



Enterprise Risk Management Procedure

PRC - Procedure

Document No.: 0000-A0-PRC-60029
Security Classification: Unrestricted

Revision	Issue Reason	Prepared By	Endorsed By	Approved By
4	Issued for Use	Melissa Kneale (Enterprise Risk Advisor)	James Cheng (Lead Risk and Assurance)	Ash Blackburn (Manager Enterprise Governance)

TABLE OF CONTENTS

ABOUT THIS PROCEDURE	3
1. BUSINESS PROCESSES.....	4
2. COMMUNICATION AND CONSULTATION	5
3. SCOPE, CONTEXT, AND CRITERIA	6
4. RISK ASSESSMENT: RISK IDENTIFICATION.....	7
5. RISK ASSESSMENT: RISK ANALYSIS.....	9
5.1. Risk Assessment: Risk Analysis – Control Effectiveness	10
6. RISK ASSESSMENT: RISK EVALUATION	12
6.1. Risk Assessment: Risk Evaluation - Overall Risk Control Effectiveness	12
6.2. Risk Assessment: Risk Evaluation - Risk Ratings.....	13
7. RISK TREATMENT.....	16
8. MONITORING AND REVIEW	17
9. RECORDING AND REPORTING.....	18
10. MONITOR, ASSURE AND IMPROVE	21
11. REFERENCE AND COMPLIANCE DOCUMENTS.....	21
12. ABBREVIATIONS AND DEFINITIONS.....	22
13. RECORD OF AMENDMENT	25

LIST OF TABLES

Table 1: Risk Ownership Guidance	8
Table 2: Control Effectiveness Evaluation Guidance.....	11
Table 3: How to determine MFE.....	13
Table 4: How to determine CRR.....	14
Table 5: How to determine TRR.....	15
Table 6: Reference and Compliance Documents.....	21
Table 7: Abbreviations and Definitions	22
Table 8: Record of Amendment	25

LIST OF FIGURES

Figure 1: ISO31000:2018 Risk Management Process.....	4
Figure 2: Risk Window and Risk Exposure Diagram	7
Figure 3: Minimum Risk Recording Criteria (based on CRR).....	18
Figure 4: Minimum Risk Reporting Criteria (based on CRR)	19
Figure 5: Serial Method for Risk Aggregation Example.....	20
Figure 6: Parallel Method for Risk Aggregation Example	20

TABLE OF APPENDICES

No table of contents entries found.

About This Procedure

Purpose

The purpose of this procedure is to define the process for risk management activities performed by entities that INPEX operates or are a joint venture partner.

In Scope

This procedure applies to all Company assets, projects, personnel, and related third-party personnel who are engaged to provide services to INPEX controlled activities in Australia and related project locations. The processes and activities listed within this procedure shall be followed when managing risks across the business. Practical application of this procedure balances efficiency and transparency in decision making, and reporting of risk.

Deviations from this procedure must be approved by the Manager Enterprise Governance. Deviations should be outlined in discipline specific documents that govern and define the process where discipline specific risks are identified, assessed, treated, and reported.

Out of Scope

Discipline specific risk management processes such as those performed by HSE (i.e., HAZOP, HAZID, ENVID assessments) are out of scope for this document.

Intended Users

Intended users of this procedure are risk advisors, risk coordinators or champions, risk owners, control owners, and risk actionees.

1. Business Processes

Overview

Risk management is a continuous process that considers changes in internal and external business environment. Implementing a structured and consistent risk assessment process supports the achievement of defined objectives by guiding prioritisation and response towards risk.

INPEX Australia follows the ISO31000:2018 [Risk Management – Guidelines] risk management process pictured below.

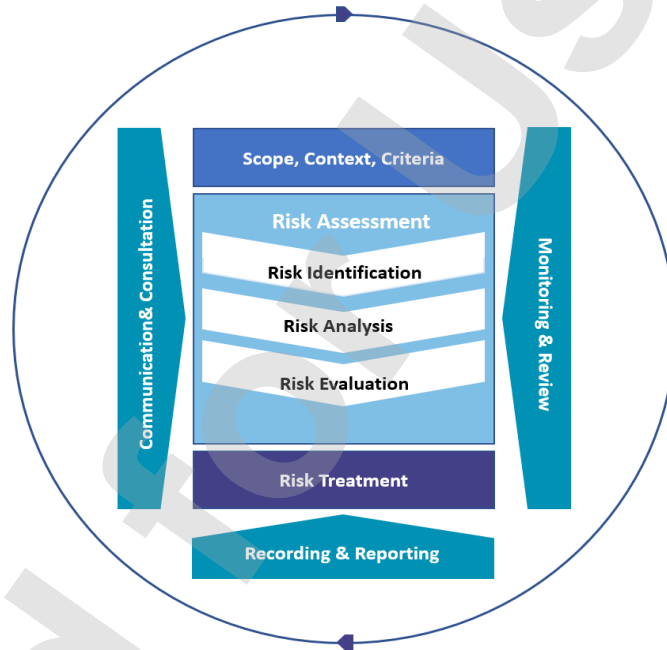


Figure 1: ISO31000:2018 Risk Management Process

Communication and Consultation

The purpose of communication and consultation is to engage and inform relevant stakeholders in understanding risk, the basis on which decisions are made, and the reasons why particular actions are required. Refer to Section 2.

Scope, Context, and Criteria

Establishing the scope, context, and criteria ensures relevance of the risk management process, enabling effective risk assessment and appropriate risk treatment. Refer to Section 3.

Risk Assessment

Risk assessment involves a systematic process to understand the nature and level of risk. It is an overall process of risk identification (Section 4), risk analysis (Section 5), and risk evaluation (Section 6).

Risk Treatment

The purpose of risk treatment is to select and implement options for addressing risk. Refer to Section 7.

Monitoring and Review

The purpose of monitoring and review is to improve the quality of the risk assessment (identification, analysis, and evaluation) to confirm that risks are accurate, current, and appropriately managed. Refer to Section 8.

Recording and Reporting

Recording and reporting outputs of the risk assessment enables communication of risk management activities across the business, and provides information to aid in decision making. Refer to Section 9.

2. Communication and Consultation

Communication

Communication promotes awareness of the risks. At INPEX Australia, communication of risk primarily occurs via designated reporting to senior leadership.

Consultation

Consultation is a strategic process aimed at stakeholder engagement where diverse views and expertise are incorporated to inform decision making. Consultation and engagement with the appropriate stakeholders (risk and control owners) during the risk assessment is likely to result in a more accurate and balanced reflection of the risk and the effectiveness of controls.

Good Practice

To ensure that information is shared across the business, it is important to consult internal and external stakeholders. Good practice would be to involve risk owners, control owners, and any impacted business areas in the review and update of risks.

3. Scope, Context, and Criteria

Scope

The risk assessment scope identifies the limits or boundary of the activity under review to ensure that any inclusions or exclusions are known.

For example: *Identify and assess the operational and financial risks as a result of delayed Phase 2B DP4.*

Context

The risk assessment context is a general prompt to include information which has either led to the requirement for the risk assessment or will have a bearing on the outcomes. Context generally considers both the internal and external factors to effectively frame the business environment.

Internal Context example:

- Company objectives,
- Organisational structure,
- Changes in Joint Venture relationships.

External Context example:

- Governmental changes,
- Political unrest in countries where INPEX conducts business,
- Commodity price fluctuations.

Criteria

Risk criteria provides the means to categorise and evaluate a risk. At INPEX Australia, the risk criteria are defined within the INPEX Australia Risk Matrix [0000-A0-TPL-60003].

Good Practice

When initiating a formal risk review / identification session (often referred to as a risk workshop), it is good practice to develop a Terms of Reference (ToR).

This ToR would outline the risk assessment scope, context, and criteria. It would also identify participants, background information, assumptions, risk techniques to be used in session, timing and deliverables. The ToR would typically be approved by the risk assessment sponsor.

4. Risk Assessment: Risk Identification

Overview

The purpose of risk identification is to recognise, and describe risks that have potential to prevent the Company achieving its objectives. Effective risk identification is about being thorough, collaborative, and context aware. It ensures that all relevant risks are surfaced early, allowing the Company to take action before they materialise.

Risk Title

The risk title is a statement used to clearly describe the risk. It is important to ensure that the risk title is specific enough to be understood by any part of the business if read in isolation.

Risk Description

The risk description is an extension of the risk title. It describes the uncertainty / ambiguity in meeting the objectives and may contain an example for further clarity.

The risk description should provide risk context that supports the identification of causes, consequences and associated controls.

Some elements used to assist in developing a robust risk description include:

- Risk Window, and
- Risk Exposure Period.

The risk window is the period of time that the risk is present for. The risk exposure period is the period of time where the consequences of the risk could eventuate (i.e., the time period that the Company is exposed to the consequences of the risk), as pictured below.



Figure 2: Risk Window and Risk Exposure Diagram

Risk Ownership

Assigning appropriate risk ownership ensures the risk is actively and effectively managed by someone with authority, accountability, responsibility, and knowledge. All risks shall be assigned a risk owner in accordance with the Risk Ownership Guidance Table within the Enterprise Risk Management Standard [0000-A0-STD-60020], as pictured below.

Table 1: Risk Ownership Guidance

CRL	Risk Ownership Level
Critical	1-level down from Managing Director, Country Chair Australia, or 1-level down from Executive VP Operations e.g., Vice President (VP), VP Operations, VP Development
High	2-levels down from Managing Director, Country Chair Australia, or 2-levels down from Executive VP Operations e.g., Deputy VP, General Manager (GM)
Moderate	3-levels down from Managing Director, Country Chair Australia, or 3-levels down from Executive VP Operations e.g., Manager, Package Manager, Site Authority, Production Manager, Operations Support Manager
Low	4-levels down from Managing Director, Country Chair Australia, or 4-levels down from Executive VP Operations e.g., Team Lead

Good Practice

Composition of attendees is important to ensure that stakeholders and subject matter experts (SMEs) are involved in the risk identification process. This will ensure information is relevant and current, that all plausible risks are identified, and that risk ownership is appropriately assigned.

To aid in risk identification, it is good practice to use a risk prompting template or risk categorisation method such as:

- Risk breakdown structure e.g. TECOPS (technical, economic, commercial, organisational, political, sustainability), or
- Work breakdown structure.

Whilst it is good practice to complete the risk identification process directly within the risk management system (RMS), other forms of recording risk identification information can be used and then the data transferred to the RMS in accordance with Section 9. To aid with recording risk identification information outside of the RMS, a Risk Register Template [0000-A0-TPL-60026] has been developed for use.

Factors for consideration regarding risk ownership:

- Risk owner does not equate to control owner.
- The risk owner should be the individual and department that has the primary responsibility to proactively manage the risk either explicitly through their responsibilities, or have been delegated responsibility from senior leadership
- In some scenarios, the risk owner may be the internal subject matter expert, with controls performed and owned by other departments. E.g. Change to, or new government regulation.

5. Risk Assessment: Risk Analysis

Overview

The purpose of risk analysis is to comprehend the nature of risk and its characteristics. Risk analysis involves detailed consideration of causes, consequences, and controls.

Causes

A cause is anything that may lead to the risk occurring. It is important to list all possible causes (controllable and uncontrollable) of a risk.

Consequences

Consequences are a description of the impact / outcome of the risk on the objectives. All credible consequences of the risk should be listed and they should not simply list the consequence categories from the risk matrix.

Controls

Whilst analysing the risk, it is important to consider any control measures including policies, standards, processes, and systems. When performing a risk assessment and identifying controls; controls performed by other departments should be included.

There are two categories of controls:

- Preventative controls – controls that are aimed at preventing the risk from occurring, and
- Mitigating controls – controls that are aimed at minimising the consequences of the risk.

Both preventative and mitigating controls can either be implemented or non-implemented. Implemented controls are those controls that have been put into effect. For example; controls have been developed and signed off, or equipment has been installed and is operating. Non-implemented controls are where the control is yet to be put into effect. For example; approval from management is pending, or equipment is being designed or is yet to be commissioned.

In addition to categorising controls as preventative or mitigating, implemented or non-implemented; controls can also be marked as key. A key control is any control that is thought to have a proportionally greater influence at preventing the causes or reducing the consequences of a risk than any other control. A greater amount of rigour should be applied to the assessment of key controls.

Discipline specific risk approaches may use different control terminology and/or categories of controls. For example:

- Emergent Asset Integrity Risk Management Procedure [X060-A1-PRC-70036] uses the terms; temporary and permanent.
- Psychosocial Hazard Management Procedure [0000-AH-PRC-70006] uses the terms; primary, secondary and tertiary interventions.

Control Ownership

There are two levels of control ownership:

- Control design owner - person with the responsibility and accountability to design, develop and maintain a control, and to assess the control's operating effectiveness, and
- Control implementer - person with the responsibility and accountability to implement a control at a local level.

All controls shall be assigned a control design owner, and may also be assigned a control implementer. Control owners shall be engaged in the risk and control assessment process. If a control owner is not present during the risk assessment, they shall be informed / made aware that they have been nominated as a control owner so that they can actively manage the effectiveness of their controls.

Good Practice

It is good practice to consider the hierarchy of controls when identifying control measures. The hierarchy of control is a system used to manage risks by ranking controls from most to least effective in this order: elimination, substitution, engineering, administrative, personal protective equipment (PPE).

If a control has been developed and signed off, but not yet rolled out then it is good practice to assign an action around the roll-out and communication of the control. This would improve the effectiveness of the control.

It is also good practice to add actions to non-implemented controls. This would ensure that the control gets implemented. Alternatively, a review date could be added to the non-implemented control to prompt the control owner that it needs to be implemented.

If the control owner is unknown at the time of risk analysis, it is recommended to nominate the risk owner in their place, until such time as the control owner is known, and informed of their control ownership.

5.1. Risk Assessment: Risk Analysis – Control Effectiveness

Control Effectiveness

Evaluating the effectiveness of controls provides assurance that the control measures identified are working as expected. Implemented controls can be assessed based on both their design and operating performance; whereas non-implemented controls can only be assessed based on their implementation progress. Once a control status changes from *non-implemented* to *implemented* the control is required to be re-evaluated.

The assessment of control effectiveness is not an evaluation of how well the control prevents the cause or mitigates the consequence of the risk.

Guidance on how to determine the relevant control effectiveness is provided in the table below.

Table 2: Control Effectiveness Evaluation Guidance

CE Rating	Implemented Controls		Non-Implemented Controls
	Design Criteria	Operating Criteria	
Control Effective	- A control design owner is identified, and has accountability linked to performance. - The control's objectives, processes, and performance criteria are documented. The documentation is comprehensive, reviewed, and integrated.	- The control's objective is well understood by the control design owner and implementer. - All elements of the control are effectively implemented and operating as designed. - There have been no control failures or control breaches since the last assessment. - Control performance is tracked and followed up.	Progressing to plan / on track
Some Improvement Required	- A control design owner is identified. - The control's objectives, processes and performance criteria are documented, but the documentation is not comprehensive, reviewed, or integrated. - Control performance is tracked but not adequately followed up.	- Increased understanding of the control's objective is required by the control design owner and implementer. - Some improvements are required for the control to be operating as designed. - There have been isolated control failures or control breaches but no systemic issues since the last assessment.	Control unlikely to be developed and / or delivered when required without additional focus
Significant Improvement Required	- No control design owner is identified. - The control's objectives, processes and performance criteria are not documented. - Control performance is not tracked.	- Significant improvement in understanding of the control's objective is required. - Significant improvements are required for the control to be operating as designed. - There have been systemic issues with the control since the last assessment.	Considerable effort needed to develop and deliver control when required for implementation
Not Assessed	Control has not yet been evaluated.		Control is identified but the details such as control implementer, performance criteria etc. have not been agreed.

Where discipline specific risk approaches use different control terminology and/or categories of controls the appropriate guiding documents should be referred to regarding how to evaluate the control.

Good Practice

Before conducting an evaluation of the control effectiveness, it is good practice to ask the following general questions:

- Which controls are key?
- Who is the control design owner or implementer?
- Is the control implemented or non-implemented?

- Is the control temporary or permanent (this particularly applies to Asset Integrity risks)?
- How do you demonstrate / verify that the control is effective (i.e., what does effectiveness look like for this control)?
- Are there any additional controls that need to be added?
- Are any actions required to improve the effectiveness of the control?
- Are any actions required to implement the non-implemented controls?

6. Risk Assessment: Risk Evaluation

Overview

The purpose of risk evaluation is to support decisions. Risk evaluation involves comparing the results of the risk analysis with the established risk criteria to determine whether additional action is required.

6.1. Risk Assessment: Risk Evaluation - Overall Risk Control Effectiveness

Overall Risk Control Effectiveness

Once individual control effectiveness levels have been determined, an overall assessment shall be performed for the risk. This assessment is called overall risk control effectiveness and considers the accumulated effectiveness of all controls assigned to the risk.

Whilst this assessment considers the effectiveness of all controls, greater consideration is given to key controls, and those on more prevalent causal pathways. For instance, those causes that are more likely to eventuate in the risk occurring need to be better controlled than others. This assessment is not intended to reflect the level of influence the Company has to control the risk. An example is below:

- Risk: New government policies impacting Company's growth aspiration.
- Controls: Lobby via industry body, Meet with regulator, Provide feedback via consultation
- The Company has limited influence on the new policy, however the overall risk control effectiveness should assess the effectiveness of the controls and actions that the Company can implement.

All relevant stakeholders (risk owners, controls owners, and subject matter experts) shall be consulted when rating the overall risk control effectiveness. As this is a subjective rating it is important to record the rating rationale within the risk register to allow for appropriate peer review and clarity for management.

6.2. Risk Assessment: Risk Evaluation - Risk Ratings

Maximum Foreseeable Exposure

The Maximum Foreseeable Exposure (MFE) describes the credible worst-case consequence level assuming control measures are ineffective or, where vulnerable to failure, fail. MFE relies on historical data, empirical evidence, and the insights of subject matter experts.

MFE is a consequence-only evaluation of risk representing the most severe outcomes. Guidance on how to determine MFE is detailed below.

Table 3: How to determine MFE

Requirement	Guidance
Describe the credible worst-case scenario	Describe the most credible scenario assuming control measures are ineffective or, where vulnerable to failure, fail.
Select the credible worst-case consequence level	For <u>each</u> of the relevant consequence categories listed in the consequence table, determine the credible worst-case consequence level based on the consequence criteria. This level assumes control measures are ineffective or, where vulnerable to failure, fail.
Determine the MFE	The MFE is the selected consequence level and is expressed in terms of being a Catastrophic, Major, Significant, Moderate, Minor, or Insignificant level.
Document the rating rationale	Record the scenario used for determining the MFE in the risk register to allow for appropriate peer review and clarity for management.

Current Risk Rating

The Current Risk Rating (CRR) describes the impact and likelihood of the risk occurring considering the effectiveness of current controls. The risk rating does not include future controls and actions to be put in place or performed.

CRR is expressed as the product of consequence and likelihood. Guidance on how to determine CRR is detailed below.

Table 4: How to determine CRR

Requirement	Guidance
Select the current consequence level	For each of the relevant consequence categories listed in the consequence table, determine the current consequence level based on the consequence criteria. This considers the effectiveness of existing controls that address consequence.
Select the current likelihood level	From the likelihood table, determine the likelihood of the consequence criteria occurring. This considers the effectiveness of any existing controls that address likelihood.
Determine the CRR and CRL	Combine the consequence level and likelihood level results to form the CRR. This is described in terms of the matrix coordinates (for example, B4). Extrapolate the results onto the 6 x 6 matrix to determine the coloured band within which this point sits. This is the Current Risk Level (CRL) and is described as Critical , High , Moderate , or Low .
Document the rating rationale	Record the scenario used for determining the CRR and CRL in the risk register to allow for appropriate peer review and clarity for management. Recording the CRR rationale is a mandatory requirement.

Target Risk Rating

The Target Risk Rating (TRR) describes the future state of the risk after treatment. This considers all prescribed controls have been implemented and improvement actions have been delivered including As Low As Reasonably Practical (ALARP) expectations. It defines the point at which the risk is deemed tolerable. Refer to the HSE Hazard and Risk Management Standard [0000-AH-STD-60003] and the ALARP Demonstration Guideline [0000-AH-GLN-60021] for further information on ALARP.

The TRR establishes a realistic expectation for proactive management, with the goal being to lower current risk until target risk is achieved. The risk owner is responsible for accepting and/or determining the appropriate TRR for the risk. Guidance on how to determine TRR is detailed below.

Table 5: How to determine TRR

Requirement	Guidance
Select the target consequence level	For <u>each</u> of the relevant consequence categories listed in the consequence table, determine the future consequence level based on the consequence criteria. Consideration should be given to improved effectiveness of any existing controls, and the addition of new controls.
Select the target likelihood level	From the likelihood table, determine the likelihood of the consequence criteria occurring. This considers improved effectiveness of any existing controls, and the addition of new controls.
Determine the TRR and TRL	Combine the consequence level and likelihood level results to form the TRR. This is described in terms of the matrix coordinates (for example, C5). Extrapolate the results onto the 6 x 6 matrix to determine the coloured band within which this point sits. This is the Target Risk Level (TRL) and is described as Critical , High , Moderate , or Low .
Document the rating rationale	Record the scenario used for determining the TRR and TRL in the risk register to allow for appropriate peer review and clarity for management.

Good Practice

It is good practice to record a rating rationale for all ratings performed on the risk; Overall Risk Control Effectiveness, MFE, CRR, and TRR.

The rationale should provide a clear and logical explanation of why the ratings have been chosen. A rationale may include the following components:

- Description – summarise the risk scenario used to determine the ratings.
- Justification – explain why the selected consequence and likelihood levels were chosen.
- Evidence – support the ratings with data, expert opinions, or examples of similar incidents.

- Management – outline the proposed measures to manage the risk.

Whilst the reported risk rating will be based on the consequence category with the highest rated combination of consequence and likelihood, it is good practice to include a rationale for all relevant consequence categories.

Clarification of the risk exposure window should be considered when performing risk evaluations and documented in the rating rationale where relevant, as this may influence the selection of both consequence and likelihood levels. For example: a risk with a longer exposure period could be considered to have a lower likelihood due to the business having time to implement its risk treatment plan. Note that this is not always the case.

7. Risk Treatment

Overview

The most common response for addressing risk is to prevent the risk from occurring, or to mitigate the consequences of the risk (prevent/mitigate). However, there are other treatment options that can be undertaken including: avoid, transfer/share, or accept.

Prevent / Mitigate

Preventing or mitigating the risk is the most common response strategy. This option aims to reduce either the consequence or the likelihood levels by implementing additional controls or putting action plans in place to strengthen the effectiveness of existing controls.

Control design owners, control implementers, and action owners shall have appropriate authority, accountability, and responsibility to complete control improvement or control implementation tasks within defined timeframes.

The risk window may help to guide prevention or mitigation options, particularly when ALARP guidance is not explicitly provided. For example:

- A short risk window requires immediate action plans, real-time monitoring, and quick resource allocation.
- A medium risk window requires contingency planning and regular reviews.
- A long risk window requires strategic, long-term initiatives and periodic reassessment.

Avoid

Risk avoidance is a response strategy that seeks to treat the risk by avoiding the activity that is likely to generate the risk. For example: if the acquisition of a new asset results in a risk above tolerance, then the response strategy may be to not purchase the asset, eliminating the risk by not partaking in the risky activity.

Transfer / Share

Risk transfer / share is a response strategy that transfers ownership and management of a risk (or certain consequences of a risk) to another party. Contracting and insurance are common forms of risk transfer. It is important to note that some elements of risk may remain after transfer, resulting in a shared risk. For example: a risk transferred through contracting is owned by the Contractor, however the consequences may still impact INPEX Australia.

Accept

Risk acceptance is a response strategy where the activity is undertaken with full knowledge that the risk remains. Risks can be accepted for several reasons including:

- no treatment options being available,
- the CRR being tolerable (and therefore not warranting treatment),
- the CRR being above tolerance but approved by management (with appropriate authority), or
- the cost of treatment being greater than the consequences of the risk.

Where a decision to accept the risk is taken, no further action is required however, the risk shall still be recorded and monitored in the risk register (with the justification for the acceptance decision documented).

8. Monitoring and Review

Risk Monitoring

Continually monitoring identified risks, controls, and the risk environment ensures that the risk response / treatment strategy remains effective and relevant. Risk monitoring shall be integrated into decision making processes to identify any changes in the risk exposure window, or the emergence of new risks.

Risk monitoring involves evaluating the effectiveness of controls, determining whether control improvements are being implemented as planned, and whether risk objectives are being met.

Risk Review

Planned, periodic reviews of risk information ensures that risks are managed appropriately, risk treatments are effective, and changes in internal or external context are considered.

Risk review involves identifying new risks, assessing appropriateness of controls, and refining treatment strategies. Findings from risk reviews can be used to improve future risk assessments and strengthen the Company's risk maturity.

Good Practice

It is good practice to integrate the risk monitoring and review process into business as usual activities such as scheduling regular periodic reviews, and escalating risks where there are changes in risk trends. It is also important to ensure that all relevant stakeholders from across the business are involved in risk monitoring and review activities.

9. Recording and Reporting

Risk Recording

The output of a risk assessment, and any subsequent reviews or updates is recorded in a risk register. The Company risk management system is used to record risks that meet the minimum recording criteria as pictured below.

Severity	Likelihood Level					
	6	5	4	3	2	1
	Catastrophic	Highly Unlikely	Unlikely	Possible	Likely	Highly Likely
A	9	8	7	6	5	4
B	8	7	6	5	4	3
C	7	6	5	4	3	2
D	6	5	4	3	2	1
E	5	4	3	2	1	
F	4	3	2	1		

Figure 3: Minimum Risk Recording Criteria (based on CRR)

Risk Reporting

A Senior Leadership risk forum is held periodically throughout the year with the primary objective to ensure there is appropriate awareness and oversight on key risks across the business, and to support decision making. At these forums, risks meeting the minimum reporting criteria pictured below are reported. Risks that aren't reported at these forums may be reported at other forums as defined in discipline specific risk management plans.

Severity	Likelihood Level					
	6	5	4	3	2	1
	Catastrophic	Significant	Highly Unlikely	Unlikely	Possible	Likely
A	Critical Risk	Critical Risk	Critical Risk	Critical Risk	Critical Risk	Critical Risk
B	Major	Major	Major	Major	Major	Major
C	Significant	Significant	High Risk	High Risk	High Risk	High Risk
D	Moderate	Moderate	Moderate	Moderate	Moderate	Moderate
E	Minor	Minor	Moderate Risk	Moderate Risk	Moderate Risk	Moderate Risk
F	Insignificant	Insignificant	Low Risk	Low Risk	Low Risk	Low Risk

Figure 4: Minimum Risk Reporting Criteria (based on CRR)

Risk Aggregation

Risk aggregation is the process of combining similar risks together to accurately depict the overall impact, understand the total risk exposure to the Company, and allow for the development and implementation of holistic control plans.

Aggregation is primarily used for reporting purposes to ensure that similar risks are escalated to the appropriate level within the Company. It also allows management to focus their time and resources on those areas of the business that will have the largest overall impact.

Aggregation is often described as a parent / child relationship where the parent risk is the combination of the related child risks. Common themed risks across registers should be aggregated for reporting to more accurately depict the total combined consequence of the risks if they were to eventuate.

Good Practice

The relevant risk coordinator or risk advisor should scan their risk register/s to identify any risks with common themes and consider creating a new aggregated risk. It is good practice to do this scan prior to reporting, and make note within both the aggregated (parent) and child risks for transparency.

Rating Aggregated Risks

There are two options for rating an aggregated risk:

- Serial method, or
- Parallel method.

Regardless of the method applied, the rationale for the risk rating shall be recorded within the risk register for transparency.

The serial method is used when the aggregated risk has an overall impact that is represented by the sum of the child risks. For example: *accrued leave liability where a financial impact is the consequence across multiple business areas*. This example would have an overall financial impact to the Company that is the sum of the individual child risks and therefore the serial method should be applied. This is shown diagrammatically below.

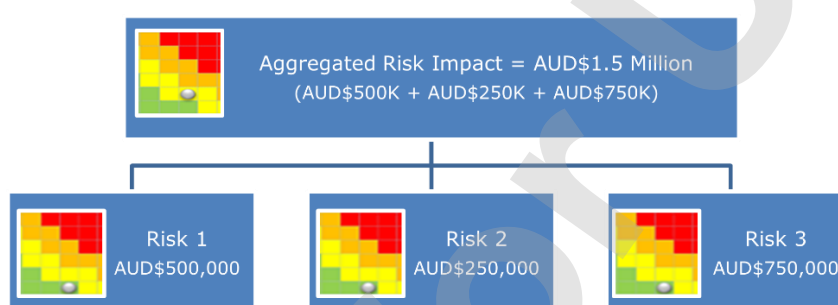


Figure 5: Serial Method for Risk Aggregation Example

The parallel method involves taking the highest rated MFE, CRR, and TRR from the child risks and applying these ratings to the aggregated risk. This method is used when the consequences of the risk are not additive. This is shown diagrammatically below.

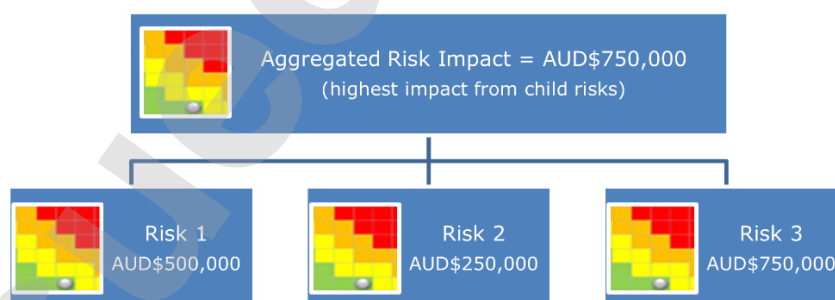


Figure 6: Parallel Method for Risk Aggregation Example

Good Practice

Regardless of the rating method applied, it is good practice for the person completing the rating to use professional judgement and / or consult with subject matter experts (SMEs).

10. Monitor, Assure and Improve

Compliance with this Procedure shall be monitored in accordance with the Company Assurance Standard. Changes made to this Procedure shall be subject to Company management of change processes. Relevant Technical Authority(s) and Subject Matter Expert(s) must be consulted and involved in revisions to this Procedure.

The Owner of this document can be found [here](#).

11. Reference and Compliance Documents

The additional documents listed below are relevant to the execution of this Procedure.

Reference documents (R) are documents referred to in the course of completing this Procedure.

Compliance documents (C) include all standards, regulatory governance, contracts, business rules or policies applicable to this Procedure.

Table 6: Reference and Compliance Documents

Document Name	R	C	Document Number
Policies			
Risk and Assurance Policy		C	0000-A0-POL-60002
Standards			
Enterprise Risk Management Standard	R	C	0000-A0-STD-60020
HSE Hazard and Risk Management Standard	R		0000-AH-STD-60003
Procedures			
Emergent Asset Integrity Risk Management Procedure	R		X060-A1-PRC-70036
Psychosocial Hazard Management Procedure	R		0000-AH-PRC-70006
Other Documents (e.g. External Documents, Specifications, Guidelines, Work Instructions, Forms, Templates)			
INPEX Australia Risk Matrix	R	C	0000-A0-TPL-60003
Application of the INPEX Australia Risk Matrix Guideline	R		0000-A0-GLN-70019
Risk Register Template	R		0000-A0-TPL-60026
ALARP Demonstration Guideline	R		0000-AH-GLN-60021

12. Abbreviations and Definitions

Table 7: Abbreviations and Definitions

Abbreviation / Term	Definition
Action	Description of a task with a defined end date and responsible person assigned.
Actionee / Action Owner	A person with the accountability and responsibility to complete a task within a defined time.
Cause	Anything that may lead to the risk occurring. It is important to list all possible causes (controllable and uncontrollable) of a risk.
Consequence	A description of the impact / outcome of the risk on the Company or Project objectives. All credible consequences of the risk should be listed.
Control	Any process, policy, device, or practice which reduces the level of risk.
Control Effectiveness	Assessment of the design and operation of the control.
Control Design Owner	A person with the responsibility and accountability to design, develop and maintain a control, and to assess the control's operating effectiveness.
Control Implementer	Person with the responsibility and accountability to implement a control at a local level.
Current Risk Rating (CRR) Current Risk Level (CRL)	The amount of risk remaining after considering the effectiveness of current controls. This does not include future controls and actions to be put in place or performed.
Key Control	A control that is thought to have a proportionally greater influence at preventing the causes or reducing the consequences of a risk than any other control.
Likelihood	The chance of the risk occurring.
Maximum Foreseeable Exposure (MFE)	The credible worst case consequence level assuming control measures are ineffective or, where vulnerable to failure, fail.
Mitigating Control	Control designed to reduce the consequence of a risk should it occur.

Abbreviation / Term	Definition
Overall Risk Control Effectiveness	A rating that considers the effectiveness of all individual controls assigned to the risks, with a greater consideration given to key controls or those controls on more prevalent pathways.
Permanent Control	A control that when implemented can reduce the risk from a tolerable and / or ALARP level to the normal (or new normal) operating risk level. The implementation of the permanent control is indefinite in duration, i.e. usually remain in place for life of field.
Preventative Control	Control designed to reduce the causal factors that could lead to a risk occurring.
Rationale	Justification of the quantification of the consequence and likelihood used to determine the risk levels (MFE, CRL, TRL).
Risk	The effect of uncertainty on objectives. NOTE: Risk may have a positive (opportunity) or negative (threat) impact (however, this document focusses on the negative impact).
Risk Aggregation	The process of combining similar risks together to accurately depict the overall impact.
Risk Analysis	Process of identifying causes, consequences, and controls for a risk.
Risk Assessment	The overall process of risk identification, risk analysis and risk evaluation.
Risk Evaluation	Process of calculating the consequence and likelihood to determine the MFE, CRL and TRL.
Risk Exposure Period	The period of time where the consequences of the risk could eventuate. The exposure period starts from the earliest point that the company could be exposed to the consequences of the risk and ends either when the activity has been completed or where the risk has eventuated, when the consequences have been fully realised.
Risk Identification	Process of recognising, documenting, and describing risks.
Risk Management	The overall process of establishing the context, risk assessment, communication, and consultation, monitoring and review, and risk treatment.

Abbreviation / Term	Definition
Risk Matrix	Tool that defines the likelihood and consequence categories and criteria used during risk evaluation.
Risk Owner	A person with the responsibility and accountability to manage a risk.
Risk Register	Documented output of risk management activities.
Risk Review	Providing visibility of risk information to management for them to review the appropriateness of the information.
Risk Window	The period of time that the risk is present for. The period starts when the risk is identified (should have been identified) and ends either when the activity has been completed or where the risk has eventuated, when the consequences have been fully realised.
Target Risk Rating (TRR) Target Risk Level (TRL)	The future amount of risk remaining after actions to improve control effectiveness levels or additional control measures have been put in place.
Temporary Control	A control that when implemented can temporarily reduce the risk from an abnormal level to a tolerable and / or ALARP level, but not yet at the normal operating risk level. The implementation of the temporary control is usually finite in duration.

13. Record of Amendment

Table 8: Record of Amendment

Revision	Section	Amendment
4	All	Alignment with revised BMS Document Template with easy to read styling.
4	All	Simplified risk management suite of documentation by combining the following documents: - Risk Management Procedure - Risk Reporting Procedure - Risk Management Guideline - Risk Aggregation Guideline - Control Monitoring Guideline
4	All	Aligned to new risk management system capability
4	5	Renaming Critical Control to Key Control throughout

NOTICE

All information contained within this document has been classified by INPEX as **Unrestricted** and must only be used in accordance with that classification. Any use contrary to this document's classification may expose the recipient and subsequent user(s) to legal action. If you are unsure of restrictions on use imposed by the classification of this document you must refer to 0000-A9-STD-60008, Sensitive Information Protection Standard or seek clarification from INPEX.

Uncontrolled when printed.

Document Endorsement and Approvals

This page has been automatically generated and appended to this document by the INPEX Australia Controlled Document Management System (CDS). This page contains key events related to this document that are listed in the tables below and the information is unable to be manually edited.

Document Identification

Document Number	Revision	Security Classification	Date
0000-A0-PRC-60029	4	Unrestricted	14/10/25 08:00

Document Revision History

Revision	Date and Time	Issue Reason
3A	29/07/25 08:00	For Review

Delegation of Authority

From Name	To Name	Date and Time	Action

Name	Title

Electronic Endorsement and Approval

Electronic approval of this document complies with the issued INPEX Electronic Approval Standard (0000-A9-STD-60011) and records evidence that the applicable person has either endorsed and/or approved the content contained within this document. The reviewers of this document are recorded in the CDS.

Name	Title	Date and Time	Action
James Cheng	Lead Risk & Assurance	14/10/25 09:16	Endorser
Ash Blackburn	Quality, Risk & Assurance	14/10/25 12:12	Approver