

Application of Risk Management

RSK-WI-001

Applicability

ARTC Network Wide SMS

Publication Requirement

Internal / External

Primary Source

RSK-PR-001 – Risk Management Procedure

Document Status

Version #	Date Reviewed	Prepared by	Reviewed by	Endorsed	Approved
2.0	8 March 2023	Corporate Risk Team	Risk Working Group	GM Corporate Risk	Executive Management

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.
1.2	19 February 2018	Various	Change of title for Executive roles. Change Division/ Business Unit.

© 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.

1.3	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.
1.4	05 April 2019	Various	Replacement of term "Strategic Risk" with "Top Risk Event.
1.5	1 June 2020	4.1	Clarification that no requirement for assessment of Inherent Risk level for project risks
1.6	29 June 2022	All	Revision of content throughout to refocus instruction and align with updated risk management procedure document.
2.0	8 March 2023	Various	Major update to procedure to align with current Risk Management Practices across ARTC, reviewed by Risk Working Group

Table of Contents

Table of Contents3

1. Introduction.....4

 1.1 Scope & Purpose4

 1.2 Benefits4

2. Overview & Application5

 2.1 Overview5

 2.2 Accountabilities & Responsibilities.....5

 2.3 Risk Management Process4

 2.4 Risk Assessment.....5

 2.4.1 Risk Assessment overview..... 5

 2.4.2 Application of Risk Management Activities 7

3. Bowtie Risk Assessment Format.....9

4. Appendix11

 4.1 Appendix A – Glossary of key risk management terms11

 4.2 Appendix B – ARTC Risk Management Responsibilities and Accountabilities13

 4.3 Appendix C – Associated Documents.....15

1. Introduction

1.1 Scope & Purpose

This Work Instruction provides further detail on ARTC’s risk assessment process and provides guidance to users on how to practically apply risk management principles in various risk scenarios. This document provides general guidelines but is not intended to be exhaustive or prescriptive. Users seeking to manage risks are encouraged to apply appropriate judgement to their specific risk management activity and consult the Corporate Risk Team if they require further assistance.

The Work Instruction is to be used in accordance with RSK-PR-001 Risk Management Procedure.

1.2 Benefits

Applying the risk management discipline effectively provides ARTC with the following benefits:

- Increased awareness of risk across the organisation
- Risk informed and effective decision making
- Increased confidence of achieving organisational goals and strategic priorities
- Improved workplace safety and security for employees and contractors
- Improved operational efficiency through consistent application of risk processes and controls
- Improved resource allocation
- Identification of opportunities

2. Risk Management Process

This work instruction focuses on the risk assessment stage of the risk management process as outlined in figure 2 below. Risk assessment is made up of 4 stages which includes the identification, assessment, evaluation, and development of actions. Stakeholder communication and consultation is a key aspect that occurs at each stage of the process

Further details regarding the end-to-end risk management process is outlined in RSK-PR-001 Risk Management Procedure.

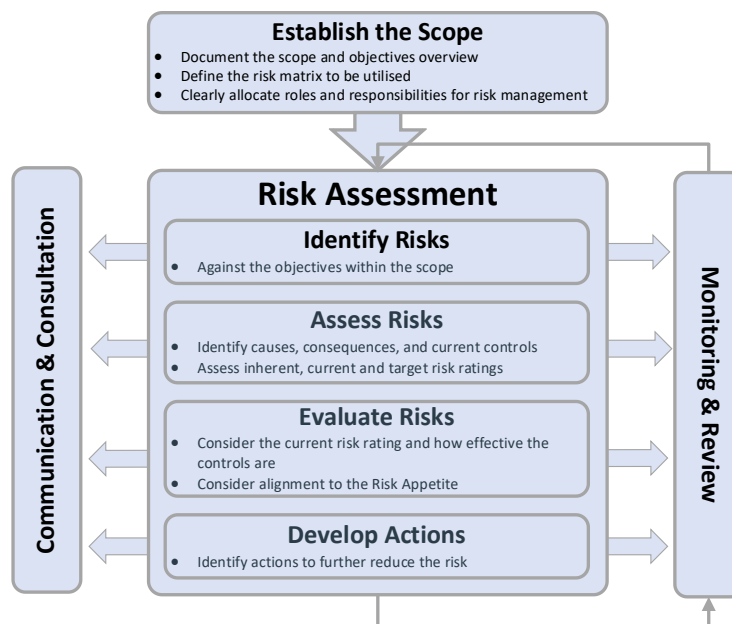


Figure 2: Risk Management Process Model

3. Overview & Application

3.1 Overview

This work instruction provides guidance on how to practically apply the assessment stage of the risk management process.

3.2 Accountabilities & Responsibilities

All employees have responsibility for managing risks within the business. An overview of relevant accountabilities and responsibilities in respect to this work instruction is outlined below:

Line Management – has responsibility for identifying where risk assessment activity may be required to be undertaken and providing relevant information and input in risk assessments. In addition, Line Management is accountable for identification of risks and monitoring, reviewing and updating the progress of Actions.

Risk Owner – has accountability for managing risks under their ownership, including the review of the risks and effectiveness of existing controls. In addition, Risk Owners are responsible for ensuring appropriate Actions are identified and updated.

Risk Manager – has delegated responsibility to manage the content and status of a risk on behalf of the Risk Owner.

Control Owner – has accountability for effective design, implementation, and ongoing application of a control.

3.3 Risk Assessment

3.3.1 Risk Assessment overview

Common events that may give rise to the need for a risk assessment include:

- Core Business Delivery, Divisional Planning & Improvement
- Project planning and delivery
- Changes to Infrastructure or Asset Configuration, including System Safety Assurance
- Deviating from established standards (e.g., Engineering Standards, System Specifications, etc)
- Deviating from Standard Operating Protocols (SOP)
- Operational Health, Safety and / or Environmental Risk Assessment
- Third-party request to access ARTC infrastructure
- Procurement

The above list is not an exhaustive list of all events. The type of risk assessment to be complete is dependent on the activity undertaken.

What	When	How	Outputs
Core Business Delivery, Divisional Planning & Improvement	During the planning phase (e.g., annual planning cycle) with periodic updates as appropriate	Broad qualitative risk assessment to establish key risks to business objectives or the success of an improvement initiative (e.g., risk workshop)	Risk statements describing how ARTC manages risks associated with the delivery of core business should be outlined in the Risk Management System. These are primarily risks to core business objectives. Business planning and improvement initiatives are also subject to risk which should also be outlined in the Risk Management System.

			These risk statements will be managed on an ongoing basis until the risk is closed.
Project planning and delivery	During the project planning phase and at regular intervals throughout the course of the project (e.g., align with project approval stage gates)	Qualitative and/or quantitative risk assessment to identify risks to successful project delivery	<p>Risks to the successful delivery of complex, high value projects should be documented in dedicated registers within the Risk Management System. This will apply to nominated projects rather than routine works that are conducted under repeatable projects.</p> <p>These risk records will be managed on an ongoing basis until each risk is closed or is transferred to the operating business.</p> <p>If a specialist risk assessment is required (e.g., QRA) it should be documented in an appropriate format to support decision making, but only needs to be captured in the risk management system as a record against the relevant project risk.</p>
Changes to Infrastructure or Asset Configuration, including System Safety Assurance	Prior to authorisation to 'go live' on new infrastructure or assets.	<p>Most infrastructure or asset changes will be managed via the established Configuration Change Management (CCM).</p> <p>Specialist system safety risk analysis will be undertaken to support major changes.</p>	<p>Evidence of appropriate risk assessment will be required to support 'go live' decisions in line with instructions provided under established Configuration Control Management (CCM) or Management of Change (MoC) processes.</p> <p>Specialist risk assessments (e.g., System Safety Assurance (SSA)) should be documented in an appropriate format to support decision making, but only need to be captured in the risk management system as records against relevant project risks.</p>
Deviating from established Standards (e.g., Engineering Standards, System Specifications, etc)	Prior to formal authorisation of the proposed deviation from a Standard by Approval Authority	Structured qualitative risk assessment involving suitable technical stakeholders	<p>Evidence of risk assessment to be submitted with the relevant authorisation (e.g., waiver, type approval, etc).</p> <p>These risks should not be captured within the Risk Management System.</p>
Deviating from Standard Operating Protocols (SOP), including Network Rules & Procedures	<p>Prior to authorisation of the proposed deviation from SOP</p> <p>Prior to authorisation of changes to a SOP</p>	<p>Appropriate risk assessment when deviating from SOP</p> <p>Structured qualitative risk assessment involving suitable technical stakeholders.</p>	<p>Evidence of risk assessment to support approval to deviate from SOP.</p> <p>Evidence of risk assessment to be submitted to support any SOP change approval decision.</p> <p>These risks should not be captured within the Risk Management System.</p>
Operational Health, Safety and / or Environment Risk Assessment	Undertaken onsite using tools and documents prescribed by the Safety Management System (SMS) or Environmental	Undertaken onsite using tools and documents prescribed by the Safety Management System (SMS) or Environmental	<p>The SMS and EMS prescribes operational risk assessment requirements.</p> <p>These risks should not be captured within the Risk Management System.</p>

	Management System (EMS)	Management System (EMS)	
Third-Party request to access ARTC infrastructure	Prior to authorisation of third-party access request.	Risk assessment as required by either operational risk assessment requirements (see SMS or EMS) or Property Access Agreements	Risk assessment as required by either operational risk assessment requirements (see SMS or EMS) or Property Access Agreements. These risks should not be captured within the Risk Management System.
Procurement	Prior to authorising significant procurement contracts.	Structured qualitative risk workshop involving appropriate stakeholders.	Output of risk assessment sent to procurement team to provide advice on the most effective way to manage contract risk These risks should not be captured within the Risk Management System.

Figure 3: Types of Assessments within ARTC

3.3.2 Application of Risk Management Activities

The following section provides some practical examples of the application of risk management at ARTC. This content is not exhaustive, and personnel are encouraged to contact the Corporate Risk Team for guidance on how best to apply a risk management process for their specific application.

3.3.2.1. Core Business Delivery, Divisional Planning & Improvement

ARTC faces a series of risks to its core business objectives and strategic priorities which are managed through the actions and decisions on a day-to-day basis.

ARTC’s business risks are documented in the Enterprise Risk Management System as discrete risk statements which describe causes, controls, and consequences of risks. These risks are formally reviewed by the Executive and Board Risk Committee several times each year

Each part of the organisation undertakes annual planning which outline key activities and initiatives to be delivered to achieve ARTC’s strategic priorities.

The Sponsor of an initiative, or process improvement, should ensure that risks are identified during the planning phase, together with appropriate mitigating actions.

These risks need to be documented in the Enterprise Risk Management System.

3.3.2.2. Project Risk Management

Project risk management activities are conducted across a project’s lifecycle to identify and control risks to the successful delivery of project objectives.

Project risks should be documented in a format that is appropriate for the type and complexity of the project. It is recommended that project risks are captured in the Enterprise Risk Management System, but this is not mandated.

Refer to the ARTC Project Management Framework for further information or contact the Corporate Risk Team for guidance.

3.3.2.3. Changes to Infrastructure or Asset Configuration

Changes to existing infrastructure or asset configuration may introduce new risks which need to be controlled prior to 'going live'. This type of risk will typically be managed through the application of the Configuration Control Management (CCM) process. The CCM process is used to identify risks, and determine the standards, equipment and any other actions required to effectively control those risks.

Similarly, risks associated with changes to other assets (e.g., management systems, ICT, etc.) are controlled through dedicated Management of Change systems rather than ARTC's Risk Management System.

Significant or very complex changes to ARTC assets, such as the introduction of major new assets (e.g., bridges, tunnels, signalling systems, etc.) may be subject to a formal risk analysis under a System Safety Assurance process.

These type of risk records do not require documentation in ARTC's Risk Management System.

3.3.2.4. Deviation from Established Standards

Deviating from established design or system standards may introduce risks that will need to be controlled – this includes the introduction of new or novel assets.

Prior to authorising the request to deviate from an ARTC Standard, the person making the request must demonstrate that risks are effectively controlled. This will typically be demonstrated through evidence of a risk assessment performed by appropriate technical stakeholders.

These risks do not need to be captured in ARTC's Risk Management System.

3.3.2.5. Deviating from Standard Operating Procedures (SOP)

Deviating from Standard Operating Procedures (SOP), including Network Rules & Procedures, introduces new risks which need to be controlled, and authorised, at an appropriate level.

The person authorising deviations must be satisfied that the risk controls are adequate.

These risk records do not need to be captured in ARTC's Risk Management System.

3.3.2.6. Operational Health, Safety & Environment Risk Assessments

Field based risk assessments are intended to support established work procedures by demonstrating controls are applied on the ground at the time of work, this may include:

- Worksite Protection Plans (WPP)
- Site Safety & Environmental Management Plans
- High Risk Work Permits (HRWP)
- Safe Work Method Statements (SWMS)
- Task Based Environmental Impact Assessment (TBIA)

The contents of these operational work procedures will be communicated to the workforce during a pre-work briefing and will be subject to control assurance by supervisors and other personnel onsite.

These risks do not need be captured in ARTC's Risk Management System.

3.3.2.7. Third Party Requests

The risks to ARTC include risks associated with third party activities (e.g., collision with rail traffic) and enduring impacts on assets associated with third party works (e.g., under boring of track).

Third Party requests to access, or otherwise impact on ARTC assets, must be reviewed and approved by an authorised person in advance of access being granted.

The ARTC Third Party Manager needs to conduct a risk workshop involving an appropriately diverse range of stakeholder’s reflective of the asset likely to be impacted and ensure that the required risk controls are documented and implemented effectively prior to authorising access.

These risks do not need to be captured in ARTC’s Risk Management System.

3.2.2.8. Procurement

Many procurement activities are routine in nature and the associated risks can be managed under established control mechanisms (e.g., specifications, conditions of contract, etc.).

Significant or complex procurement activities require additional evaluation to ensure that risks to ARTC are effectively managed.

Prior to authorising high-risk procurement contracts, a formal risk assessment needs to be completed.

These risks do not need to be captured in ARTC’s Risk Management System.

4. Bowtie Risk Assessment Format

4.1 Simple Risk Assessment

The simple risk format is a straightforward way to depict risks and to manage controls, causes and consequences within a risk record. This is primarily used when recording risks associated with Business Objectives, or projects.

4.2 Bow Tie Risk Assessment

ARTC also utilises the bowtie risk assessment format to depict risk statements in its Enterprise Risk Management System. The bowtie format depicts the risk event in the centre of the diagram whilst causes and consequences are on the left-hand and right-hand edge respectively. Risk controls sit between causes and the risk event and act to prevent to the risk event occurring, whilst risk mitigants sit between the risk event and the consequence and act to reduce the severity of the outcome.

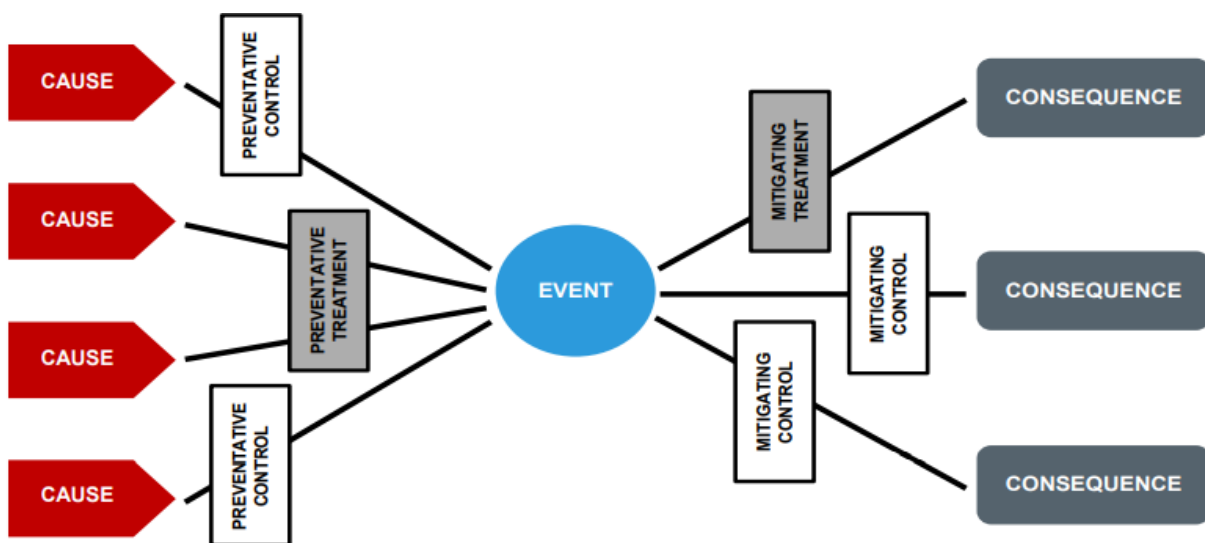


Figure 4: Bowtie Risk Assessment Format

Suggestions for developing a high-quality risk bowtie include the following:

- Clearly describe the risk event
- Risk causes and consequences should clearly articulate a direct relationship with the risk event
- Risk controls and mitigants must act directly on their respective cause or consequence, avoid duplication of controls across multiple causes where possible

It is essential to properly describe the risk event and avoid articulating controls which are not working effectively as a risk. An example of this could be '*asset inspections do not identify major defects*' where the asset inspection activity is a control mechanism over the risk (e.g., derailments caused by major defects).

When assessing the risk rating consider impacts across all SAFERR consequence categories and ideally take a worst credible scenario view (i.e., the most credible consequence as opposed to the worst-case scenario). The risk rating is assessed across inherent, current and target rating perspectives:

- Inherent Risk: Credible rating considered without controls.
- Current Risk: Rating considered with current controls in place, the vector between inherent and current risk rating demonstrates the effectiveness of the risk controls in place and is subject to control assurance testing.
- Target Risk: Estimated rating at a future time after additional controls or mitigants are implemented, or existing controls are enhanced.

Bowtie risk statements that are intended to reflect core business risks within the Enterprise Risk Management System are to be developed to a high quality and are subject to review by the Corporate Risk Team.

5. Appendix

In this section additional information is provided to assist staff with risk management, and to encourage a consistent and comprehensive language and approach to managing risk across the whole of the ARTC.

The information includes:

- Glossary of key risk management terms
- ARTC Risk Management Responsibilities and Accountabilities
- Associated documents

Other tools and resources can be found on the ARTC website under Risk Management.

5.1 Appendix A – Glossary of key risk management terms

Term	Description
Actions	Activities to be undertaken to align risk with the organisational risk appetite.
Cause	A condition or set of conditions leading to a risk. Used in this document to describe the cause contributing to a risk.
Consequence	Outcome of an event affecting ARTC reaching its objectives. A consequence may also be referred to as an impact.
Control	A measure that modifies risk by either preventing the risk or reducing the consequences of the risk.
Current Risk Level	The risk level given the effectiveness of controls currently in place. Also referred to as the residual risk level.
Level of Risk	Inherent Risk Level – the risk level without any controls in place Current Risk Level – the risk level given the effectiveness of controls that are currently in place Target Risk Level – the risk level that is expected to remain after implementation of Actions
Likelihood	The probability of a risk occurring
Objectives	ARTC's Organisational, Business Unit or project deliverables.
Opportunity	An uncertainty that could have a positive effect leading to benefits or rewards.
Review	Activity undertaken to determine the effectiveness of controls in place.
Risk	The chance of something happening that will have either a negative or positive impact. The level of risk reflects the likelihood of the unwanted event and the potential consequences of the unwanted event.
Risk Assessment	The process of identifying, analysing and evaluating risk.
Risk Impact Categories	ARTC's identified organisational areas of risk focus, as captured under ARTC's Risk Appetite;

Risk Identification	The process of finding, recognising and describing risks. Risk identification involves the identification of risk sources, events, their causes, and their potential consequences.
Risk Management	The systematic application of policies, procedures, and practices to better understand risks and reduce risk exposure.
Risk Management Framework	Set of components that provide the foundations for designing, implementing, monitoring, reviewing and continually improving risk management throughout the organisation. The foundations include policy, objectives, mandate and commitment to manage risk.
Risk Register	A record of identified risks relating to the objectives of the organisation, business division or project.
Scope	Clearly defined set of parameters that enable focussed risk assessment.
SFAIRP	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. This need only be applied in the context of safety risks.
Target Risk Level	The risk level expected to remain after implementation of actions.
Significant risk	A risk determined by the Executive as a high-level risk which can adversely affect the achievement of the company's objectives.

5.2 Appendix B – ARTC Risk Management Responsibilities and Accountabilities

Role	Responsibility / Accountability
Chief Executive Officer	Chief Executive Officer is accountable for: <ul style="list-style-type: none"> • Ensuring risks are managed in line with ARTC's Risk Appetite as set by the ARTC Board.
General Counsel & Company Secretary	General Counsel & Company Secretary is accountable for: <ul style="list-style-type: none"> • Ensuring systems and processes are in place for the identification, assessment and management of all risks in accordance with the ARTC Risk Appetite as set by the Board; and • Ensuring systems are in place to meet legislative requirements for the management of risk; and • Periodic reporting to the Executive Committee and Board Risk Committee on the status of risks and risk management practices across ARTC.
Group Executives	Group Executives are responsible for: <ul style="list-style-type: none"> • Ensuring the risks within their area of responsibility are managed in accordance with the ARTC Risk Appetite as set by the Board; and • Ensuring legislative obligations in respect to risk management are met for risks within their area of responsibility; and • Providing updates on risks within their area of responsibility to satisfy reporting requirements to the Executive Committee and Board Risk Committee
General Manager Corporate Risk	General Manager Corporate Risk is responsible for: <ul style="list-style-type: none"> • Developing and implementing systems and processes across ARTC to enable effective management of risks; and • Coordinating risk information for the purpose of reporting to the Executive Committee and Board Risk Committee
Line Management	Line Management are responsible for: <ul style="list-style-type: none"> • Identifying where risk assessment activity may be required to be undertaken, and providing relevant information and input in risk assessments, where requested; and • Ensuring relevant information and training in risk management is provided to employees and other stakeholders (including contractors) within their area of responsibility. Line Management are accountable for: <ul style="list-style-type: none"> • The identification of risks within their area of responsibility; and • Monitoring, reviewing, and updating the progress of Actions and Proposed Treatments of the risks identified within their area of responsibility.
Risk Owners	Risk Owners are accountable for: <ul style="list-style-type: none"> • 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 as set by the Board; and

	<ul style="list-style-type: none"> • Ensuring that periodic reviews of the risks that they own are conducted, including the effectiveness of their existing Controls, in accordance with required timeframes and appropriate records of review and updates are made; and • Reporting information on risks in accordance with escalation requirements and governance arrangements. <p>Risk Owners are responsible for:</p> <ul style="list-style-type: none"> • Ensuring that appropriate Proposed Treatments and Actions are identified and being actioned for the risks that they own.
<p>Risk Manager</p>	<p>Risk Administrators are responsible for:</p> <ul style="list-style-type: none"> • Updating the content of a risk record, as requested by or on behalf of the Risk Owner; and • Monitoring that Actions associated with risks are completed in a timely manner; and • Submitting a risk record for approval to the Risk Owner when transitioning a risk from a 'draft' state; and • Placing a risk under formal review as requested by or on behalf of the Risk Owner; and • Closing out risk records as requested by or on behalf of the Risk Owner.
<p>Control Owner</p>	<p>Control Owners are accountable for:</p> <ul style="list-style-type: none"> • Ensuring effective design, implementation, and ongoing application of a controls they are responsible for; and • Communicating any changes to a control to impacted parties.
<p>Staff at all levels</p>	<p>Workers are responsible for:</p> <ul style="list-style-type: none"> • Identifying and communicating local worksite hazards and their controls to all personnel at that particular worksite, and reporting risks to their line manager; and • Providing relevant information and input in risk assessments, where requested.
<p>Contractor</p>	<p>Where ARTC employees engage contractors, suppliers or consultants they are required to ensure these organisations and individuals are aware of ARTC requirements for risk management and as a minimum, apply these for the work and services they provide for us.</p> <p>Where contractors, suppliers or consultants undertake risk assessments on behalf of ARTC, they are required to be undertaken in accordance with this procedure.</p>

5.3 Appendix C – Associated Documents

Relationship	Associated documents
Parent	<p>The following documents are parent to this procedure:</p> <ul style="list-style-type: none"> • RSK-GP-004 - ARTC Risk Management Framework • COR-PO-006 - ARTC Risk Management Policy • RSK-GP-007 - ARTC Risk Appetite Statement
Subordinate	<p>The following documents are subordinate to this procedure:</p> <ul style="list-style-type: none"> • RSK-GP-003 ARTC Risk Management (SMS process – available via ARTC SMS) • RSK-WI-001 - Application of Risk Management • RSK-WI-005 - Project Risk Management • RSL-FM-005 - Project Risk Management Plan Template
Reference documents	<p>The following documents were referenced in this procedure:</p> <ul style="list-style-type: none"> • ISO 31000:2018 Risk Management – Guidelines • SA/SNZ HB 436:2013 Risk management guidelines – Companion to ISO 31000:2009