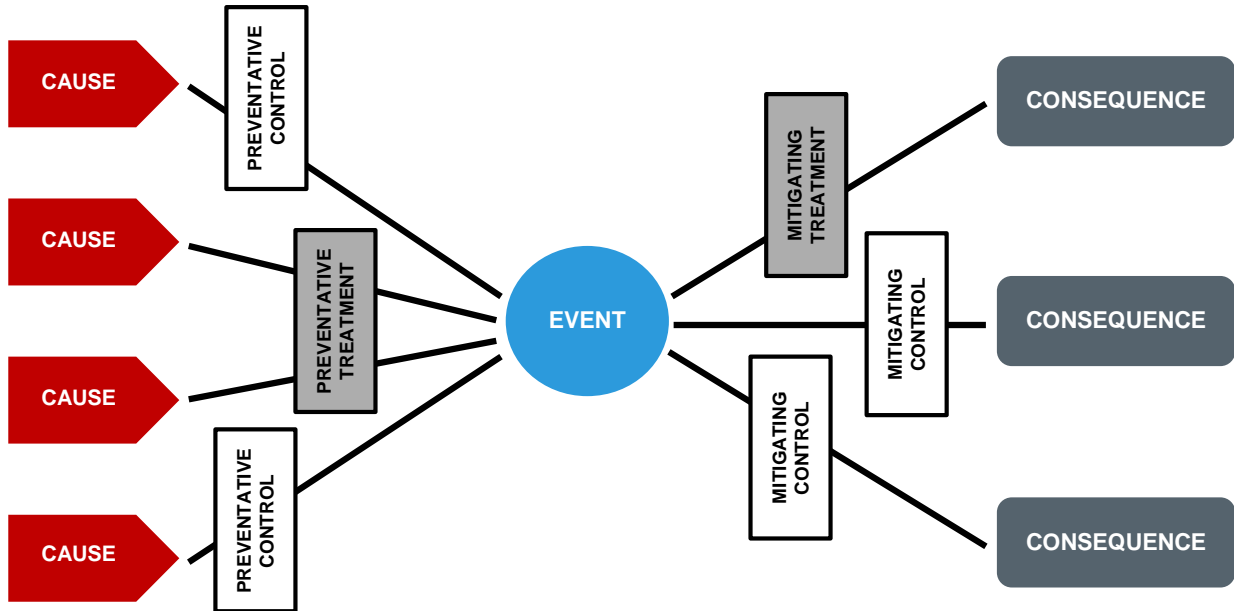


Figure 2: Bow Tie Diagram

Bow tie analysis is undertaken in a sequenced process:

1. Demonstrate the problem (risk event) clearly
2. Identify the causal and contributory factors
3. Identify the consequences
4. Determine the inherent risk level (the risk level without controls)
5. Identify the controls to prevent the risk and determine their effectiveness
6. Identify the mitigating controls that reduce impacts should the risk event occur and determine their effectiveness
7. Determine the most likely consequence given the controls in place
8. Determine the current risk level (the risk level with current controls)
9. Identify additional treatments (preventative and mitigating)
10. Determine the target risk level (the risk level with current controls and proposed treatments)

Note: An Enterprise Risk Management System (ERMS) is being progressively implemented across ARTC. Project risks not yet transferred into the system will continue to be managed via stand-alone project risk registers until the project has been transitioned into the system, where transition is deemed appropriate, or until the project end. Decisions will be made on a case by case basis as to whether project registers will be transitioned into the system.

Where risk analysis has not been previously undertaken in a bow tie format, these entries will be converted into bow tie format post transfer.

2.2 Communication & Consultation

Effective internal and external communication and consultation is essential to ensure that those accountable for implementing the risk management process and stakeholders understand the basis on which decisions are made, and the reasons why particular actions are required.

Communication and consultation occurs at all stages of the risk management process and can be undertaken both formally and informally. It can include:

- Liaison with workers or other stakeholders on current and emerging risks and potential new or improved controls
- Formal input on risk and control assessment from subject matter experts and other stakeholders
- Communication and coordination with other internal or external parties on shared risks and actions to prevent or mitigate risks

2.3 Risk Registers

Risk registers are created in ARTC's Enterprise Risk Management System to capture risks for all Risk Tiers, including programme and project risks.

Approved risk matrices are programmed for each Risk Register within the system to allow selection of customised consequence criteria specific to each register. For example each project will have different financial and schedule consequence criteria.

Risks may move from one register to another. Examples of where this may occur are:

- Where a project finishes and residual risks remain
- Following organisational restructure
- Following changes in responsibility for activities and/or assets

Where a risk is moved between registers and a different risk matrix is programmed, the risk is to be reassessed using the applicable risk matrix.

Where there are new ongoing residual risks that have arisen from a project, the risk type within the system is to be changed from project to non-project and the risk tier reallocated.

2.4 Determining and Allocating Risk Ownership

Risk ownership is determined by the scope of the risk, the applicable risk tier, and responsibility and accountability for the infrastructure, task, process, plant or project for which the risk is associated. A risk owner would be expected to have:

- Responsibility and accountability for the infrastructure, task, process, plant/equipment or project for which the risk is associated; and
- Have authority to be able to initiate treatment(s) (either directly authorise or be able to seek authorisation/ budget from a higher level) that they will be ultimately responsible for; or
- Ability to influence, or seek to influence, the initiation of treatment(s) that need to be implemented by other areas for which they are not directly responsible.

Where it has been determined that the proposed Risk Owner does not have the appropriate attributes, as stated above, risk ownership is to be assigned to another appropriate person. This may be the direct line manager, or another appropriate person.

3 IDENTIFYING RISK

Risk is the chance of something happening or circumstances arising or changing that will have an impact upon objectives, measured in terms of likelihood and consequence. It encompasses both positive and negative impacts.

3.1 Components of risk

A risk generally includes a source (e.g. hazard), cause, risk event, and consequence.

Risks are often incorrectly expressed as consequences only, yet this is not the best way to define a risk. Consequences are the effects or impacts of a risk or combination of risks that result after a risk event occurs. Examples of a risk include:

- Operator fails to notice a warning signal (cause)... that leads to...
- Train SPADs (source)... that leads to...
- Low speed collision of rolling stock (risk event) ... that results in...
- Rolling stock damage and/or personal injury (consequence).

For clarification, the following shows poor examples of descriptions of a risk, with an explanation of why.

- Someone falling off a bridge — does not state the cause and the consequence;
- SPAD — does not describe the cause, risk event and consequence; and
- Train collision — does not state the source, cause and consequence.

Fields in the Enterprise Risk Management System allow for the risk to be described in a succinct manner (referred to as Risk Name), as well as a more comprehensive description of the risk (referred to as Risk Description).

3.2 Risk Identification

3.2.1 Determining Areas of Focus

It can sometimes be challenging to determine where to prioritise risk identification and assessment. A criticality assessment can assist in identifying prioritised areas for focus, by asking the question:

“What critical assets (tangible and intangible) am I dependent upon to deliver my project/operational activity?”

It may be useful to think across the following categories:

- people
- physical assets
- IT and systems, and
- external parties, such as suppliers.

3.2.2 Methods of Risk Identification

The aim of risk identification is to generate a comprehensive list of hazards, circumstances, consequences and risk events that might have an impact on the achievement of each of the activity/proposal/project objectives.

Methods used to identify risk issues include checklists, brainstorming, experience and historical records, stakeholder consultation, flow charts, systems and scenario analysis and systems engineering techniques.

Risk identification can also be embedded within normal day to day practices, for example, inclusion of identification of emerging issues and changing internal and external environments as part of team meetings.

The approach taken will depend on the type of activities and risks that are being identified.

Examples of risk identification methods are attached in Appendix 1.

3.3 Causes and Contributory Factors

Causes & Contributory Factors are the factors which alone (“causal” factor), or combined (“contributory” factor), could lead to the risk eventuating.

As part of the risk assessment process, these causal and contributory factors must be determined in order to consider appropriate controls to prevent the risk.

Methods that may assist in determining causal factors include:

- Review of outcomes of internal investigations
- Review of outcomes from other operator investigations
- Analysis techniques such as “5 Why”.

A library of common causes and contributory factors is held within the Enterprise Risk Management System.

3.4 Identification of Consequences

Consequences, also known as impacts, are what may occur as a result of the risk event occurring. Identification of potential consequences is essential in order to determine appropriate controls to reduce (mitigate) negative impacts should the risk event occur. Methods that may assist in determining potential consequences include:

- Review of outcomes of internal investigations
- Review of outcomes from other operator investigations
- Brainstorming of “worst case” events

A library of common consequences is held within the Enterprise Risk Management System.

3.5 Identification of Controls

A list of all ARTC controls is available within the Enterprise Risk Management System. This collective list is known as the ARTC Control Library and is regularly updated as new controls are identified or implemented. Knowledge of ARTC’s Control Library is critical at this stage and getting the right mix of stakeholders to participate when assessing risks will greatly assist.

Detailed Control information should be recorded for all Operational, Geographic/Location and Project risks. Detailed Control information is optional for Strategic and Enterprise Wide risks if subsidiary related risks contain detailed control information. RSK-GL-001 Risk Management Terms and Data Guideline gives further instruction on the naming and describing of Controls.

3.5.1 Hierarchy of Controls

The Hierarchy of Controls is a tool that facilitates selection of the most appropriate means for reducing or eliminating the risk.

The principle behind the Hierarchy of Controls is that risk controls dependent on individual behaviour are less reliable and durable than risk controls that engineer or design out risks.

The Hierarchy of Controls (from most effective and desirable through to least effective and desirable) is as follows:

Elimination: Removing or otherwise eliminating the risk.

Substitution: Substituting the hazard that gives rise to the risk with a hazard that gives rise to a lesser risk.

Isolation: Isolating the hazard from the person(s) put at risk.

Design/engineering: Minimising the risk through engineering means.

Administrative: Minimising the risk through administrative means (for example, by providing appropriate training, or adopting safe work practices)

Personal Protective Equipment (PPE): Providing some type of personal barrier between the risk source and an individual (for example, protective eyewear, hi-visibility clothing, hearing protection etc.).

Usually a combination of measures will be the most effective approach. For example, PPE may be required in combination with other measures, such as engineering controls. Judgements must be made about the suitability and effectiveness of existing and proposed controls for reducing the risk. All possible control options should be considered, and selection made of the combination that will produce the most effective and reasonable level of risk reduction or elimination.

3.6 Determining Control Effectiveness

It is essential to determine the effectiveness of controls in order to:

- Determine whether the control (or combination of controls) adequately reduces the risk level
- Identify whether additional control(s) are required
- Determine whether remedial action is needed to increase effectiveness
- Determine if any mechanisms for monitoring need to be put in place.

There are two key factors to consider when determining the effectiveness of the control:

1. Whether the control is adequate
2. How susceptible the control is to human error or non-compliance

3.6.1 Determining Adequacy of the Control

Adequacy of the control relates to whether the control is appropriate for the related causal or contributory factor(s) that it is intended to address, and how effective it is in meeting the intended objective in addressing the risk. Questions that may be appropriate to consider include:

- Is the control appropriate for the causal or contributory factors?
- Does the control operate as intended?
- Are there any circumstances or scenarios where the control may be deficient?
- Is the control implemented in all applicable areas?
- Are there other controls that this control is reliant on, or interacts with in combination? If so, are they in place and considered adequate?
- Are there any known issues?

3.6.2 Considering Human Fallibility

Controls that are dependent on human actions or behaviours can be susceptible to unintended errors or deliberate non-compliance. Where this occurs, the control cannot be considered to be fully effective. Questions that may be appropriate to consider when considering if the control is susceptible to human fallibility include:

- Can errors be made? For example:
 - Omission of the control completely, or omission of a step in a process
 - Undertaking steps in a process in the wrong order
 - Incorrect / substandard technique
- If error(s) can occur, will the error be able to be identified and rectified before any adverse outcome occurs?
- Can the control be deliberately bypassed or ignored?

3.6.3 Control Effectiveness Criteria

There are five levels of control effectiveness. Specific Criteria for each of the levels of Control Effectiveness are described in Table 1.

LEVEL OF EFFECTIVENESS	EFFECTIVENESS CRITERIA
<p>5. Fully effective</p>	<ul style="list-style-type: none"> • The control is not susceptible to human error; • No further improvements are considered required for this control; • The control is considered to be appropriate in addressing the related causal / contributory factors; • Appropriate barriers are in place, tested, and not able to be bypassed; • Control verified in use in all applicable areas with no (current) Non-Conformances or issues identified. <p><i>NOTE: (Administrative controls and Personal Protective Equipment cannot be considered fully effective due to the possibility of human error or non-compliance)</i></p>
<p>4. Substantially effective</p>	<ul style="list-style-type: none"> • Control could potentially be impacted by human error, however error would usually be able to be detected and situation recovered; • No further improvements are considered required for this control; • The control is considered to be appropriate in addressing the related causal / contributory factors; • Appropriate barriers are in place, however could potentially be removed or overridden; • Control verified in use in all applicable areas with no (current) Non-Conformances or issues identified.
<p>3. Partially effective</p>	<ul style="list-style-type: none"> • Control is susceptible to human error, which may or may not be able to be detected and situation recovered; • The control partially addresses the related causal / contributory factors; • Barriers are in place, however may not be effective in all situations; • Anecdotal evidence that control is in use in all applicable areas <p>OR</p> <p>Control verified in use in all applicable areas with low risk Non-Conformance(s) or issues identified;</p> <p>OR</p> <p>Control implemented in some areas with no (current) Non-Conformances or issues identified.</p>
<p>2. Minimally effective</p>	<ul style="list-style-type: none"> • Control is vulnerable to significant or undetectable human error; • The control is not currently implemented in a manner that satisfactorily addresses the related causal / contributory factors; • Regulatory intervention is in place that is directly related to the control; • Current medium or high risk Non-Conformance(s) or issues have been identified that are directly related to the control.
<p>1. Not yet assessed</p>	<ul style="list-style-type: none"> • Level of implementation and effectiveness has not yet been assessed or verified.

Table 1: Control Effectiveness Criteria

4 ANALYSING RISK

4.1 Determining risk level

All identified risks are assessed in terms of likelihood and consequence criteria in order to determine the associated risk level. Relevant stakeholders must be consulted to achieve an agreed level of likelihood and consequence for identified risks. There are three calculations of risk level that can be determined:

Inherent Risk Level – the risk level when the risk is considered without any controls in place

Current Risk Level – the risk level when the risk is considered given the effectiveness of controls that are currently in place

Target Risk Level – the risk level that is expected to be applicable once additional Proposed Treatments have been implemented.

The assessed levels of likelihood and consequence are analysed and ranked using the ARTC Risk Matrix or the ARTC Project Risk Matrix (for project related risks only) to determine the overall level of risk for the activity, situation or circumstance. The risk may be described as Very High, High, Medium or Low.

ARTC Non-Project Risks Criterion

		Consequence					
Safety		Injury or illness with no impairment (may or may not require treatment)	Injury or illness with short-term impairment	Injury or illness with moderate but recoverable impairment	Injury or illness with long term to permanent impairment	One or more fatalities	
Assets: Network Performance		Immaterial disruption to non-critical track section	Material disruption to non-critical track section or Immaterial disruption to critical track section	Material disruption to a critical track section recoverable in the short-term	Material disruption to critical track section not recoverable in the short term	Material disruption to critical track section not recoverable in the short term with significant long term impacts on customers	
Assets: Organisational Capability		Manageable impact to internal operations, which may or may not require internal reallocation of existing resources	Missing short-term targets which may or may not require use of additional resources	Reduced ability to achieve business goals with some business impact	Material failure to achieve business goal(s) with significant business impact	Failure to achieve business goals with lasting impacts	
Financial		Enterprise	Less than \$2M operating profit loss of enduring impact; or One off impact of less than \$10M; or Less than \$50M impact to balance sheet	\$2M to \$10M operating profit loss of enduring impact; or One off impact of \$10M to \$50M; or \$50 to \$250M impact to balance sheet	\$10M to \$50M operating profit loss of enduring impact; or One off impact of \$50M to \$250M; or \$250M to \$500M impact to balance sheet	\$50M to \$150M operating profit loss of enduring impact; or One off impact of \$250M to \$750M; or \$500M to \$1B impact to balance sheet	More than \$150M operating profit loss of enduring impact; or One off impact of more than \$750M; or More than \$1B impact to balance sheet
		Interstate	Less than \$700K operating profit loss of enduring impact; or One off impact of less than \$3M; or Less than \$25M impact to balance sheet	\$700K to \$3M operating profit loss of enduring impact; or One off impact of \$3M to \$15M; or \$25 to \$125M impact to balance sheet	\$3M to \$15M operating profit loss of enduring impact; or One off impact of \$15M to \$80M; or \$125M to \$250M impact to balance sheet	\$15M to \$50M operating profit loss of enduring impact; or One off impact of \$80M to \$250M; or \$250M to \$500M impact to balance sheet	More than \$50M operating profit loss of enduring impact; or One off impact of more than \$250M; or More than \$500M impact to balance sheet
		Hunter/Valley	Less than \$1.5M operating profit loss of enduring impact; or One off impact of less than \$7M; or Less than \$25M impact to balance sheet	\$1.5M to \$7M operating profit loss of enduring impact; or One off impact of \$7M to \$35M; or \$25 to \$125M impact to balance sheet	\$7M to \$35M operating profit loss of enduring impact; or One off impact of \$35M to \$180M; or \$125M to \$250M impact to balance sheet	\$35M to \$100M operating profit loss of enduring impact; or One off impact of \$180M to \$500M; or \$250M to \$500M impact to balance sheet	More than \$100M operating profit loss of enduring impact; or One off impact of more than \$500M; or More than \$500M impact to balance sheet
		Support Services	Less than \$400K operating profit loss of enduring impact; or One off impact of less than \$2M; or Less than \$10M impact to balance sheet	\$400K to \$2M operating profit loss of enduring impact; or One off impact of \$2M to \$10M; or \$10 to \$50M impact to balance sheet	\$2M to \$10M operating profit loss of enduring impact; or One off impact of \$10M to \$50M; or \$50M to \$100M impact to balance sheet	\$10M to \$30M operating profit loss of enduring impact; or One off impact of \$50M to \$150M; or \$100M to \$200M impact to balance sheet	More than \$30M operating profit loss of enduring impact; or One off impact of more than \$150M; or More than \$200M impact to balance sheet
Environment		Minimal environmental impact	Limited and recoverable environmental impact	Significant and recoverable environmental impact	Permanent impact to area of less than high environmental significance	Permanent impact to area of high environmental significance	
Regulatory		Expected to prompt regulatory interest	Increased oversight by regulator	Limited fine, official caution and/ or direction to act	Formal regulatory action impacting on operating activities and/ or material fine	Prosecution of the company and/ or its office holders	
Reputation		Short term loss of confidence from other than key stakeholders	Sustained loss of confidence from other than key stakeholders	Short-term loss of confidence from a key stakeholder	Sustained loss of confidence from a key stakeholder	Loss of Shareholder support	
		Not Significant	Minor	Moderate	Major	Extreme	
		1	2	3	4	5	
Likelihood	Almost Certain	Once per month (Is expected to occur in most circumstances)	MEDIUM 1A	MEDIUM 2A	HIGH 3A	VERY HIGH 4A	VERY HIGH 5A
	Likely	Between once a month and once a year (Will probably occur in most circumstances)	LOW 1B	MEDIUM 2B	HIGH 3B	VERY HIGH 4B	VERY HIGH 5B
	Possible	Between once a year and once in five years (Might occur at some time)	LOW 1C	MEDIUM 2C	MEDIUM 3C	HIGH 4C	VERY HIGH 5C
	Unlikely	Between once in 5 years and once in 20 years (Could occur at some time)	LOW 1D	LOW 2D	MEDIUM 3D	MEDIUM 4D	HIGH 5D
	Rare	Once in more than 20 years (May occur in exceptional circumstances)	LOW 1E	LOW 2E	LOW 3E	MEDIUM 4E	MEDIUM 5E

Figure 3: ARTC Risk Matrix

ARTC Project Risk Criterion

	Consequence				
Safety	Injury or illness with no impairment (may or may not require treatment)	Injury or illness with short-term impairment	Injury or illness with moderate but recoverable impairment	Injury or illness with long term to permanent impairment	One or more fatalities
Assets: Network Performance	Immaterial disruption to non-critical track section	Material disruption to non-critical track section or Immaterial disruption to critical track section	Material disruption to a critical track section recoverable in the short-term	Material disruption to critical track section not recoverable in the short term	Material disruption to critical track section not recoverable in the short term with significant long term impacts on customers
Assets: Organisational Capability	Manageable impact to internal operations, which may or may not require internal reallocation of existing resources	Missing short-term targets which may or may not require use of additional resources	Reduced ability to achieve business goals with some business impact	Material failure to achieve business goal(s) with significant business impact	Failure to achieve business goals with lasting impacts
Assets: Programme/Project Objectives	Minor impact on a programme / project objective	Minor impact on more than one programme / project objective	Significant impact on a programme / project objective	Severe impact on a programme / project objective or significant impact on more than one objective	Severe impact on more than one programme / project objective
Financial	Minor cost impact, that is able to be absorbed within existing project budget*	Minor cost impact to project budget*	Moderate cost impact to project budget*	Major cost impact to project budget*	Significant cost impact to project budget*
Environment	Minimal environmental impact	Limited and recoverable environmental impact	Significant and recoverable environmental impact	Permanent impact to area of less than high environmental significance	Permanent impact to area of high environmental significance
Regulatory	Expected to prompt regulatory interest	Increased oversight by regulator	Limited fine, official caution and / or direction to act	Formal regulatory action impacting on operating activities and / or material fine	Prosecution of the company and / or its office holders
Reputation	Short term loss of confidence from other than key stakeholders	Sustained loss of confidence from other than key stakeholders	Short-term loss of confidence from a key stakeholder	Sustained loss of confidence from a key stakeholder	Loss of Shareholder support
Schedule	*Schedule milestone exceeded with no significant impact on business objectives &/or cost	Schedule milestone exceeded with minor impact on business objectives &/or cost*	Schedule milestone exceeded with moderate impact on business objectives &/or cost*	Schedule milestone exceeded with major impact on business objectives &/or cost*	Schedule milestone exceeded with severe impact on business objectives &/or cost*

			Not Significant	Minor	Moderate	Major	Extreme	
			1	2	3	4	5	
Likelihood	Almost Certain	Once per month (Is expected to occur in most circumstances)	A	MEDIUM 1A	MEDIUM 2A	HIGH 3A	VERY HIGH 4A	VERY HIGH 5A
	Likely	Between once a month and once a year (Will probably occur in most circumstances)	B	LOW 1B	MEDIUM 2B	HIGH 3B	VERY HIGH 4B	VERY HIGH 5B
	Possible	Between once a year and once in five years (Might occur at some time)	C	LOW 1C	MEDIUM 2C	MEDIUM 3C	HIGH 4C	VERY HIGH 5C
	Unlikely	Between once in 5 years and once in 20 years (Could occur at some time)	D	LOW 1D	LOW 2D	MEDIUM 3D	MEDIUM 4D	HIGH 5D
	Rare	Once in more than 20 years (May occur in exceptional circumstances)	E	LOW 1E	LOW 2E	LOW 3E	MEDIUM 4E	MEDIUM 5E

* parameters to be defined by project

Figure 4: ARTC Project Risk Matrix

Key terms used within the risk matrix are defined in Table 2.

Key Term	Meaning
Short-term impairment	An injury or illness with a level of impairment where full recovery is anticipated within a short period.
Moderate but recoverable impairment	An injury or illness with expected recovery of less than 12 months where a full recovery is anticipated.
Long term to permanent impairment	An injury or illness with expected recovery of 12 or more months, or where full recovery is not anticipated.
Material disruption	A disruption that causes significant impact on scheduled train movements.
Immaterial disruption	A disruption that causes little to no impact on scheduled train movements.
Critical track section	A section of track that is essential for the functioning of the network. Without that track section, train movements cannot occur.
Limited impact	Environmental impact that is restricted in size, amount, extent or harm.
Significant impact	Environmental impact that is restricted in size, amount, extent or harm.
Recoverable environmental impact	Temporary environmental impact where the ecosystem or land will recover naturally or via intervention to its pre-impact state.
High environmental significance	Landscape features, species or ecological communities that are listed in State or Commonwealth legislation or have high social, ecological or economic value.
Key stakeholder	<p>Stakeholders who can have a fundamental impact on the achievement of ARTC's business objectives.</p> <p>Key stakeholders would be expected to include ARTC Board, customers, partnership organisations, government bodies, regulators, and other organisations with influence over ARTC operations.</p>

Table 2: Risk Matrix Key Terms

4.2 Analysing risk

When analysing risk, there are two sets of consequences that are considered for each risk:

- The worst case – is a description of the worst consequence that could occur should controls be absent or fail. “Worst Case Consequence” is considered when determining the inherent (untreated) consequence, likelihood and risk level;

and

- The most likely – this is the consequence that is likely to occur, given the effectiveness of the controls that are currently in place. “Most Likely Consequence” is considered when determining the current consequence, likelihood and risk level.

Most likely consequence is also utilised when determining the target consequence, likelihood and risk level. In this context, the most likely consequence will include consideration of the likely effectiveness of the additional proposed treatments that are to be implemented.

ARTC has six risk impact categories: Safety, Asset (Network Performance and Organisational Capability), Financial, Environmental, Regulatory and Reputation; which are documented on the ARTC Business Risk Profile and are assessed using the risk matrix. The Project risk matrix includes further impact categories of Programme/Project Objectives and Schedule.

For many risks, consequences may occur across more than one of these categories. The Enterprise Risk Management System allows different consequence ratings to be applied across these different impact categories. The consequences should be identified first, and then the likelihood of that particular consequence eventuating. The highest consequence rating will then be used to calculate the risk level.

5 EVALUATING RISK

The purpose of risk evaluation is to make decisions about the degree of control required for each risk to ensure that it is being managed within ARTC’s risk appetite and risk tolerance. It involves the identification of the range of options that can be deployed for treating the risks.

These options will require assessment in terms of which is the best to adopt and the subsequent preparation and implementation of treatment plans and activities. ARTC uses the terminology Current Control to describe existing controls that are in place and Proposed Treatment to describe the additional measures that are to be put in place. Risks can be treated via a single strategy or the combination of a number of strategies.

For risks with potential safety impacts, ARTC adopts the SFAIRP (So Far As Is Reasonably Practicable) principle when addressing this phase of the assessment.

5.1 ARTC Risk Management and SFAIRP

It is essential that the process for identifying, analysing, evaluating and controlling risks that have potential safety impacts is rigorous, structured and auditable.

The ARTC risk management framework, including the Enterprise Risk Management System, is structured in such a way that, when followed effectively, provides evidence and justification in the determination of the provision of safety So Far As Is Reasonably Practicable (SFAIRP).

In determining what is 'reasonably practicable', the following five factors must be considered:

1. The likelihood of the risk concerned eventuating;
2. The consequence, or degree of harm, that would result if the risk eventuated;
3. What was known or ought reasonably to be known, about the risk and any ways of eliminating or reducing the risk;
4. The availability and suitability of ways to eliminate or reduce the risk; and
5. The cost of eliminating or reducing the risk.

Consideration of what is "reasonably practicable" is undertaken in two stages:

1. Identification of what is possible to be done to ensure safety
2. Consideration of whether it is reasonable, in the circumstances, to do all that is possible.

In the evaluation and control of identified risks, the Hierarchy of Controls is a key tool used to consider all possible controls to eliminate or reduce a risk from most desirable (elimination) to least desirable (administration and personal protection equipment). Where risks are managed rather than eliminated, ARTC must:

- ensure adequate controls are applied;
- provide training, education, instruction and information;
- provide supervision; and
- periodically review the relevant risk(s) and its controls.

5.2 Evaluation and control for Non-SFAIRP risk assessment

During a risk assessment or risk review for a risk with no potential safety impacts, the following five questions should be asked in order to determine the best ways to eliminate, reduce or optimise the level of risk:

1. Can we eliminate or avoid the risk entirely?
2. Can we control the cause of the risk?
3. Can we control the scenario or circumstance associated with the risk?
4. Can we reduce the likelihood of the risk occurring?
5. Can we reduce the consequence of the risk?

Identifying options for the control of risks with positive outcomes

- Actively seek an opportunity to start or continue with an activity likely to create or maintain the positive outcome
- Change the likelihood, to enhance the likelihood of beneficial outcomes
- Change the consequences, to increase the extent of gains

Identifying options for the control of risks with negative outcomes

- Eliminating or avoiding the risk
- Change the likelihood of the risk, to reduce likelihood of negative outcomes
- Change the consequences, to reduce the extent of losses

Understanding ways to eliminate, reduce or optimise risk can be gained by:

- Reference to established standards, where applicable. This may include local and international standards, codes of practice, company procedures and track access agreements. The standards used must be applicable to the risk;
- Reference to 'good practice';
- Drawing on knowledge held by those performing the assessment and of stakeholders.

The following should be considered when establishing what is 'good practice'

- The practice is established in the jurisdiction, or another jurisdiction which has railway operations that are similar in scale to the operation in question;
- The practice is established and widely implemented in a similar industrial sector;
- The practice is enforced by legislation in more than one other country.
- The practice has demonstrably improved safety in its current application;
- The application of the risk elimination or control measure is relevant to the circumstances, as shown by experience of other organisations facing similar operating conditions;
- The established risk elimination or control measure of combination thereof has a proven track record in terms of incident history both locally and internationally; and
- The application of the risk measure is supported by existing reports or studies.

6 TREATING RISK

6.1 Proposed Treatments

Where the risk level is not acceptable and/or where causes or consequences have no current controls, additional controls may need to be implemented, referred to as a "Proposed Treatment". This may be a new control, strengthening of a current control, or mechanisms for monitoring that controls are being properly maintained.

While applying a Proposed Treatment may not reduce the overall Risk Level, it may address a specific causal or contributory factor that is otherwise not controlled, and therefore provide an additional level of protection against the possibility of the risk eventuating. This can be important when determining whether the risk is addressed SFAIRP.

Actions to confirm decisions for proposed treatments or to implement additional approved treatments are to be recorded. This may include mechanisms for monitoring that the controls are being properly maintained.

Responsibility for additional treatments should be allocated to those best able to control the risk. Responsibilities should be agreed between the stakeholders at the earliest opportunity at appropriate actions recorded in the Enterprise Risk Management System with progress status periodically updated.

Review should take place soon after the implementation of the proposed treatment and then at intervals afterwards dependent on the level of risk and anticipated effectiveness.

Guidance on conducting a review of a control is provided in section 8.4.

6.1.1 Suitability of Proposed Treatments

A proposed treatment needs to be assessed for its suitability under the circumstances. This involves whether the proposed treatment:

- Is effective in eliminating or minimising the likelihood and/or consequence of the risk; and
- Does not introduce new or higher risks; and
- Is available, technically suitable and practical to implement under the circumstances.

This includes considering the following:

- How effective would the additional and/or improved controls be?

Consider how available and suitable the controls are, the level of effort that is required to implement them, how much time is needed to deploy them and any other relevant factors. Consider the effectiveness of individual controls and how they will work together in combination.

- What would be the relative cost to implement the additional and/or improved controls?

Relative to the benefits likely to be provided by any new or improved controls, what are the relevant cost implications to implement the controls? Consider such costs as capital, maintenance, installation, commissioning, administration, training etc.

Further information on determining the suitability of controls is available in *Meaning of Duty to Ensure Safety So Far As Is Reasonably Practicable Guideline*, Office of the National Safety Regulator, issued December 2014.

6.1.2 Implications of Proposed Treatments

When considering potential treatments, consideration needs to be given to whether any new risks will arise from the additional controls and/or whether effectiveness of other current controls will be negatively affected.

This can be an important factor in deciding whether to proceed with implementing the control. Where an additional control is possible, but negative implications have been identified, a careful decision has to be made regarding which risk may be higher.

6.2 Rejecting a Proposed Treatment

Demonstrating SFAIRP requires that all possible controls are considered, analysed and decisions made regarding whether to proceed with implementation.

It is essential that rejected proposed treatments and information regarding the decision to reject the proposed treatment is recorded against the risk record in the Enterprise Risk Management System. This includes:

- Why the proposed treatment was rejected
- Reference to information / documents utilised in making the decision
- Who made the decision to reject the proposed treatment
- When the decision was made

Rejected proposed treatments should be regularly reconsidered to see if any factors have changed since the decision has been made that may mean that implementation of the proposed treatment is now “reasonably practicable”. This can include:

- An increase in likelihood or consequence of the risk, which may alter cost-benefit assessments
- Reductions in cost for implementation
- Technological changes which may mean implementation is now technically feasible
- Increased expectations from stakeholders

6.3 Determining Target Risk Level

Once Proposed Treatments have been identified, the Target Risk Level can be determined with consideration given to likely effectiveness of the Proposed Treatments in combination with Current Controls.

If there are no additional Proposed Treatments or where additional Proposed Treatments are to be implemented, however are not expected to result in a reduction in risk level, Target Risk Level is to be recorded as the same as Current Risk Level and appropriate notes recorded explaining why no further reduction can be achieved.

6.3.1 Setting the Target Date for Risk Reduction

If the Target Risk Level is lower than the Current Risk Level and/or the risk is anticipated to be closed in the future, a Target Date for the risk reduction is to be recorded. Only dates in the future are to be selected.

If the Target Date is yet to be determined, an appropriate comment must be added and the Target Date recorded once known. If there is no expectation that the risk can be reduced or closed, no Target Due Date is to be recorded.

7 REMOVING A CONTROL (REVERSE SFAIRP)

On occasion, it may be appropriate to remove an existing control. Examples of where it may be appropriate to remove a control include:

- Where another control has been implemented that more effectively reduces risk, rendering the initial control irrelevant or unnecessary
- Where it has been identified that an existing control is causing adverse effects, or increasing other risks
- Where it has been identified that the relevant causal or contributory factors are no longer present, and the control is therefore no longer required

Decisions to remove a control (either fully or partially) need to be carefully considered and all potential impacts assessed prior to removing the control. Items to consider during the decision making process include, but are not limited to:

- Is the control relevant to other risks, and if so, will these be adversely affected?
- Will the removal of the control potentially introduce other, new, risk sources (hazards) or reintroduce risks previously considered eliminated?
- If the control is removed, will the relevant causal and contributory factors have other appropriate controls in place?
- Will removal of the control mean that the residual risk is no longer eliminated or minimised SFAIRP?

Information regarding the decision to remove (or reduce) an existing control is to be recorded. This includes:

- Why the existing control was removed or reduced
- Reference to information / documents utilised in making the decision
- Who made the decision to remove or reduce the existing control
- When the decision was made

8 MONITORING AND REVIEWING RISK

Depending on the nature of the risk, risk level and the activity for which it has been identified, it may be appropriate for reviews to be scheduled to occur:

- At a set timeframe
- At a certain stage of activity, for example, in advance of key milestones, at completion of a Project Phase or a Project Hold Point
- At a time when it is anticipated Proposed Treatments will be fully implemented and operational

Where a Project's size and complexity merits, it may be appropriate to schedule a regular monthly risk review. Where Projects have ongoing monthly risk reviews detailed 'deep dive' review of individual risks can be scheduled on a rotating basis.

Requirements for minimum timeframes for scheduled risks are prescribed in RSK-PR-001 Risk Management and RSK-WI-005 Project Risk Management.

Scheduled reviews and their planned due date are to be documented in the Enterprise Risk Management System, and if appropriate relevant records uploaded (or referenced).

Following the review, the risk entry is to be updated to reflect any changes or additional information identified during the risk review or control review.

Note: An Enterprise Risk Management System is being progressively implemented across ARTC. Project risks not yet transferred into the system will continue to be managed via stand-alone project risk registers until the project has been transitioned into the system, where transition is deemed appropriate, or until the project end. Decisions will be made on a case by case basis as to whether project registers will be transitioned into the system.

8.1 Preparing for the Review

Risk reviews may be undertaken in a number of different ways, including:

- Embedding reviews of risks into other forums, for example regular team meetings or project meetings, and reviewing one or two risks at each meeting;
- By reviewing a single entry when information regarding the risk is received, for example an investigation or audit finding, or after Proposed Treatment(s) have been implemented; or
- A dedicated risk review workshop where a number of risks are reviewed at the same time.

Preparing for a risk review is undertaken in a similar way to preparing for a risk assessment.

Consider who needs to contribute to the risk review. This could include:

- Risk Owners and Managers
- Relevant Control Owners
- Subject Matter Experts

Gather any information that may be required to be considered during the review. This could include:

- Relevant audit reports
- Investigation reports
- Incident data
- Updates on the progress of implementation of additional Proposed Treatments

Consider whether any information needs to be distributed prior to the review. Depending on the risk, attendees and confidentiality of any information to be utilised during the review, it may be appropriate to have reference material available at the review, but not distributed in full to all attendees.

8.2 Conducting the Review

Depending on the nature, scope and context of the risk(s), a number of factors will need to be considered during the review.

Factors commonly considered include the following:

General Factors

- Is the risk still a current valid risk?
- Is any amendment required to the Risk Owner, Risk Manager, business unit, location etc.?
- Is the risk assigned to the correct risk tier?
- Is the risk adequately and appropriately described?

Context

- Have any external factors changed? For example, legislative changes, changes to customers, environment changes etc.
- Have any internal factors changed? For example, new internal requirements (standards, rules, procedures etc.), organisational changes, operations changes etc.

Related Incidents

- Have there been any related incidents? What happened? What was the outcome of investigation?
- Any new (or previously unidentified) causal or contributory factors?
- Were controls effective or not effective for those incidents?
- Are incident numbers trending upwards or downwards? What does this indicate about control effectiveness?

Related Audits

- Have there been any audits relevant to the risk and/or controls?
- If so, what were the findings?
- Are there any recommendations that could be considered as additional Proposed Treatments?

Controls and Proposed Treatments

- Are all current controls adequately described with information completed correctly?
- Are there additional Proposed Treatments that are being implemented, that are not documented?
- Are there any indications that effectiveness of current controls have changed?
- Are controls in place for all causal and contributory factors? What else could be done?
- Are there treatments that have been previously rejected? If so, is it feasible for them to now be considered?
- Is safety provided SFAIRP?

Once all factors have been considered, the risk level is to be assessed, and modified if required.

Risk Reviews can be documented in the Enterprise Risk Management System using the Workshop capability as prescribed in RSK-GL-001 Risk Management Terms and Data Guideline. Where the full Workshop functionality is not appropriate (for example, where a single risk has been reviewed and updated) notes are to be made.

8.3 Unscheduled Risk Review

A review of a risk may be required to be conducted prior to the scheduled review. Examples of where it may be appropriate to conduct an unscheduled risk review include:

- Following a significant related incident
- Following an audit where significant findings have been identified
- As part of change management processes
- Where a new (or previously unidentified) causal or contributory factor has been identified
- Where there has been a change to the internal or external context that significantly impacts the risk

Unscheduled risk reviews are performed in a similar manner to a scheduled risk review however the scope of the review may be more limited and focused on a particular area of interest. Where this occurs, the limited scope should be appropriately documented and retained against the risk entry.

8.4 Reviewing a Control

Sometimes it is appropriate to review a control independently of a full risk review. This is particularly the case where a control is applicable to a number of separate risks. A review of a control is undertaken for a number of reasons:

- To determine the effectiveness of a control
- Following implementation of a new control or following implementation of changes to a control
- As part of change management processes, where a change is intended to be made to the control
- To identify why a control has failed or not been effective, for example as part of an investigation

How the control review is conducted often depends on why the review is being undertaken.

Where the control review is conducted following the implementation of a new control or changes to the control, the review is to include determining effectiveness of the control and whether new risks, or changes to other existing risks have occurred.

Appropriate notes should be recorded against the applicable control entry.

8.4.1 Monitoring and Validating Controls

The effectiveness of controls can be validated by a number of different methods. This includes:

- Formal audit
- Investigation
- Data monitoring
- Inspection
- Observation of activities
- Anecdotal evidence

The method utilised to validate the effectiveness of the control is to be appropriate for the associated risk, risk level and the level of criticality of the control.

For some controls, it may be appropriate to use a combination of methods to provide assurance of the ongoing effectiveness of the control.

8.5 Determining Next Review

Appropriate timing for the next review will depend on the type of review that has been conducted and the scope of that review.

Where a control review has been undertaken with limited scope (i.e. not all relevant controls for the risk were considered) a full scheduled review of the risk is still required to occur in accordance with RSK-PR-001 Risk Management.

Where an unscheduled risk review has occurred, if the review was conducted with sufficient scope to be considered a full review then the next scheduled risk review may be calculated based on the date of the unscheduled risk review. Where an unscheduled risk review is conducted with a narrow, limited scope, the planned date for next scheduled review is to remain as originally scheduled.

Where scheduled risk reviews are conducted, timing for the next review will be calculated in accordance with RSK-PR-001 Risk Management and recorded against the risk entry in the Enterprise Risk Management System.

Note: An Enterprise Risk Management System is being progressively implemented across ARTC with risks being progressively transferred into the system. Review and reassessment of risks in accordance with the new matrix will be required and for many risk entries, additional information may be required to be populated and/or relationship mapping undertaken. Following transfer, review to complete this activity should be undertaken within six months of the risk owner receiving system training. Review dates may be extended beyond the specified timeframes to enable this to be undertaken.

9 CONDUCTING WORKSHOPS

Risk workshops may be conducted in a number of different contexts, including:

- Identification and assessment of new and emerging risks
- Identification of changes to existing risks, for example, as part of management of change processes
- Review of a series of risks associated with a particular activity, asset or topic

A risk workshop could also focus on a specific control and all risks to which it relates, for example, in situations where major changes are anticipated to an existing control or a significant control review is to be undertaken.

It is not mandatory that identification, assessment and review activities are conducted within workshop settings. Embedding of these activities into other regular forums and day to day practices is encouraged, however where dedicated workshops are conducted this section gives guidance on requirements and processes to be undertaken.

9.1 Allocate Responsibility

Responsibility for convening a workshop rests with the person with management responsibility for the risks being identified or reviewed. A workshop may also be convened by the person with management responsibility for a control. The Workshop Convenor has the responsibility to appoint an appropriate Workshop Facilitator.

Responsibility for the facilitation of the workshop and completion of risk information in the Enterprise Risk Management System is to be clearly allocated. When allocating responsibility for facilitating a risk workshop, the following factors should be considered:

- Does the person meet the required criteria to be a Workshop Facilitator?
- Does the person have sufficient capacity to undertake the required activities within the required timeframe?
- Does the person have experience in the specific risk identification or assessment methodology that is proposed to be utilised? (For example, where a specific methodology such as Quantitative Risk Analysis is proposed)
- Is the person sufficiently independent / able to facilitate objectively and without bias?

Note: Although outcomes of risk workshops are to be recorded in the Enterprise Risk Management System, there may be occasions where the most appropriate facilitator does not have access to the system, for example, an external facilitator. In this circumstance, responsibility for ensuring recording of information must be assigned to an appropriate system user.

9.2 Identify Key Stakeholders

Risk Management activities should be conducted in consultation with stakeholders and Subject Matter Experts. Consideration of appropriate stakeholders allows for identification of suitable people and organisations to be involved in the Risk Management process. Those identified stakeholders should also be involved in ensuing communication and consultation processes.

The roles of stakeholders in the risk assessment may vary and can include:

- Stakeholders who provide information prior to risk assessment or review activity
- Stakeholders who actively participate in a risk assessment or risk review workshop
- Stakeholders who provide feedback on outcomes of a risk workshop
- Stakeholders who may be requested to complete activities to implement additional controls

Internal or external subject matter expertise may be required, which commonly includes:

- Technical experts specific to the scope of the risk assessment
- Work Health and Safety / Rail Safety
- Environment
- Human Factors

Stakeholders can also include people or organisations that are, or may be, affected by the risk or the control measures and may include individuals, groups of people, alliance partners, other organisations, regulatory bodies, the public etc. Where external stakeholders are included, careful consideration needs to be given to any matters likely to be discussed that may be of a confidential nature and whether it may be appropriate to hold more than one workshop or seek their input via other mechanisms.

Information about stakeholders and their involvement in the risk workshop is to be documented in the Enterprise Risk Management System.

9.3 Organise Risk Workshop

Sufficient facilities, time and space are essential to a successful risk workshop. Factors to consider when organising a risk workshop include:

- Sufficient allocation of time for discussions/brainstorming activities;
- Suitable notice period for any required travel arrangements to be organised;
- Internet access to enable use of the Enterprise Risk Management System, where the workshop is being directly facilitated using the system; and
- Required facilities, including access to teleconference facilities, overhead projectors, white boards / note boards for brainstorming, room size etc.

9.4 Establish the Objectives, Context and Scope

Establishing the Workshop Objectives, Scope, Background and Context can assist with appropriately determining participants, identifying any information that needs to be collated prior to the workshop, and the successful completion of the workshop.

This step shall be carried out by the workshop convenor prior to the workshop taking place.

Information regarding the Background and Context and Scope of the Workshop is to be recorded in the Enterprise Risk Management System. The amount of information available at this point may depend on the scope and complexity of the process/proposal that is being considered however should include the information detailed in sections 9.4.1 and 9.4.2.

Where required information is unable to be appropriately determined prior to the Workshop, this information shall be determined and documented as part of the finalisation of risk entries, either at the workshop or following the workshop and prior to distribution of draft workshop outcomes.

9.4.1 Establish the Context

The Context of a workshop is made up of a number of factors.

9.4.1.1 Workshop Title

Workshop Title is a clear summary statement of the intent of the workshop such as “Assessment of the safety/operational risks associated with the construction of ABC over the area bounded by x and y”, or “Review of risks associated with the operation of Road Rail Vehicles”.

9.4.1.2 Workshop Objectives

The Workshop Objective(s) outlines what ARTC wants to achieve as a result of the workshop.

There may be a number of objectives that are expected to be addressed. For example, objectives may include identifying risks associated with an activity or interface, identifying controls to reduce those risks So Far As Is Reasonably Practicable (SFAIRP) or provide supporting analysis to a submission etc.

9.4.1.3 Background and Context

Background and Context record information that clarifies the nature of the workshop being undertaken.

Background and Context information may include:

- Background - any background information that helps to set the context of the workshop.
- Assumptions - any assumptions that have been made.
- Qualifications/Conditions - what qualifications or conditions are needed to ensure that there is no misunderstanding of any of the context setting components. A qualification can be a dependency or requirement that needs to be highlighted.
- Critical Success Factors - the critical success factors of the activity/proposal/project being risk assessed. For example, the objectives of a particular project may be to remain on budget, on schedule and deliver to specifications. Once we know the objectives of the activity we are risk assessing, we can then identify risks that affect achievement of those aims.

This information should be prepared, entered into the Enterprise Risk Management System and distributed to stakeholders in advance of the risk assessment workshop. The information can take the form of a spreadsheet, PowerPoint, drawing, report, or any other format or combination of formats. Documents distributed are to be linked to the workshop either via hyperlink or upload, whichever is appropriate. Refer to section 9.5 for further information.

At the commencement of the risk workshop, it is good practice for the Workshop Facilitator, or other suitable Subject Matter Expert, to verbally explain the situation, including supporting background information.

9.4.2 Determine the Scope

The scope outlines what is to be included within the risk workshop, and what is to be excluded.

Scope descriptions may also include:

- Exclusions - those items that are specifically excluded from the scope of the discussion such as the interfaces with another organisation
- Constraints - what constraints the proposal is operating under which can be broadly categorised as: Political (including regulatory), Economic, Social Technological Legal and Environmental
- Boundaries - the boundaries of the risk assessment which can be made up of such things as: Geographical, Operational, Interface, Phase, Time driven and Other boundaries

Once the scope of the risk workshop has been defined it may be appropriate to divide the scope into smaller parts.

If the scope of the task is very large or complex, it is often appropriate to divide the scope into the component sections, areas, projects, activities, tasks or functions to make the next stage easier to progress with. For example, risk assessment related to a project may be broken down into design, construction and implementation phases that are assessed at separate risk workshops.

9.4.3 Additional Information

Other information may also need to be recorded. This may include reference to any relevant standards / documents or any other comments and information that can assist in understanding the context clearly.

9.5 Distribute Pre-Workshop Reading

A copy of the Risk Workshop Objectives, Background and Context and Scope is to be distributed to enable review by attendees prior to the workshop.

Other information that may be appropriate to distribute prior to the risk workshop can include:

- Any relevant procedures or documents
- Relevant incident statistics, and/or investigation outcomes
- Copies/extracts of relevant legislation or standards
- Briefing papers

Pre-workshop reading material should be distributed with adequate time for review prior to attendance at the workshop.

Where existing risks are relevant to the risk workshop, these should also be included as pre-workshop reading material.

When distributing pre-workshop reading, it may also be appropriate to request workshop attendees commence identifying risks and controls relevant to context of the workshop, and to either forward these to the workshop facilitator prior to the workshop and/or bring their notes to the workshop.

9.6 Conduct Risk Workshop

Information collated and documented prior to the workshop is to be reviewed and amended if required.

Where required information was unable to be appropriately determined prior to the risk workshop, these sections shall be completed at the workshop / prior to finalisation of the risk and/or control entries.

RSK-GL-003 Risk Management Overview is a reference guide that provides a summary of key information that workshop participants find useful to refer to during the workshop process. RSK-GL-005 Project Risk Management Overview is an editable version of the reference guide that may be customised for a specific programme or project.

Outcomes of the risk workshop are to be documented in the Enterprise Risk Management System using the workshop functionality. Ideally the workshop should be run live with the information time-stamped to that workshop, although this may not always be possible. Where this is not possible outcomes are to be recorded including details of attendees.

Risk and/or control entries are to be created or updated in the Enterprise Risk Management System. Supplementary information may also be uploaded or linked as appropriate.

Following the workshop, new or updated risk entries are to be submitted to the applicable Risk Owner for approval. Outcomes of the risk workshop may also need to be distributed to other key stakeholders as deemed appropriate.

APPENDIX 1 – RISK IDENTIFICATION METHODS

General Methods of Risk Identification & Assessment

Risk issues may be identified in a number of ways. Methods that are within the capability of ARTC to carry out without external assistance include, but are not limited to:

Checklists

An extensive although not exhaustive list of sources of safety related risk is included in Appendix 1 of this work instruction. Checklists should be used as a “memory jogger” during risk assessments to aid in the capture of risks that might otherwise be overlooked.

Brainstorming

Brainstorming with the right mix of stakeholders can be a very powerful way to extract good quality risk information. When conducted as a group activity, brainstorming should be done in a controlled and structured manner, otherwise such matters as ‘group think’ occur. Group think is the acceptance of obviously wrong answers simply because it is socially unacceptable to disagree, where there are conflicts of interest.

A good technique is to ask individuals to write any potential risks on a sticky note. This can be done either at the start of a workshop or as a separate short 30 minute exercise. The notes are then stuck to a board and further analysed and grouped by the participants. Either after the workshop or during a break, the facilitator assesses the relevance of the risk issues and summarises them for further workshop analysis.

Railway Safety Records & Reports and Historical Records

The ARTC Train Control Report (TCR) is the initiating reporting document for the management of safety, asset and operational related events on the ARTC network and is also the basis of reporting rail safety incidents to the Rail Safety Regulators.

TCRs are submitted to Network Controllers and Train Transit Managers from a wide range of internal and external stakeholders, and are then entered through NRAMS, which is linked to the Safety Information Management System (SIMS). SIMS data is analysed regularly to identify the appearance of new risks or a change in risks already identified.

A Generic Checklist that has been primarily derived from TCR and other incident data provides a high level list of potential risks and precursor events that can be utilised to assist in this process (refer RSK-GL-001 Risk Management Overview).

Findings from major incident investigations and audits are analysed individually and in conjunction with the Risk Register to identify possible new risks. Historical records, databases and articles on incidents and accidents both foreign and domestic should be sought out where possible and appropriate.

Horizon Scan

A horizon scan is performed by brainstorming with other stakeholders any significant events or changes that may occur over a relevant timescale, such as over the course of the next year.

Once these have been brainstormed, consider how these might impact your business objectives. For example:

- Will they introduce new risks that we need to manage?
- Do they affect the likelihood or consequences of current risks? Or
- Are there other implications?

PESTLE analysis

A PESTLE analysis provides a structured approach to brainstorming that can help to identify internal and external factors that may impact your activities.

PESTLE is an acronym for six areas for consideration:

- Political
- Economic
- Social
- Technological
- Legal, and
- Environmental

The results of a PESTLE analysis can be combined with a horizon scan to provide a more thorough analysis in order to identify where you may have potential risks.

Additional Specific Methods of Risk Identification & Assessment

The following methods are useful tools for the identification of risks, but require specialist assistance. The techniques below require technical knowledge and a level of competency to be carried out effectively. Depending on the level of complexity of the risk scenario or activity being assessed, external assistance may be required to conduct the following risk identification techniques:

Decomposition Techniques

Where a proposal or project can be broken down into component parts, each of which is then considered on its own if risk events occur.

Process Maps

By describing a process using flow charts it is sometimes possible to identify risks involved at each stage in the process.

Fault Tree Analysis (FTA)

FTA can be used to identify risks in a process or system. These techniques are detailed methods of risk identification and staff should be trained in using these approaches before applying them.

HAZOPs and FMECA studies

This includes past accident and incident data from databases within the organisation and external to the organisation in a related industry. This could also include near miss incident data.

Human Factors Assessment

Human Factors Assessments focus on the identification of potential Human Factors issues between the human user and the system they are interacting with. There are a number of different types of specific techniques that can be utilised.

Quantitative assessment

The risk assessment workshop shall assess the requirement for a quantitative assessment on the basis of the complexity of the risks being assessed.

Where a quantitative approach is required, based on the conclusion that the qualitative approach is not adequate, there needs to be an evaluation of the type of quantitative approach to adopt. Considerations should include the availability of existing tolerability data for the subject in question and the determination of the final outcome of the quantitative analysis.