Government of **Western Australia**
Department of **Mines, Industry Regulation and Safety**

Petroleum safety and major hazard facility – guide

Risk assessment and management including operational risk assessment

February 2020

Disclaimer

The information contained in this publication is provided in good faith and believed to be reliable and accurate at the time of publication. However, the information is provided on the basis that the reader will be solely responsible for assessing the information and its veracity and usefulness.

The State shall in no way be liable, in negligence or howsoever, for any loss sustained or incurred by anyone relying on the information, even if such information is or turns out to be wrong, incomplete, out-of-date or misleading.

In this disclaimer:

State means the State of Western Australia and includes every Minister, agent, agency, department, statutory body corporate and instrumentality thereof and each employee or agent of any of them.

Information includes information, data, representations, advice, statements and opinions, expressly or implied set out in this publication.

Loss includes loss, damage, liability, cost, expense, illness and injury (including death).

Creative commons

Contact

This publication can be available on request in other formats for people with special needs.

Further details of safety publications can be obtained by contacting:

Safety Regulation Group – Regulatory Support

Department of Mines, Industry Regulation and Safety

100 Plain Street

EAST PERTH WA 6004

Telephone: +61 8 9358 8001

NRS: 13 36 77

Email: SafetyComms@dmirs.wa.gov.au

Guides

A guide is an explanatory document that provides more information on the requirements of legislation, details good practice and may explain means of compliance with standards prescribed in the legislation. The government, unions or employer groups may issue guidance material.

Compliance with guides is not mandatory. However, guides could have legal standing if it were demonstrated that the guide is the industry norm.

This Guide has an operations focus and is set out in the context of risk assessment and legislative requirements of all responsible persons. Consequently, each operation needs to understand its limitations and skills base.

The Guide is based on current experience and is not claimed to be complete.

Who should use this Guide?

You should use this Guide if you are responsible for hazard identification and risk assessment and ongoing risk management.

Contents

1 Introduction

This document has been developed to provide assistance and guidance to licensees and operators to meet the Western Australian Petroleum safety and major hazard facility legislation administered by the Department of Mines, Industry Regulation and Safety (the Department).

The legislation covered by this Guide is listed in Appendix 1.

1.1 Scope and objective of this Guide

This Guide has been developed to assist licensees and operators to meet their obligations for effective risk assessment and management, including operational risk assessments

For the purpose of this Guide, the term “safety case” is used to cover all of the safety documents referred to in the respective regulations.

The term “facility” covers offshore and onshore facilities and pipelines, including above ground structures associated with onshore pipelines and major hazard facilities.

The Dangerous Goods Safety (Major Hazard Facility) Regulations 2007 use the term “major incident”, whereas petroleum legislation refers to “major accident events” (MAEs). This Guide uses MAE to encompass “major incident”.

The use of “as low as reasonably practicable” (ALARP) throughout this document also covers the major hazard facility term “so far as reasonably practicable” (SFARP) in this Guide.

The Dangerous Goods (Major Hazard Facility) Regulations 2007 refer to “harm to people, property and the environment” (which includes the general public), whereas petroleum legislation refers to “occupational safety and health of all people”. Where specific reference is made to both the petroleum safety and major hazard facility regulations, both descriptions will be included; otherwise, for generic references, the term “safety and health” will encompass the additional requirements of property and environment in this Guide.

The objective is to provide clarity to both industry and Department personnel on areas of the legislation which may be ambiguous or open to interpretation.

The following appendices are included:

Appendix 1 Legislative provisions

Appendix 2 References and acknowledgements

Appendix 3 Glossary of terms

Appendix 4 Further information

1.2 Definitions and abbreviations

Definitions and abbreviations are included in Appendix 3 Glossary of terms.

1.3 Use of standards and approved codes of practice

There are a number of standards and approved codes of practice that can provide guidance and assistance to licensees and operators for completion of their risk assessments and then ongoing risk management. Examples are:

- AS ISO 31000 *Risk Management – Guidelines*
- IEC ISO 31010 *Risk management – Risk assessment techniques*
- ISO 17776 *Petroleum and natural gas industries – Offshore production installations – Major accident hazard management during design of new installations*
- AS/NZS 2885.6 *Pipelines – Gas and liquid petroleum – Part 6: Pipeline safety management*
- AS IEC 61882 *Hazard and operability studies (HAZOP studies) – Application guide*

- AS IEC 61511 *Functional safety – Safety instrumented systems for the process industry sector*
- CCPS *Guideline for initiating events and independent protection layers in layer of protection analysis*.

Approved codes of practice for dangerous goods – information is located on the Department website.

Licensees and operators should reference the current versions of these publications to support the safety management system (SMS) and formal safety assessment requirements of the safety case and how risk assessments and risk management needs to be conducted effectively within their organisations.

1.4 Aims and outcomes of risk assessment

Risk assessment creates knowledge, awareness and preparedness within an organisation. Knowledge of hazards and their implications is necessary to prevent and deal with dangerous occurrences.

The main aims and outcomes of risk assessment are to:

- provide the licensee or operator and the members of the workforce with sufficient knowledge, awareness and understanding of the risks from safety and health hazards and, in particular, the risks from major accident events (MAEs) to be able to manage the facility safely
- provide the licensee or operator and the members of the workforce with sufficient knowledge, awareness and understanding of risks from dangerous goods hazards which may cause harm to people, property and environment and, in particular, the risks from major incidents, to be able to manage the facility safely
- provide a basis for identifying, evaluating, defining and justifying the selection, or rejection, of control measures for eliminating or reducing risk and to lay the foundations for demonstrating that the risks have been reduced to a level that is as low as reasonably practicable (ALARP)
- provide the specific information required by the legislation administered by the Department.

Risk assessments carried out at a time when they can affect decisions of significance for the risk level are key for designing and operating a facility safely. The systematic development, implementation, use and follow up of risk assessment is an important contribution towards managing risk through all stages of a facility's life cycle.

A *detailed risk assessment* for the facility should cover:

- all potential MAEs and all aspects of risk to people, property and environment for each identified potential MAE (consequence and likelihood)
- all risks associated with emergencies
- all risks associated with fires and explosions
- all aspects of the facility design, construction, installation, maintenance and modification
- the whole life cycle of a facility, or an explicitly defined period.

A *continual risk assessment* is carried out on a regular and ongoing basis as a result of:

- problems reported by the workforce
- lessons learned from accident or near miss reports, both localised and external
- any significant changes or improvements that need to be made
- changes in technology or other factors that mean better, more effective risk controls are available, revealing that the current risk management approach for an MAE is no longer ALARP.

1.4.1 Risk assessment for dangerous goods

A dangerous goods risk assessment is required to be conducted and documented by the licensee of a proposed dangerous goods site in order to obtain a dangerous goods licence. This licence precedes the site being classified by the Chief Officer as a major hazard facility.

Licensees and operators associated with dangerous goods sites and major hazard facilities should reference the published guide *Risk assessment for dangerous goods* to assist with this requirement.

1.5 Linked guides

The following guides have been developed to provide information to assist licensees and operators with risk assessment, risk management and the development of the formal safety assessment of the safety case:

- *Hazard identification*
- *Major accident events, control measures and performance standards*
- *ALARP demonstration*

These three guides, together with this document, provide information for effective hazard identification, risk assessment and management, including identification of MAEs and control measures.

Figure 1 gives an example of the overall formal safety assessment process which may be used by licensees and operators to identify and manage the hazards and risks within their organisations and meet the requirements of the relevant regulations.

Formal safety assessment process

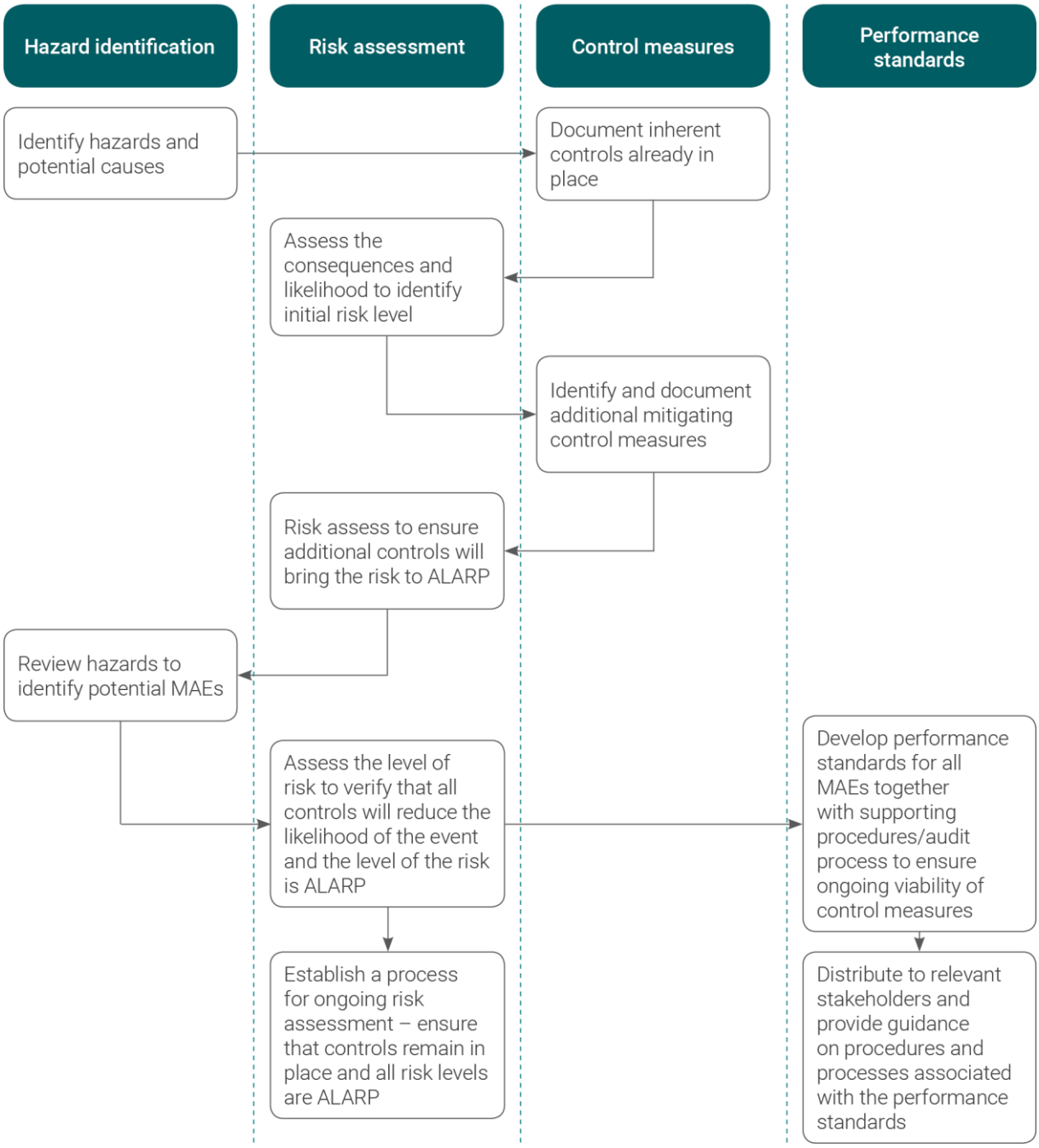

Figure 1 Formal safety assessment process

2 Risk assessment

Risk assessment is the key element of a formal safety assessment.

While licensees and operators and their workforce perform task focussed safety assessments, such as job safety analysis (JSA) or job hazard analysis (JHA), as part of normal routine and non-routine activities, the formal safety assessment is a defined exercise to assess risk across the entire facility undertaken by the licensee or operator and members of the workforce.

Assessing risks is not the same as managing risk. Management of risks is covered in more detail in Section 6 of this Guide. A risk assessment is aimed at informing and improving the licensee's or operator's knowledge and understanding of the nature of risks on the facility, and what might be needed to eliminate or minimise those risks and reduce them to ALARP.

Figure 1 shows how the process of hazard identification, risk assessment, identification of MAEs, identified control measures, ALARP and ongoing risk management may be achieved.

2.1 Risk assessment techniques

The risk assessment process takes into account:

- the objective of the risk assessment
- the anticipated level of risk
- the detail needed in the assessment results.

Licensees and operators should ensure that they have an overall understanding of the risks of their operation and the activities conducted on the facility.

For licensees and operators to acquire the required level of information and to understand the risks impact their facility and manage them accordingly, the risk assessment technique is critical.

Some common risk assessment techniques and the key points of each approach are listed in Table 1.

Table 1 Risk analysis techniques

Technique	Risk assessment method	Key aspects of risk analysis technique
Qualitative	Risk matrix method	• likelihood and consequences expressed on a scale described in words • risk output is not expressed as a numerical value • emphasis is placed on relative grouping of hazards (e.g. into negligible, tolerable and intolerable) or on rough ranking of hazards from highest to lowest • risk assessment workshop participants estimate the site/facility specific risk resulting in greater ownership of the risk results • based on subjective judgement so a higher potential for uncertainty • difficult to calculate cumulative risk • often used as a preliminary risk assessment or screening tool • often used for operation or task based risk assessments • suitable for simple facilities or where the exposure of the workforce is low • can take into account intangible issues such as impact on the public and company reputation

Technique	Risk assessment method	Key aspects of risk analysis technique
Semi quantitative	Risk matrix method LOPA	• generates a numerical risk value (although this value is not an absolute value of risk) • provides greater capacity to discriminate between hazards on the basis of risk • better for assessing cumulative risk although still coarse and difficult for large facilities • some methods provide a more structured technique for understanding the effectiveness of controls
Quantitative	QRA Fault tree Event tree LOPA	• based on calculated estimates of consequence (usually software modelling) and likelihood (estimates based on failure rate data – site or industry) • provides a calculated value of risk • better suited to more complex decision-making or where risks are relatively high • some quantitative techniques (e.g. fault and event trees) can provide a more detailed knowledge of the causal chain and the influence of controls • more rigorous, detailed and objective than other methods and can better assist choice between different control options • more time intensive and expensive than other methods • QRA can provide risk levels if necessary for demonstrating exposure and effect, does not necessarily provide a full understanding of the impact of controls

2.2 Input information for risk assessment

The key information for a risk assessment workshop is the results of the hazard identification. However, the input used for the hazard identification process should be available during the risk assessment for reference purposes and any clarification of the activities taking place on the facility, including:

- site drawings including process flows, layouts, pipeline and instrumentation diagrams (P&IDs)
- detailed description of the equipment to be installed on the facility and its mode of operation. Any new equipment (that is, not previously installed on similar facilities) should be clearly identified as this may require additional analysis
- any previously documented workshops on the facility under review or similar facilities which may be relevant to the scheduled study
- details of hazards associated with chemicals used, stored or produced in a process on the facility
- details of any incidents or accidents reported either on the facility under review or similar facilities.

If there have already been multiple risk assessments conducted for the facility currently under review (e.g. hazard and operability study (HAZOP), safety management study as required by AS 2885.6, safety integrity level), then the results of these risk assessments may need to be taken into account to give overall depth to the risk assessment.

All of these risk assessments form part of the formal safety assessment, identification of MAEs and the relevant control measures and safety critical elements which need to be documented within a safety case.

2.3 Risk assessment team

The knowledge and competency of workshop participants is critical to the successful outcome of any risk assessment process.

The following should be considered when selecting participants:

- the overall scope of the proposed process and the activities to be conducted during the phase of facility under review; e.g. design, construction, operational or decommissioning
- which subject matter experts are required to attend the workshop; e.g. leadership, engineering, design, operational and, if relevant, decommissioning
- include personnel with a thorough knowledge of the facility, or similar facilities if appropriate, and its history
- which areas of the general workforce need to attend, taking into account any interactive areas within the facility, shift rosters, simultaneous operations (SIMOPs) and third party impacts.

Consider appointing a workshop facilitator to guide participants through the risk assessment process. A facilitator should have the appropriate level of independence, expertise and knowledge of the technique adopted for the risk assessment process and any relevant standards or codes of practice applicable.

2.4 Workforce involvement in risk assessment

Workforce involvement should be integral to the risk assessment process.

In the event that a proposed risk assessment process relates to a new facility where the workforce has not yet been fully identified and put in place, involving members of the workforce from a similar facility should be considered.

Licensees and operators should ensure that contributions from the workforce are considered on the basis of technical and working knowledge and not on the seniority of the contributor. Ensure workshops are not dominated by individual persons or groups within the organisation.

Those members of the workforce invited to attend the risk assessment process should be involved in:

- development of the risk assessment process
- forming the team and workshop scheduling
- relevant workshops conducted
- reviewing the workshop results
- implementation of any actions arising from the process
- assisting in provision of feedback of the workshop outcomes to the rest of the workforce.

Refer to the *Involvement of members of the workforce* guide for further details.

3 Risk assessment process

The risk assessment process is covered in detail by the standards listed in Section 1.3 of this Guide.

All risk assessments need to consider the likelihood and consequences of each potential MAE and all other risks not assessed as very low or negligible.

To ensure consistency of results across a risk assessment, it is essential assumptions are documented and recorded at the outset or when identified in the risk assessment process. This should include the threshold or category definitions and the risk acceptability criteria of the organisation.

Where a risk matrix is a key tool for the risk assessment, the same format of matrix should be used throughout the process. For example, in some standards, the risk matrix is in a 5 x 5 format. If a corporate risk matrix is brought into use which has been developed in a different format, the results of the assessment of risk level may vary due to inconsistency in the risk matrix format.

3.1 Likelihood analysis and estimation

The likelihood of an event occurring needs to be estimated during the risk assessment. When using a qualitative risk assessment process this is often based on the selection of a category on a risk matrix. Workshop participants will often base the selection on their experience and justify their decision using historical accident event data.

For a more complex quantitative risk assessment process, the frequency may be selected using a failure database and historical event data, details of which should be documented within the risk assessment. Event tree analysis may be used to determine the likely probability of escalating events such as fires and explosions following an initial event.

Guidance material for likelihood estimation should be documented to ensure consistency across multiple risk assessments. For a risk matrix, it is suggested that likelihood categories are assigned to quantitative frequencies (for example at least once a year, 1:10 years, 1:100 years) to allow for correlation with accident event history and failure databases. Estimation of likelihood for very low frequency events can be difficult and unreliable.

The following options may be used to facilitate the estimation of the likelihood of occurrence for extremely low frequency events:

- referring to the frequencies in terms of experience on the facility, within other areas of the organisation, within the industry locally and internationally
- referring to industry guidance material or failure frequency databases
- use of fault trees to analyse the combination of contributing factors that may lead to a hazardous event.

Likelihood should be determined on the basis of the hazard, not the reliability of the controls that are in place. Otherwise, the likelihood may be determined to be low based on an assumption that the control is reliable when, in fact, it may not be.

All assumptions made and references used during the determination of likelihood estimation should be fully documented. This provides evidence of a robust analysis and can be beneficial for future risk assessments and reviews.

3.2 Consequence analysis and estimation

Consequence analysis should be conducted to a level sufficient for the estimation of risk and appropriate for the facility under review.

When conducting a risk assessment on identified hazards, evaluate the consequences of an event resulting from the hazard. This should be performed for all identified hazards, especially those hazards identified as having the potential to result in a MAE.

The assessment should evaluate the consequences of each MAE in terms of severity and magnitude.

Severity and magnitude for a MAE are defined as:

- the severity of an MAE in the context of regulatory requirements is an event connected with a facility, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility
- the magnitude of the MAE is the size or scale of the effect created by the MAE within which a number of fatalities could occur.

Possible outcomes need to include consideration of what may go wrong if measures to eliminate or prevent accident events are not present, are wrongly implemented or fail to function as intended.

The possibility of the event intensifying or accelerating, or of one event triggering another, should be taken into account when considering the most likely events as this may affect the adequacy of control measures in place. This is important when assessing the adequacy of emergency management.

Document the results from the consequence analysis and make them available for use to improve the licensee or operator's decision-making. Results from the consequence analysis could be used to influence aspects of design, as well as operational procedures and controls, and in defining emergency response arrangements

Estimates of consequence may be either qualitative or quantitative.

For qualitative risk evaluation, consequence needs to be defined, such as 'lost time injury', 'single fatality' or 'multiple fatalities'.

Quantitative estimates of consequence can be produced through consequence modelling. Ensure this type of modelling is performed by personnel with adequate training and experience. Examples of consequences that can be modelled include:

- pool fires
- jet fires
- confined and partially confined explosions
- flash fires
- toxic release and effects
- gas dispersion (flammable or toxic)
- dropped objects
- collision impact
- loss of structural stability
- loss of containment resulting in fire and/or explosion
- process explosion
- search and rescue
- over pressure
- occupied building studies (e.g. control rooms).

The results of consequence modelling may be used in conjunction with qualitative or semi-quantitative risk analysis to justify the consequence of categories selected.

3.3 Control measure assessment

Control measures eliminate, prevent, reduce or mitigate the hazards, their consequences and reduce the risk associated with hazardous events.

When applying control measures to hazards, it is critical that the root cause of that hazard has been clearly identified to ensure that the correct controls are put in place.

While some control measures may be recorded as already being in place during the hazard identification process, the risk assessment aims to identify any new mitigating control measures that will reduce the level of risk.

When determining causes, likelihood and consequences, record existing and potential new control measures. It is essential to define what control measures are included and how they are considered to influence the risk. Other controls that have been considered but rejected, may be documented with the reason why they were not implemented.

During the risk assessment process it is important to consider the reliability of the control and how effective it might be in specific situations. The process should provide the following details in relation to control measures:

- identification or clarification of existing and potential control measure options
- evaluation of control measure influence on risk
- a basis for selection or rejection of control measures
- information for setting performance standards for control measures.

All of these factors will feed into a licensee's or operator's demonstration that the risks have been reduced to a level that is ALARP.

The following should be considered when setting control measure performance standards:

- control measures associated with high risk hazards or MAEs require rigorous performance standards
- the reliability or number of control measures should reflect the risk of the corresponding MAEs or other hazardous events.

The risk assessment process should provide licensees and operators with an understanding of which controls have the most influence on reducing risk and need to be assessed in greater detail.

Licensees and operators should provide a description of the methodologies employed and the summary of the results, such as a list of the MAEs and the associated controls, in the formal safety assessment area of the safety case. The controls applied would generally be described in the facility description section for hardware-related controls or the SMS description section of the safety case for management system or procedure-related controls.

3.3.1 Evidence that risks are reduced to ALARP

The control measures for a MAE should be shown to collectively eliminate or reduce the risk to a level that is ALARP. This information and justification should be described in detail in the formal safety assessment area of the safety case.

The SMS should describe the system arrangements for hazard identification and risk assessment processes (such as policies and procedures) as evidence that brings risk reduction to a level that is ALARP in the safety case.

Refer to the *ALARP demonstration* guide for further details.

3.4 Risk assessment outputs

Upon completion of the risk assessment process, the information available for input into the formal safety assessment and the SMS of the safety case should include:

- an understanding of the factors that influence risk and the controls that are critical to reducing risk. In particular, the risk controls required to ensure adequacy of the design construction, installation, maintenance or modification of the facility for the relevant stage or stages in the life of the facility for which the safety case has been developed
- the likelihood of potential MAEs and other hazardous events with potential to affect the safety and health of people at or near the facility
- the magnitude and severity of the range of possible consequences arising from identified hazards that could lead to MAEs
- the magnitude and severity of the consequences arising from other hazardous events with potential to affect safety and health of people at or near the facility, including the nature of injury or occupational illness
- clear linkages between hazards, the associated consequences, likelihood and risk and the associated control measures.

Licensees and operators should provide some examples of the risk assessment process for specific MAEs that will assist those reading the safety case to understand the process taken and any linkages that are present.

3.5 Use of risk assessment outcomes

Risk assessment outcomes can be used:

- as an input to engineering design to ensure the appropriate level of performance is incorporated into engineered barriers, particularly at front end engineering and detailed design stages
- to ensure that the workforce understands the hazards and risks associated with the facility, the control measures in place to manage these risks and their role in the prevention of MAEs and other hazardous events
- to provide evidence that risks are reduced to a level that is ALARP
- to assist in the development of emergency response plans
- to enable priorities and resource allocations to be based on appropriate information and assessment, resulting in a cost effective improvement of risk
- to assist in the improvement of procedures and management systems
- as an input into training needs analyses
- to assist with other processes such as management of change and accident and dangerous occurrence investigation.

4 Success factors for risk assessment

Some of the factors critical to the success of the risk assessment include:

- a full understanding of the consequence and likelihood of all potential MAEs
- uncertainties are explicitly identified
- all methods, results assumptions and data are fully documented
- control measures and their effects on risk are explicitly addressed
- risk assessment outcomes are used as a basis for adoption of control measures, including improvements to the safety management system and emergency planning
- the safety philosophy adopted by the organisation should be relevant to the facility
- information is provided to persons who require it in order to work safely
- an appropriate number of members of the workforce have been actively involved in the risk assessment process and consultation with others has occurred
- the risk assessment report is quality assured to verify the accuracy of the results and that the report has been reviewed by the workshop participants
- the risk assessment is regularly maintained and reviewed, and used as a live document which is communicated to the appropriate stakeholders as and when required.

5 Potential weaknesses in risk assessment

If a risk assessment process is not conducted with care and understanding, the outcomes may be incorrect and lead to poor decision-making. Examples of this are:

- conducting a risk assessment to attempt to justify a decision already made
- using a generic assessment when a site specific assessment is needed
- only considering the risk from one activity
- not involving a team of people in the assessment, or not including members of the workforce with practical knowledge of the process or activity being assessed
- ineffective use of consultants as subject matter experts or as workshop facilitators
- failure to identify all hazards associated with a particular activity
- failure to consider all possible outcomes
- inappropriate use of data
- inappropriate definition of a representative sample of events
- no consideration of ALARP or further measures that could have been taken
- inappropriate use of cost benefit analysis
- using ‘reverse ALARP’ arguments (i.e. using cost benefit analysis to attempt to argue that it is acceptable to reduce existing safety standards)
- not using the results of the assessment
- not linking hazards to risk controls
- substituting a task risk assessment (such as a JHA or JSA) in place of a risk assessment.

6 Ongoing risk management

Completion of the initial risk assessment is only the first step in risk management. All risk assessment reports should be treated as live documents that are subject to ongoing review and update.

Figure 2 depicts the process to ensure continual review and revision of risk assessments.

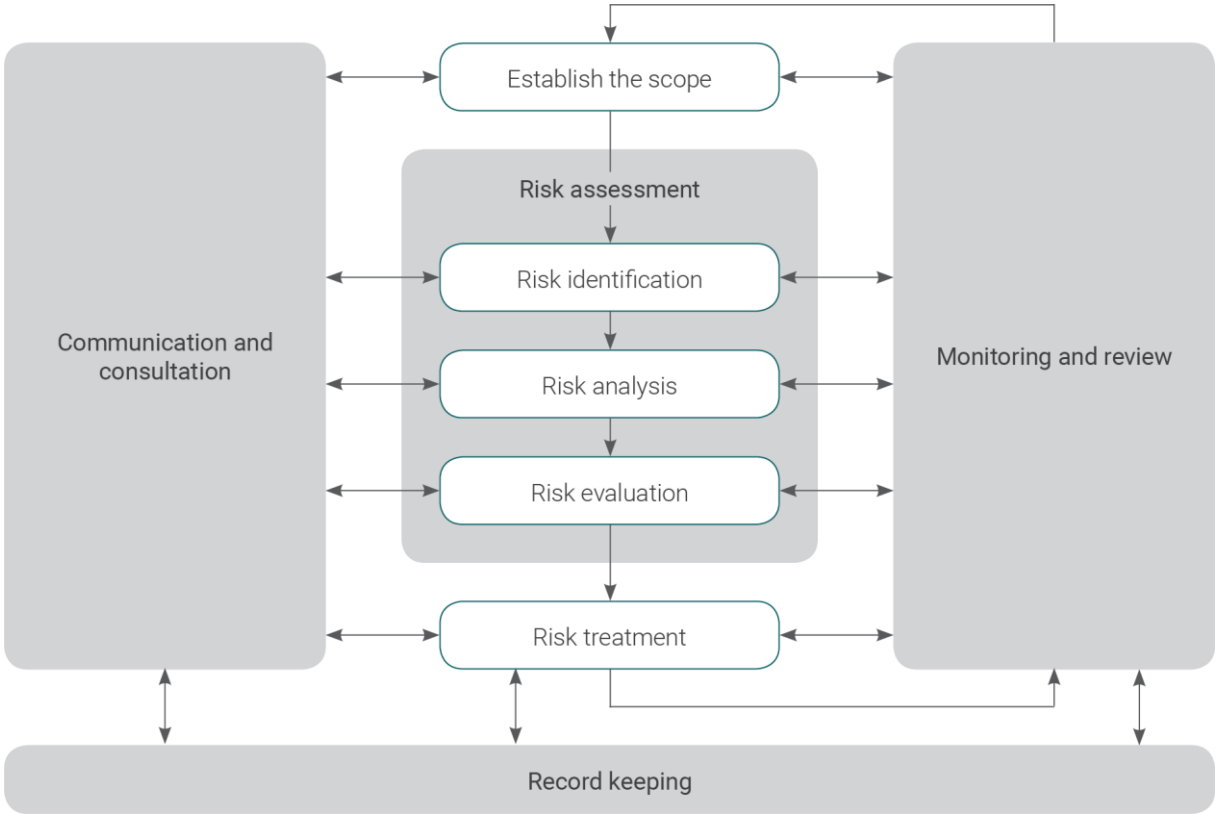

Figure 2 Risk management process

6.1 Review and revision of risk assessments

Licensees and operators should ensure a process is in place where risk assessments are reviewed and updated at regular intervals to check the controls in place are still appropriate. There is an ongoing responsibility to understand and reduce the risks to a level that is ALARP, including risks associated with proposed changes to the facility.

Some possible triggers for risk assessment review are:

- further information emerges that can help to refine the risk assessment. This particularly applies to areas of uncertainty in the previous risk assessment
- an accident or near miss investigation identifies further hazards or indicates the risk may be higher than previously thought. Safety alerts from other facilities and operators should be reviewed for their relevance in this respect
- the audit and review process of performance standards identifies areas of non-compliance and possible impairment of safety critical elements
- changes have occurred to plant or equipment in terms of hardware or software
- changes in the workforce could lead to changes in work practices or in knowledge of the facility and potentially alter the level of risk and additional control measures may be necessary
- new hazards are identified
- industry developments have occurred with respect to technology or systems of work that may be applied to reduce risk.

7 Operational risk assessments (ORA)

All licensees and operators should have in place processes and procedures to provide an effective and systematic approach to operational risk assessment (ORA). This includes a protocol for regular periodic reviews of operational risks, and for short-term operational risk assessments arising from any impaired safety critical elements identified, or other management of change requirements on facilities.

The procedures should give clear guidance to personnel on the appropriate application of the ORA and should reinforce that facility management is obliged and empowered to take immediate shut down action where, in their judgement, the increase in risk arising from safety critical element impairment is not adequately provided for in the safety case.

When plant has been shut down, the ORA will assess the risk of restarting the affected plant or equipment and support a decision to continue operations with a known impaired safety critical element where the assessment outcome shows that mitigations can be implemented to maintain the risks to ALARP.

7.1 Organisational requirements for ORA

When developing their procedures and processes for ORA, organisations need to ensure that they are adequately and appropriately resourced and use competent personnel.

7.1.1 Adequate resources, roles and responsibilities

Technical authorities, engineers responsible for safety critical elements and other support personnel (including relevant members of the workforce) should be involved in the ORA process. The procedure should document any constraints to participation, and how this will be managed for conducting, reviewing and approving an ORA.

The procedure should clearly identify the roles and responsibilities in the management and control of the ORA and detail the level of involvement in the process in line with the risk being assessed. Roles and responsibilities may be shown in table format, or by using a responsible, accountable, consulted and informed (RACI) chart. This should align and describe the levels of authority and at what point an ORA is approved by relevant managers.

7.1.2 Training and competence

Adequate training is essential for all personnel involved in an ORA. For an effective approach to an ORA with links to MAE hazards, personnel should possess or attain the necessary knowledge and skills as follows:

- a thorough understanding of MAE hazards specific to the facility
- the related safety critical elements, their interaction, verification and performance standards
- awareness and understanding of key information contained within the facility safety case, main plant isolatable inventories, incident escalation pathways and prevention, control and mitigation barriers
- process safety and integrity management principles, engineering standards and specifications
- understanding of operational status and plant conditions
- understanding of any safety critical elements impairment procedures already in place
- understanding of site specific emergency response plans and procedures.

7.2 Planning and implementation

To be effective, an ORA process should have in place:

- identification of the circumstances in which an ORA is necessary and appropriate
- a procedure-based approach to safety critical element management
- the methodology and key considerations in assessing risk

- consideration of combined risk and connectivity, including any changes in risk level over the period the abnormal situation is experienced
- ORA review and approval process
- ongoing management until permanent remediation is achieved.

Figure 3 summarises an ORA process and may assist licensees and operators in the development of specific procedures for their organisations.

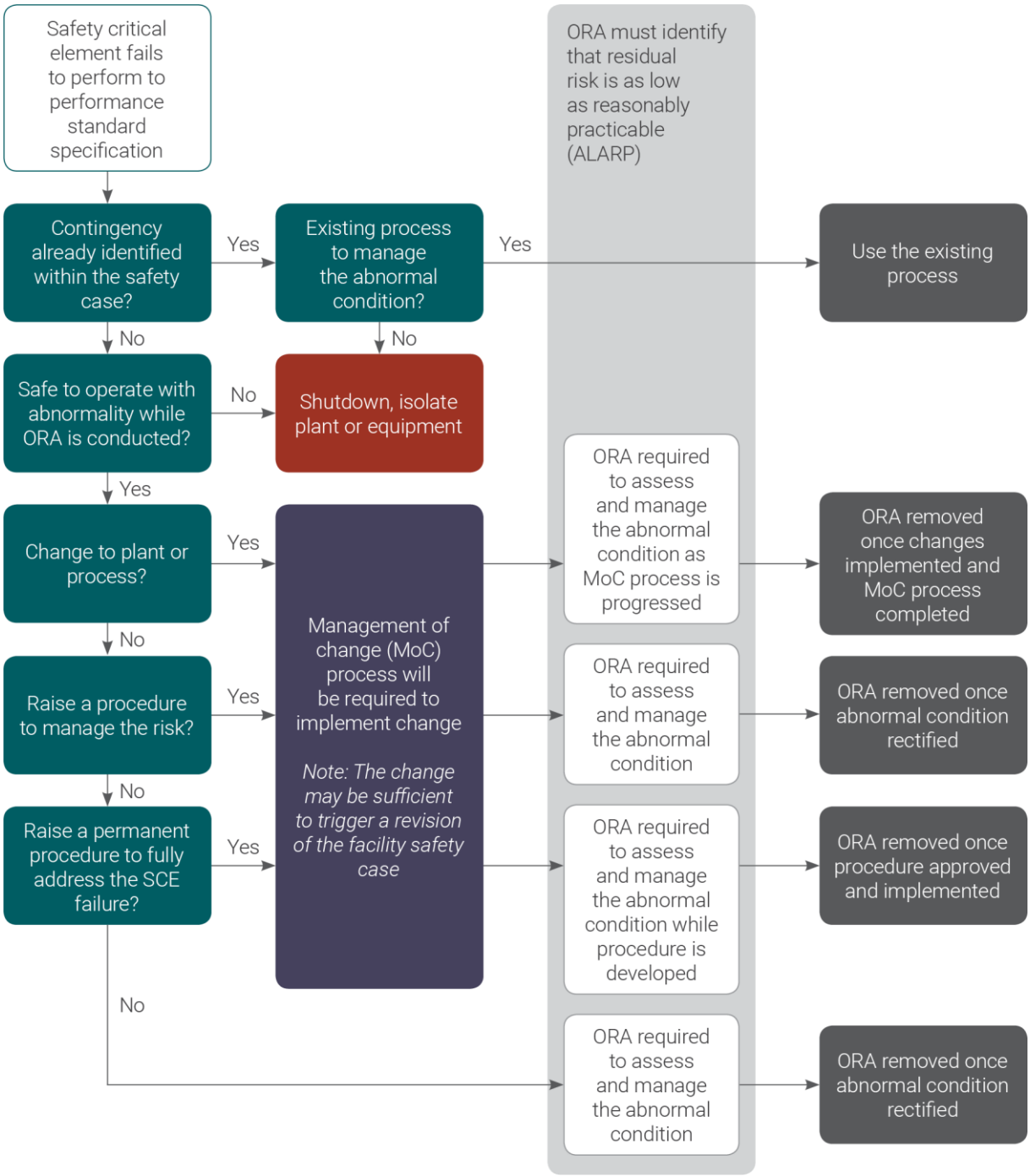

Figure 3 Example of ORA process flow

7.2.1 ORA procedures and considerations

This section outlines steps to take to develop effective procedures and protocols for the ORA. Licensees and operators should use this information as a guide to developing more detailed procedures relevant to their facilities.

(i) Initial response

The licensee or operator, in consultation with the relevant technical and other support personnel, should develop a procedure to guide development of initial response actions.

An appropriate initial response considers:

- the immediacy of the response required; e.g. shut down safely
- if the safety critical element impairment impacts other ORAs
- what other work or circumstances (e.g. weather) are taking place on the facility that may worsen the abnormal situation currently being identified
- difficulty in assessing the situation because not all support resources are available, or where the identified safety critical element impairment may be compounded by other known deficiencies or ORAs in place on the facility
- the remaining control measures and their adequacy under current circumstances
- information sourced from the safety case required to make the decision.

Procedures should be developed based on these considerations to assist informed decision-making about the initial response actions. The procedure may include information extracted from the safety case in the form of a check list which can support the initial qualitative assessment of increased risk.

Such information may include:

- MAE hazards
- summary of main plant with isolatable hydrocarbon inventories
- predicted hydrocarbon leak frequencies from those inventories and other associated leak frequencies
- significant escalation pathways
- probability and likelihood of escalation for each main inventory
- relative impact or significance of various barriers against immediate or escalated risks.

Questions on a checklist could include:

- What is the impaired system used for?
- Under what circumstances the system would be required to work?
- If these circumstances manifest, what will be the effects of the impairment?
- What can be done to reduce the potential for these circumstances to arise?
- What measures can be put in place to replace the functionality lost due to the impairment?
- How effective are these measures likely to be under the circumstances in which they are most needed?
- Are all of these measures sufficient to manage risk effectively, and for what duration?

The identification of remaining control measures as part of this initial assessment can be supported by reference to existing hazard management tools including bowtie diagrams.

If the answers are insufficient to provide confidence in the ongoing operation of the impaired safety critical element, then a precautionary approach should be adopted (i.e. affected activities or operations suspended or shut down) until further assessment can be undertaken.

Any decision to continue operations and proceed to ORA rather than suspend or shut down affected activities or operations should be supported by clearly and thoroughly documented reasons.

(ii) Preparation to conduct ORA

Once the initial response action has been taken and the need for an ORA identified, a team should be nominated to undertake the risk assessment. The ORA team should comprise appropriate technical, engineering, subject matter experts, third party specialists and members of the workforce who have the relevant knowledge and experience in relation to the risk being assessed.

Supporting documents should be collated for the ORA and team members should be familiar with those documents. Examples include:

- safety critical element performance standard(s)
- standard operating procedures
- plant layout diagrams
- piping and instrument diagrams
- cause and effect charts
- bowtie or similar hazard analysis outputs as available
- details of any other ORAs in place
- details of safety critical element maintenance backlogs
- details of outstanding inspection and assurance activities
- any relevant layers of protection analyses (LOPA) or safety integrity level assessments.

(iii) Description of safety critical element failure and hazard identification

The ORA should commence with a detailed description of the impaired safety critical element together with reference to the relevant performance standard(s) and description of the nature and extent of the safety critical element degradation. The description should identify the affected plant and equipment, what MAE(s) the safety critical element relates to and the failure gives rise to, and what barriers are affected by the failure.

Strict adherence to hazard identification processes is essential at this stage in order to provide the basis for all aspects of the ORA. Failure can result in flawed hazard identification and result in an ineffective ORA output.

Information should allow all team members of the ORA to fully understand the nature and extent of the failure of the safety critical element or abnormal situation.

(iv) Risk evaluation

Once the team has identified MAE hazard(s) associated with the impaired safety critical element, they can evaluate the risks arising from that event. The ORA needs to compare the risk of operating with an impaired safety critical element against the normal operating risk and should consider the following key factors.

Consequence

The risk evaluation should consider the potential consequences of the impaired safety critical element, identify and list all reasonably foreseeable scenarios and describe how these are affected by the impairment. The initial assessment should have considered the consequences that may result if no additional mitigating controls are put in place to compensate for the impaired safety critical element.

Information from the safety case and the performance standards should be available to the ORA team to support this aspect of the assessment. The team should be particularly mindful of any wider impacts of the impairment and the combined effect of any other ORA already in place on the facility.

Consequence assessment should consider the possibility of event escalation that may result from the impaired safety critical element. The emphasis in the ORA should be on the determination of potential consequences of the abnormal situation.

Likelihood

The second area of risk evaluation covers the likelihood of the identified consequences being realised. This again relates to the impairment without any mitigation measures being in place.

In most circumstances, this will be a qualitative or semi-quantitative assessment and is most relevant where the impaired safety critical element is preventive, such as ignition prevention. The ORA procedures should provide clear guidance on likelihood criteria specific to the identified MAEs.

Risk estimation (ranking)

Once the consequence and likelihood phases have been completed, the ORA team is able to do a risk estimate and ranking in terms of high, medium or low.

A risk criteria should already be in place for MAE risks, and the consequence and likelihood criteria should be relevant to MAE assessment rather than task-related personal injury outcomes.

The risk ranking is then used to:

- drive the requirement to shut down or limit activities or operations
- drive the identification and implementation of appropriate mitigation measures
- ensure appropriate levels of review, endorsement and approval of the ORA
- identify and prioritise remedial or recovery actions; for example, the time to repair the safety critical element under consideration
- decide specific times for review, revalidation and closure of the ORA.

Impact on other safety critical elements

The ORA team needs to maintain awareness and consider risks that may arise due to interrelationship and dependencies between safety critical elements. These should be documented in the relevant performance standards which the team needs to consider at the start of the risk evaluation. An example of this could be a faulty gas detector which affects alarm systems, ventilation trips and emergency shut down initiation.

(v) Identification of mitigation measures

The team needs to identify and consider control measures that will mitigate the risk identified and assessed against the impaired safety critical element. Strict compliance with the hierarchy of controls should be used when considering these mitigating measures in descending order as follows:

- elimination of the hazard by shutting down the affected plant or equipment
- use of an engineering solution to replace or supplement the impaired safety critical element
- procedural controls that restrict certain work activities or tasks in an affected area
- human intervention.

All available controls should be considered and decisions documented as to why mitigation measures are chosen and put in place. Mitigation in relation to human intervention should always be a last resort, with elimination and engineering solutions considered first. Procedural and human intervention controls should be considered in detail and assurance provided that this is manageable in both normal and abnormal conditions.

Performance standards, bowtie diagrams or other hazard management tools should be reviewed and updated to reflect that sufficient effective control measures remain in place to justify continued operation. Following implementation of additional mitigation measures, checks are required to verify that these measures are available and reliable. This could be achieved by rescheduling routine assessments to provide confidence in the availability and reliability of the additional mitigation measures.

(vi) Assessment of residual risk and risk determination

The residual risk for each of the identified hazards should be assessed by the ORA team taking into account the risk reduction effect of the mitigation measures. This assessment should assign the new risk ranking (high, medium or low) and enable the team to determine the acceptability of continued safe operation of the impaired safety critical element. The organisation should have in place a suitable procedure that provides direction as to the acceptable levels of residual risk to enable a recommendation for shut down or continued safe operation to be made as appropriate.

The lowering of the residual risk below that of the original risk level for the safety critical element does not necessarily mean that the proposal is acceptable. Focusing on the consequences identified should prompt consideration of the residual risk level and drive efforts to further reduce the risk.

(vii) Demonstration of ALARP and risk acceptability

Demonstration that control of MAE risks complies with the relevant statutory provisions and that the level is as low as reasonably practicable (ALARP) is already contained within the facility safety case.

An impaired safety critical element will temporarily raise the level of risk defined in the safety case to a level that is higher than the ALARP level. The results of the ORA should show that when all reasonably practicable risk reduction measures have been implemented, the determination of residual risk is acceptable or unacceptable and enables the team to make a judgement to continue operations or to shut down.

(viii) Combined risk

Facility management and the ORA team should have information of other ORAs on the facility as well as other issues such as:

- integrity issues
- deferred preventative maintenance or corrective maintenance activities
- specific summary of any ORAs where human controls are in place
- the level of activity on the facility
- the nature and effect of any simultaneous operations.

Licensees and operators should have a means to record and ensure visibility of all current ORAs, impaired safety critical elements and temporary mitigation measures. This will provide facility management with an overview of all ORAs in place and the combined effect on MAE hazard management on the facility at any given time.

Facility managers should ensure that procedures exist for an effective means of collating, reviewing and communicating the status information of the ORAs and the effect on the facility risk profile.

(ix) Review, endorsement and approval

Documented procedures should show clear routes and levels of authority for the review, endorsement and approval of documented ORAs to be adhered to. Levels of authority should reflect and align with levels of assessed risk or relative safety-criticality of the impaired safety critical element.

(x) Validity period

Procedures in place should define the acceptable periods for an ORA to remain in force and should cause the ORA review team to specify a validity period during which the impairment situation should be rectified.

These arrangements should be linked to the revised level of risk and should ensure timely restoration of the safety critical element functionality and original level of MAE risk. Ongoing renewal of the ORA or adjusting the safety critical element restoration dates is not generally considered to be an acceptable practice or ALARP.

(xi) Recording and communications of ORA

The organisation should have procedures in place that specify the means of recording outputs of the ORA. A template is normally used for this purpose.

It is crucial that members of the workforce exposed to the risk, or personnel making risk-based decisions (in particular process operators, control room operators and emergency response team members) are kept informed of operational risk assessments and associated changes to a safety critical element.

The arrangements put in place should pay attention to, and specify how, visibility is maintained over the life cycle of the ORA; for example, across crew or shift changes.

7.3 Monitoring, audit and review

Licensees and operators should have procedures and protocols for ongoing monitoring, audit and review of the ORA process.

Monitoring should include a mechanism for tracking the number of ORAs in place on each facility, the length of time each ORA has been in place and assurance that the impairment situations are resolved effectively.

The ORA process should be subject to regular audits as part of the organisation's safety management assurance. The audit should examine the ORA procedure, its implementation and continued adherence to documented measures to demonstrate that the procedure and its implementation across the facility remains robust. The audits should assess compliance with the procedure and demonstrate the system is effective in managing the MAE risks.

A review process should be in place through the organisation's SMS to provide assurance that MAE hazards are well managed and operational risk management processes are applied appropriately and effectively.

8 Operational risk and change management requirements

All changes at a facility should be managed to ensure that the change does not introduce a new hazard or increase the risk of an existing hazard. Change may provide an opportunity to reconsider controls and re-evaluate whether that change will facilitate modification of controls or additional controls which were not considered practical before.

Change may consist of one or more of:

- temporary change
- permanent change
- technical change
- hardware or software change
- organisational or administrative change
- procedural change
- maintenance change
- construction change.

There are a number of systems in place within an operating company to manage the type of change, including:

- technical change management
- operational risk assessment
- job safety assessment
- document control.

Licensees and operators should assess all change management requirements and consider the possibility that the facility safety case may need to be updated. If this is required, then the safety case will need to be updated accordingly and re-submitted for acceptance by the Minister or in the case of a major hazard facility, the Chief Officer.

Related information can be found in the *Management of change* guide.

Appendix 1 Legislative provisions

Petroleum (Submerged Lands) (Management of Safety of Offshore Facilities) Regulations 2007

r. 16 Facility description, formal safety assessment and safety management system

Petroleum (Submerged Lands) (Pipelines) Regulations 2007

r. 29 Description of pipeline management system

Petroleum (Submerged Lands) (Diving Safety) Regulations 2007

r. 7 Contents of DSMS

Petroleum and Geothermal Energy Resources (Management of Safety) Regulations 2010

r. 10 Principal provisions of safety management systems

r. 11 Risk assessment for major accident events

r. 12 Ongoing management of safety

Petroleum Pipelines (Management of Safety of Pipeline Operations) Regulations 2010

r. 10 Pipeline operation description, formal safety assessment and safety management system

Dangerous Goods Safety (Major Hazard Facilities) Regulations 2007

r. 23 Risk assessment, operator of major hazard facility to prepare

r. 27 Safety report, approval of by Chief Officer

Appendix 2 References and acknowledgements

Development of this Guide has used:

- NOPSEMA suite of guidance notes
- AS/NZS ISO 31000 *Risk management – Principles and guidelines*
- IEC ISO 31010 *Risk management – Risk assessment techniques*
- ISO 17776 *Petroleum and natural gas industries – Offshore production installations – Guidelines on tools and techniques for hazard identification and risk assessment*
- AS IEC 61511 *Functional safety – Safety instrumented systems for the process industry sector*
- AS 2885 *Pipelines – Gas and liquid petroleum - suite of standards*
- AS IEC 61882 *Hazard and operability studies (HAZOP studies) – Application guide*
- CCPS *Guideline for initiating events and independent protection layers in layer of protection analysis*

Appendix 3 Glossary

ALARP. As low as reasonably practicable. Also includes the term “so far as reasonable practicable (SFARP) for the purpose of this Guide.

Facility. The term facility has been adopted throughout this document to cover offshore and onshore facilities and pipelines including aboveground structures associated with onshore pipelines.

FSA. Formal safety assessment.

HAZID. Hazard identification study.

HAZOP. Hazard operability study.

JHA. Job hazard analysis.

JSA. Job safety analysis.

LOPA. Layers of protection analysis.

MAE. Major accident event – an event connected with a facility, including a natural event, having the potential to cause multiple fatalities of persons at or near the facility (or as defined within the relevant legislation pertaining to a facility).

Major incident. An incident involving or affecting a Schedule 1 substance (Dangerous Goods Safety (Major Hazard Facilities) Regulations 2007) that causes serious harm to people, property or the environment. Referred to as an MAE in this Guide.

MoC. Management of Change.

MHF. Major hazard facility.

ORA. Operational risk assessment.

P&ID. Pipeline and instrumentation diagram.

Performance standard. A standard established by the operator defining the performance required for a safety critical element typically defining the functionality, availability, reliability, survivability and interdependency of the safety critical element.

QRA. Quantitative risk assessment.

Safety Case. In this document covers all safety management systems, plans and other safety-related documents referred to in WA legislation.

Safety critical element. Any item of equipment, system, process, procedure or other control measure the failure of which can contribute to an MAE.

SIMOPS. Simultaneous operations.

SME. Subject matter expert.

Appendix 4 Further information

Other guides available:

- *ALARP demonstration*
- *Audits, review and continual improvement*
- *Bridging documents and simultaneous operations (SIMOPS)*
- *Diving safety management system*
- *Dangerous goods safety guide – Risk assessment for dangerous goods*
- *Dangerous Goods Safety (Storage and Handling of Non-explosives) Regulations 2007 - guide*
- *Emergency planning*
- *Hazard identification*
- *Major accident events, control measures and performance standards*
- *Involvement of members of the workforce*
- *Management of change*
- *Offshore facility safety case*
- *Pipeline management plan*
- *Pipeline operation safety case*
- *Records management including document control*
- *Reporting of accidents. incidents and dangerous occurrences*
- *Reporting dangerous goods incidents – guideline (6th edition)*
- *Safety management system*