Board Meeting: May 2017	Agenda Number: 8 (iv)	Record: ED17/70

LORD HOWE ISLAND BOARD
Business Paper

OPEN SESSION

ITEM

Risk Management Policy and Guidelines

RECOMMENDATION

It is recommended that the Board endorse the draft Risk Management Policy and Guidelines.

BACKGROUND

The most explicit legislative requirement for management of risk is established by the *Work Health and Safety Act 2011.*

Other legislative obligations for management of risk arise under the following:

- *Work Health and Safety Regulation 2011* and supporting codes of practice,
- *Explosives Act 2003*,
- *Workplace Injury Management and Workers Compensation Act 1998*,
- *Workers' Compensation (Dust Diseases) Act 1942*,
- *Workers' Compensation (Bush Fire, Emergency and Rescue Services) Act 1987*, and
- *Dangerous Goods (Road and Rail Transport) Act 2008*.

Section 11 of the *Public Finance and Audit Act* requires the heads of government agencies to ensure there is an effective system of internal control over the financial and related operations of the agency. However Government's expectation that agencies will undertake systematic management of risk has been clearly established through, for example, NSW Treasury Policy Paper TPP 1503, *Internal Audit and Risk Management Policy for the NSW Public Sector*, which requires that agencies have a risk management framework in place that supports the agency to achieve its objectives by systematically identifying and managing risks to increase the likelihood and impact of positive events, and mitigate the likelihood and impact of negative events.

CURRENT POSITION

The Draft Risk Management Policy and Guidelines provide the context in which all the Board's specific risk management plans and activities operate. The subordinate plans and systems include the following:

- WH&S Policy and Risk Management System,
- Aerodrome Transport Security Program,
- Lord Howe Island Aerodrome Manual,

- Electricity Network Safety Management Plan, and
- Lord Howe Island Local Emergency Management Plan (and its subordinate suite of plans).

The Risk Management Policy and Guidelines are based on AS/NZS/ISO 31000:2009, Risk Management (the Standard). It details the common methodology to be used to assess and address the level of risk inherent in Agency operations and activities.

RECOMMENDATION

It is recommended that the Board endorse the draft Risk Management Policy and Guidelines.

Prepared: Bill Monks, Manager Business and Corporate Services

Endorsed: Penny Holloway, Chief Executive Officer

LORD HOWE ISLAND BOARD
INTERNAL POLICY

TITLE	**Draft Risk Management Policy and Guidelines**		
DATE ADOPTED			
REVISED	May 2017	**REVIEW**	2 years
FILE REFERENCE	PO0018		
ASSOCIATED LEGISLATION, POLICIES & PROCEDURES	• *Work Health and Safety Act 2011*. • *Work Health and Safety Regulation 2011* and supporting codes of practice. • *Explosives Act 2003*. • *Workplace Injury Management and Workers Compensation Act 1998*. • *Workers' Compensation (Dust Diseases) Act 1942*. • *Workers' Compensation (Bush Fire, Emergency and Rescue Services) Act 1987*. • *Dangerous Goods (Road and Rail Transport) Act 2008*.		

1 Introduction

The Lord Howe Island Board (LHIB) operates in demanding physical, environmental, social and business contexts and faces a diverse and complex array of issues. In this situation, effective management of risk is critical to the achievement of our corporate goals and is an important element of our corporate governance.

Risk management involves informed and responsible risk taking; it is not only about risk avoidance. A systematic risk management approach fosters creativity and innovation as well as controlling and mitigating unacceptable risk.

Effective risk management is achieved by systematically identifying and assessing risks in relation to the achievement of objectives, and thoughtfully assessing options for dealing with each risk before deciding what to do.

The risk management policy and guidelines set out in this document are intended to help ensure risk in LHIB is managed systematically, efficiently and effectively. The LHIB's risk management policies and procedures are based on the Australian/New Zealand Risk Management Standard, and so are consistent in their approach and methodology.

2 Objectives

The objectives of LHIB's Risk Management Policy and Guidelines are to:

a. Make risk management an integral part of LHIB's business planning and performance monitoring processes.

b. Encourage systematic identification and assessment of risk to inform and improve decision making processes at all levels.

c. Provide openness and transparency in decision-making and ongoing management processes.

d. Promote a culture of continuous improvement in the management of risk across the organisation.

e. Encourage and support a proactive approach to the identification and management of strategic and operational issues throughout the organisation.

f. Improve integration and coordination of risk management practices in LHIB.

3 Scope and Application

The policy and guidelines apply to all LHIB staff and management processes. The management processes to which this policy relates include strategic and business planning, policy development, project management, and decision making at both strategic and operational levels.

4 Definitions

1. ***Risk*** is the chance of something happening that will have an impact on objectives.

2. ***Risk management*** is the culture, processes and structures directed towards realising potential opportunities whilst managing adverse effects.

Definitions of other terms used in relation to risk management are at Appendix C.

5 Relevant Legislation and Other Mandating Instruments

The most explicit legislative requirement for management of risk is established by the *Work Health and Safety Act 2011.*

Other legislative obligations for management of risk arise under the following:

- *Work Health and Safety Regulation 2011* and supporting codes of practice,
- *Explosives Act 2003*,
- *Workplace Injury Management and Workers Compensation Act 1998*,
- *Workers' Compensation (Dust Diseases) Act 1942*,
- *Workers' Compensation (Bush Fire, Emergency and Rescue Services) Act 1987*, and
- *Dangerous Goods (Road and Rail Transport) Act 2008*.

There is no specific legislative requirement that NSW government agencies implement general risk management, although Section 11 of the *Public Finance and Audit Act* requires the heads of government agencies to ensure there is an effective system of internal control over the financial and related operations of the agency. However Government's expectation that agencies will undertake systematic management of risk has been clearly established, through, for example:

- NSW Treasury – *Internal Audit and Risk Management Policy for the NSW Public Sector – TPP 15-03*, which requires that agencies have a risk management framework in place that supports the agency to achieve its objectives by systematically identifying and managing risks to increase the likelihood and impact of positive events, and mitigate the likelihood and impact of negative events.

- NSW Treasury - *Total Asset Management Submission Requirements TPP 13-03*, which places significant emphasis on risk management.
- The *Annual Reports (Departments) Regulation 2015* under which agencies are required to report on their risk management activities.

The *Electricity Supply (Safety and Network Management) Regulation 2014* requires the LHIB to take all reasonable steps to ensure that the design, construction, commissioning, operation and decommissioning of its network (or any part of its network) is safe. This regulation requires a safety management system for the network to be established in accordance with AS 5577 (this standard deals with network risk management).

Policy

6 Key Principles

LHIB is committed to efficiently and effectively managing risks to the achievement of our strategic, management and operational objectives in order to:

(a) Protect life, property, and environmental values, both natural and cultural;

(b) Minimise losses and take advantage of opportunities in all areas of our operations;

(c) Improve and maintain the quality of our decision making; and

(d) Enhance our capacity to influence and support the community.

To this end, LHIB will:

a. Systematically identify, assess, treat and monitor risk in accord with Australian/New Zealand Standard AS/NZS ISO 31000:2009 and best practice guidelines published by the NSW Treasury.

b. Conduct a strategic corporate risk assessment every three years to inform development of our management plans, specific risk control strategies, and audit and compliance program.

c. Establish a risk management system that:

i. Determines and communicates authorities, accountabilities and responsibilities of all staff;

ii. Provides for appropriate training and resourcing;

iii. Covers the full range of risks that require management;

iv. Uses risk assessment criteria consistently throughout the organisation;

v. Facilitates the systematic, structured identification and assessment of risks;

vi. Formalises action planning and review; and

vii. Enables LHIB to demonstrate that all significant risks are being diligently managed, with the risk treatment proportional to the risk and the selection of treatment options taking into account relevant factors such as feasibility, cost and effectiveness.

7 Responsibilities

Every LHIB staff member has a responsibility to contribute to the risk management process:

a. By identifying, reporting and/or managing risks;

b. By encouraging and supporting other LHIB staff in identifying, reporting and/or managing risks; and

c. By complying with LHIB policies and procedures designed to address particular types of risk.

In addition, the LHIB expects that contractors and consultants employed to do work in, or on behalf of, the agency will also contribute to the risk management process by identifying, reporting and/or managing risks and by complying with LHIB policies and procedures. Contract conditions are to include specific provisions in relation to risk management.

8 Risk Tolerance

LHIB accepts that not all risks can be controlled, and that resource constraints can limit capacity to control risks. However, the Board seeks to minimise risks whilst working towards the achievement of the Board's strategic and operational objectives. In doing this, the Board's approach is informed by the following principles:

1. Priority will always be given to the protection of life and property, consistent as far as possible with the protection of environmental values,

2. Risks will be treated in accordance with their rating, with risks rated as extreme being addressed first, followed as resources permit by those rated high, then medium and lastly low,

3. Action to reduce or control risks rated as extreme will commence immediately management becomes aware of the assessed risk level, while action to address risks rated as high will commence as soon as practicable,

4. In managing risk, the Board seeks to ensure that any reasonably foreseeable risk of the type which could give rise to a claim for civil liability is actively assessed and managed, and

5. Through its regular and systematic risk assessment processes, and this clear statement of risk tolerance, the Board seeks to continue to foster creativity and innovation whilst concurrently ensuring that unacceptable risk is controlled and risk taking within the agency is informed and responsible.

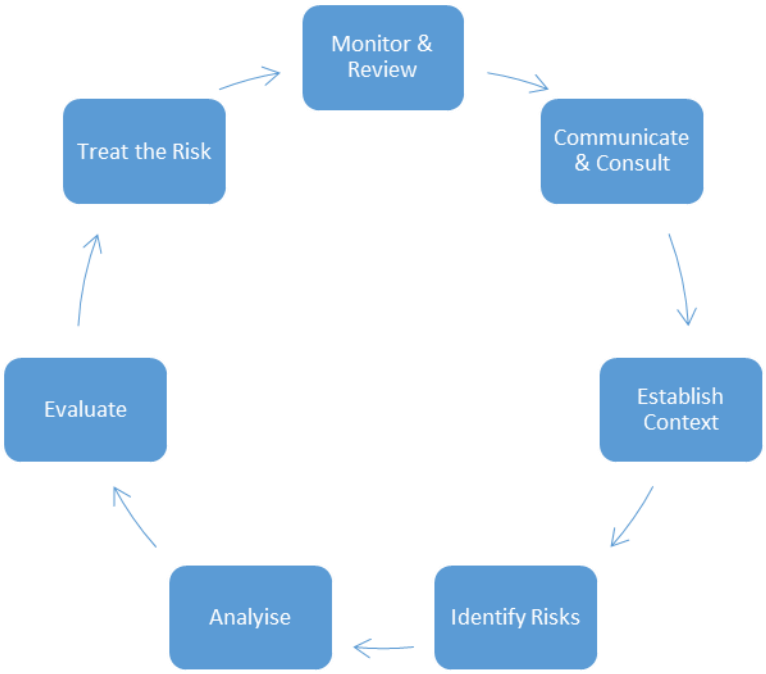
Operational Risk Assessment Guidelines

Overview

This procedure is based on AS/NZS/ISO 31000:2009, Risk Management (the Standard). It details the common methodology to be used to assess and address the level of risk inherent in Agency operations and activities. For guidance in relation to the application of this procedure or assistance in the conduct of operational risk assessments, refer to the Standard; HB 436 – Risk Management Guidelines; or the SICorp website.

An overview of the Risk Management process detailed in the Standard (Flowchart) is attached as Appendix A. Operational risk advice and assistance is provided by GIO and may be sourced through LHIB's Client Services Manager.

Process



Communicate and Consult

Has everybody who needs to know been contacted, involved, informed and kept up to date? Communication and consultation are important considerations at each stage of the risk management process. They should involve a dialogue with all stakeholders (both internal and external) with a focus on consultation, rather than a one way flow of information from the decision maker to stakeholders.

All stakeholders must be confident that their views have been appropriately valued and considered, and that they have been kept informed of the actions being taken and the reasons behind those actions. This may extend to the preparation and implementation of a stakeholder communication strategy. Broad "ownership" of the risk and the plans to manage it is essential to a successful risk management outcome.

Establish the Context

The first step in risk management is to establish the context of the risk. This can be done by asking a series of questions, such as:

What do we want to do or achieve? Define the desired outcomes of the event, activity or project.

How will we know we have been successful? Identify the success measure or measures for each desired outcome.

W*ho will be involved in or affected by what we want to do?* Identify the major stakeholders for this activity, both internal and external to LHIB.

Do any of the Stakeholders need to be involved in the Risk Assessment? All stakeholders who may feel they have a right to be consulted should be. A formal risk assessment should not proceed until all appropriate stakeholders can be assembled and/or consulted. All stakeholders who are actively involved in the achievement of the success measures **must** be involved in the risk assessment.

What records do we need to keep? The likely consequences of the decisions to be made and the importance of future stakeholders being able to understand why these decisions were made will dictate the level of record keeping required. Decisions concerning the making and capturing of records should take into account:

The legal and corporate governance needs for records (*State Records Act* 1998).

The cost of creating and maintaining records.

The benefits of re-using information in the future.

What criteria will we use to analyse the risk? The criteria contained in Table 1 and Table 2 below is generic, based on financial and other considerations. They will not be appropriate for the analysis of every risk faced by LHIB and a decision on their applicability to the particular risk under consideration must be made. Other criteria may be developed in-house, based on operational, technical, legal, social or environmental considerations, to name just a few. Criteria may be either qualitative or quantitative in nature.

How will the rest of the risk management process be structured? Determine the elements or steps that the activity/event/project can be divided into to create a logical framework that helps ensure significant risks are not overlooked.

Identify the Risks

What, where, when, how and why can things happen to prevent us from achieving our success measures? Risks that have not been identified cannot be assessed. Alternative methods to identify risks include:

A brainstorming session with all stakeholders.

Checklists developed for this or similar events/activities/projects.

An examination of previous events/activities/projects of this type.

The constitution of an experienced panel to consider the event/activity /project.

Risk areas may include, but are not limited to:

Management (planning, supervision, leadership).

People (competence, skills, experience, reliability, safety, training, insurance).

Property and other Assets (availability, suitability, damage, insurance).

Financial (funding, sponsorship, salaries, budgeting, control).

Regulatory/Legal (statutory requirements, committee duties and responsibilities, duty of care to stakeholders).

Political (community participation and support, government policies, risk of adverse publicity).

Weather (heat, cold, rain, fire ban, fog).

Communication (Memorandum of Agreement/Memorandum of Understanding required, meetings, marketing, methods and frequency of contact?).

Anything else you can think of (nobody knows your activity better than you!)

All risks identified should be communicated to your immediate supervisor, if he or she did not participate in the risk identification exercise.

Analyse and Evaluate the Risks

How big are the risks we have identified? Determine how likely a risk is to occur and how large the impact would be if it did occur. **These tables are generic in nature and careful consideration should be given to their applicability for the specific risk profile being assessed.** Consider risk in terms of the most plausible worst case scenario.

A vast array of methodologies may be sourced from ISO 31010: 2009 – Risk Management – Risk Assessment Techniques.

9 Table 1: Likelihood

Descriptor	Description	Indicative Frequency
Almost Certain (A)	The event will occur on an annual basis	Once a year or more frequently
Likely (B)	The event has occurred several times in your career	Once every three years
Possible (C)	The event might occur once in your career	Once every 10 years
Unlikely (D)	The event does occur somewhere from time to time	Once every 30 years
Rare (E)	Heard of it occurring elsewhere	Once every 100 years

10 Table 2: Consequence

CONSEQUENCE					
Category	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Environment	Minimal environmental impact; isolated release only	Minor environmental impact; on-site release immediately controlled	Significant environmental impact; on-site release contained with assistance	Major environmental impact; release spreading off-site; contained with external assistance	Fatalities occur; extensive release off-site; requires long term remediation
Financial	Negligible financial loss ($10,000), no impact on program or business operation	Minor financial loss ($10,000-$50,000); minimal impact on program or business operation	Significant financial loss ($50,000-$500,000); considerable impact on program or business operations	Major financial loss ($500,000- $1M); severe impact on program or business operation	Extensive financial loss ($1M+); loss of program or business operation
WHS	First aid only required	Minor medical treatment with or without potential for lost time.	Significant injury involving medical treatment or hospitalisation and lost time	Individual fatality or serious long term injury	Multiple fatalities or extensive long term injury
Professional Indemnity	Isolated, internal or minimal complaint; minimal loss to organisation	Contain complaint or action with short term significance; medium loss to organisation	Significant complaint involving statutory authority or investigation; prosecution possible with significant loss to organisation	Major complaint with litigation and long term significance; very high loss to organisation	Extensive litigation with possible class action; worst case loss to organisation; threat to viability of program or service.
Public Liability	First aid only required; minimal loss to organisation	Some medical treatment required; medium loss to organisation	Significant injury involving medical treatment or hospitalisation; high loss to organisation	Severe injuries or individual fatality; very high loss to organisation	Multiple fatalities or extensive long term injuries; worst case loss to organisation
Property & Infrastructure	Isolated or minimal loss; short term impact; repairable through normal operations	Minor loss with limited downtime; short term impact; mostly repairable through normal operations	Significant loss with temporary disruption of services; medium term impact on organisation	Critical loss or event requiring replacement or property or infrastructure; long term impact on organisation	Disaster with extensive loss and long term consequences; threat to viability of service or operation
Reputation	Isolated, internal or minimal adverse attention or complaint	Heightened local community concern or criticism	Significant public criticism with or without media attention	Serious public or media outcry, broad media attention	Extensive public outcry; potential national media attention

CONSEQUENCE					
Category	Insignificant (1)	Minor (2)	Moderate (3)	Major (4)	Catastrophic (5)
Natural Hazards	Minimal physical or environmental impact; isolated hazard only; dealt with through normal operations	Minor physical or environmental impact, hazards immediately controlled with local resources	Significant physical or environmental impact; hazards contained with assistance of external resources	Major physical or environmental impact; hazard extending off-site; external services required to manage	Extensive physical or environmental impact extending off-site; managed by external services; long term remediation required.
Information Technology	No measurable operational impact to organisation	Minor downtime or outage in single area of organisation; addressed with local management and resources	Significant downtime or outage in multiple areas of organisation; substantial management required and local resources	Loss of critical functions across multiple areas of organisation; long term outage; extensive management required and extensive resources	Extensive and total loss of functions across organisation; disaster recovery management required
Political and Governance	Isolated non-compliance or breach; minimal failure of internal controls managed by normal operations	Contained non-compliance or breach with short term significance; some impact on normal operations	Serious breach involving statutory authorities or investigation; significant failure of internal controls; adverse publicity at local level	Major breach with formal inquiry; critical failure of internal controls; widespread adverse publicity	Extensive breach involving multiple individuals; potential litigation; viability of organisation threatened
Industrial Relations	Isolated, internal or minimal impact on staff morale or performance; minimal loss to organisation	Contained impact on staff morale or performance of short term significance; medium loss to organisation	Significant impact on staff morale or performance of medium term significance; significant loss to organisation	Major impact on staff morale or performance with long term significance; very high loss to organisation	Extensive impact or organisational morale or performance; threat to viability or program or service
Contractual and Legal	Isolated non-compliance or breach; negligible financial impact	Contained non-compliance or breach with short term significance and minor financial impact	Serious breach involving statutory authority or investigation; prosecution possible with significant financial impact	Major breach with fines and litigation; long term significance and major financial impact	Extensive fines and litigation with possible class action; threat to viability of program or service.
Positive Consequence	Small benefit, low financial gain.	Small benefit, low financial gain.	Some enhancement to reputation, high financial gain.	Enhanced reputation, major financial gain.	Significantly enhanced reputation, huge financial gain.

11 Table 3: Risk Probability Matrix

Likelihood	Consequence				
	1	**2**	**3**	**4**	**5**
A	Medium	High	High	Very High	Very High
B	Medium	Medium	High	High	Very High
C	Low	Medium	Medium	High	High
D	Low	Low	Medium	Medium	High
E	Low	Low	Medium	Medium	High

ACTION: Determine the Risk Level for each identified risk and enter it in the Risk Register.

12 Table 4: Risk Rating

Low	Medium	High	Very High
Managed in day to day operations, by individual staff or small unit/team. Generally handled by SOP's, SWMS or checklists. Not normally entered on Risk Register.	Managed by designated responsible officer, may require specific procedures or processes. Monitored at Supervisor level. May be entered on risk register Notified to Risk Officer.	Managed by designated key responsible officer, entered on the Risk Register. Risk Action Plan compiled implemented. May require allocation of additional resources, procedures, processes or training. Monitored by Unit Manager and where one exists, notified to Risk Management Committee.	Managed by responsible Unit Manager. Entered on Risk Register. Requires immediate attention, including internal and external resources. Risk Treatment Plan written and implemented. Documented procedures. Monitored work processes and training. Monitored & resourced by Senior Management. Where one exists, monitored directly by Risk Management Committee/delegate.

13 Table 5: Risk Control Effectiveness

RISK CONTROL EFFECTIVENESS (RCE) - Assessing the Control Suite for a particular risk:	
Good	Nothing more to be done except review and monitor the existing controls. Control is well designed for the risk, address the root causes and Management believes that they are effective and reliable at all times.
Satisfactory	Most controls are designed correctly and are in place and effective. Some more work to be done to improve operating effectiveness or Management has doubts about operational effectiveness and reliability
Poor	While the design of controls may be largely correct in that they treat most of the root causes of the risk, they are not currently very effective. **Or** Some of the controls do not seem correctly designed in that they do not treat root causes, those that are correctly designed are operating effectively.
Very poor	Significant control gaps; Either control/s do not treat root causes or they do not operate effectively.
Uncontrolled	Virtually no credible control. Management has no confidence that any degree of control is being achieved due to poor control design and /or very limited operational effectiveness.

Evaluate the Risks

Are there any controls already in place? Determine if there are any existing controls already in place to address the identified risks. Establish if in fact the controls have actually been implemented and are operational. Existing controls could include any policies, processes or procedures established to:

Eliminate or reduce the likelihood of a risk occurring.

Mitigate the impact if a risk does occur.

Share or transfer the identified risk (e.g. insurance and /or indemnity clauses).

Once existing controls have been identified, risks need to be re-evaluated and prioritised, to ensure that the greatest risks are addressed first. The process to follow is:

Note any existing controls identified against the appropriate risks in the Risk Register.

Re-assess the risk in light of existing controls and adjust its Risk Level accordingly to establish a residual risk rating.

Make a recommendation as to whether the risk is considered to be acceptable or unacceptable, with the reasons why.

Forward a copy of the completed risk assessment and recommendation to your manager, who will then present all information to the Risk Management Committee for confirmation or modification of the recommendation and Risk Level. If the risk is deemed unacceptable (a confirmed Risk Level of High or above), it will then be:

- Prioritised in relation to other registered risks (considering the confirmed Risk Level rating, the nature of the people and/or property at risk and the impact on Lord Howe Island Board's reputation and credibility, should the risk event occur).
- Entered onto the Risk Register.

Treat the Risks

What are we going to do about the risks we have identified? After a risk has been entered onto the Risk Register, options to treat it must be considered and action plans developed. Risk Treatment Plans (RTP) must detail:

The actions which will be taken to address the risk.

The manager responsible for ensuring that the RTP is carried out (Responsible Manager).

The officer/s responsible for carrying out individual actions specified in the RTP (Responsible Officer/s).

When the specified actions are to be completed by (due date).

Unless actions are determined and responsibilities for them are allocated, the Risk Identification and Assessment processes will have been wasted

The outcome of any actions specified should be to (in priority order):

Eliminate the possibility of a risk occurring.

Reduce the likelihood of occurrence to an acceptable level.

Mitigate (reduce) the consequences, should a risk occur.

Transfer or share the risk, generally through insurance or contracting out.

Actions to be taken in relation to specified Risk Levels are:

Very High – immediate action to be initiated and RTP's to be developed and implemented under the direct control of Senior Management. All documentation must be retained for future reference.

High – action timeframe to be determined by Senior Management, with RTPs developed by Responsible Manger/s for approval.

Medium – action timeframe determined and RTP's developed by Responsible Manager/s,

Low – Risk noted and treated appropriately by those affected.

Remember, all risks identified as High and above are to be entered into the Risk Register and have a RTP developed and implemented.

Risks identified as low and medium should, as a minimum, have this rating recorded as a file note, along with the reasons for that rating and any decisions/actions taken as a result of the Risk Assessment undertaken.

In a climate of constrained resources, careful consideration must be given to how resources are allocated to action plans. You may find it more valuable to reduce higher priority risks to an acceptable level, rather than eliminate them altogether and then use any resources saved to address lower priority risks.

Finally, consult your supervisor and any stakeholders who may not have been available the Risk Assessment, to ensure that you have left nothing out.

Monitor and Review

Have we got it right? Registered risks will remain open until they have been reduced and accepted, or eliminated. The Responsible Manager and the Risk Management Committee are to monitor the implementation of RTPs to ensure that agreed actions are being taken and review the risk levels, to reflect changes made.

Whenever an action is taken against a RTP, the Responsible Officer is to notify the Responsible Manager, who will:

Assess the effectiveness of the action taken.

Reassess the RTP to:

- Confirm its continued applicability; or
- Determine any changes that may now be required.

Reassess the risk rating and notify the Risk Officer (or equivalent) of the new suggested rating and any recommended changes to the RTP.

The details of the reassessment will then be confirmed or modified by the Risk Management Committee to determine whether or not the risk rating should be adjusted.

Once all directed actions have been completed, the risk will be re-assessed by the Responsible Manager and the Risk Management Committee and a decision made as to its acceptability or otherwise.

If a risk is considered to be unacceptable, further action needs to be taken to address that risk.

No activity should proceed with a risk that has been identified as unacceptable.

If in doubt, all Stakeholders involved with the original Risk Assessment are to be consulted, prior to a risk being closed off.

Record the Risk Management Process

Each stage of the Risk Management process must be recorded appropriately, as determined during the 'Establish the Context' step. For risks assessed as moderate and above, assumptions, methods, data sources, analyses, results and reasons for all decisions should all be recorded.

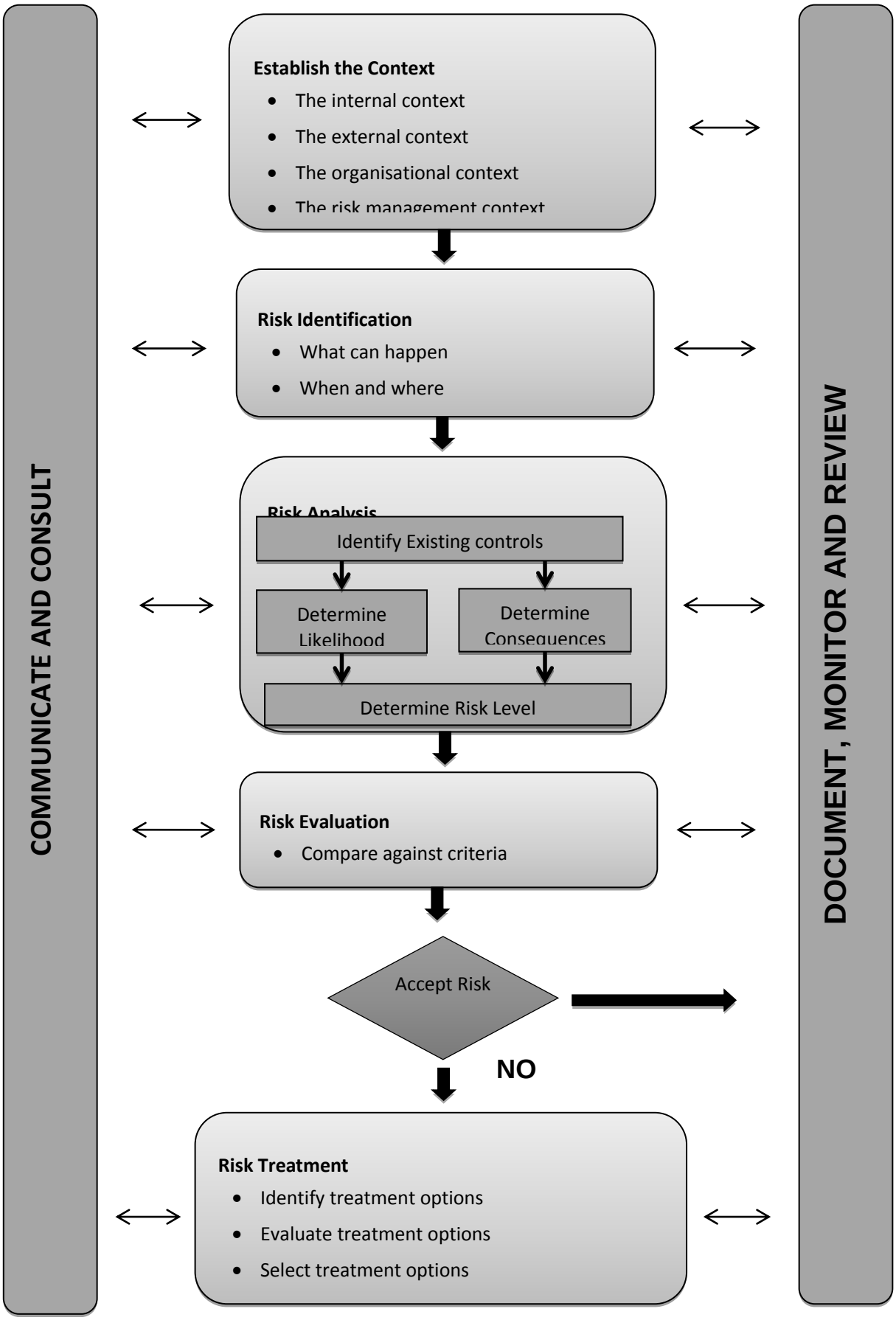
During the conduct of an event, activity or project for which a Risk Assessment has been undertaken, make notes on how effective the RTPs have been and what (if any) changes were made to the original Plans. This will allow better planning for the same or similar activities in the future.

All Risk Assessments and RTPs must be documented and appropriately filed for future reference: even if a risk is assessed to be insignificant and a decision is taken to do nothing, the reasoning that led to this decision must be recorded.

Integration of LHIB Risk Management Policy and Guidelines with Operational and Business Activities

The integration of this Risk Management Policy and Guidelines with the operational and business activities of the LHIB is shown in the chart at Appendix B.

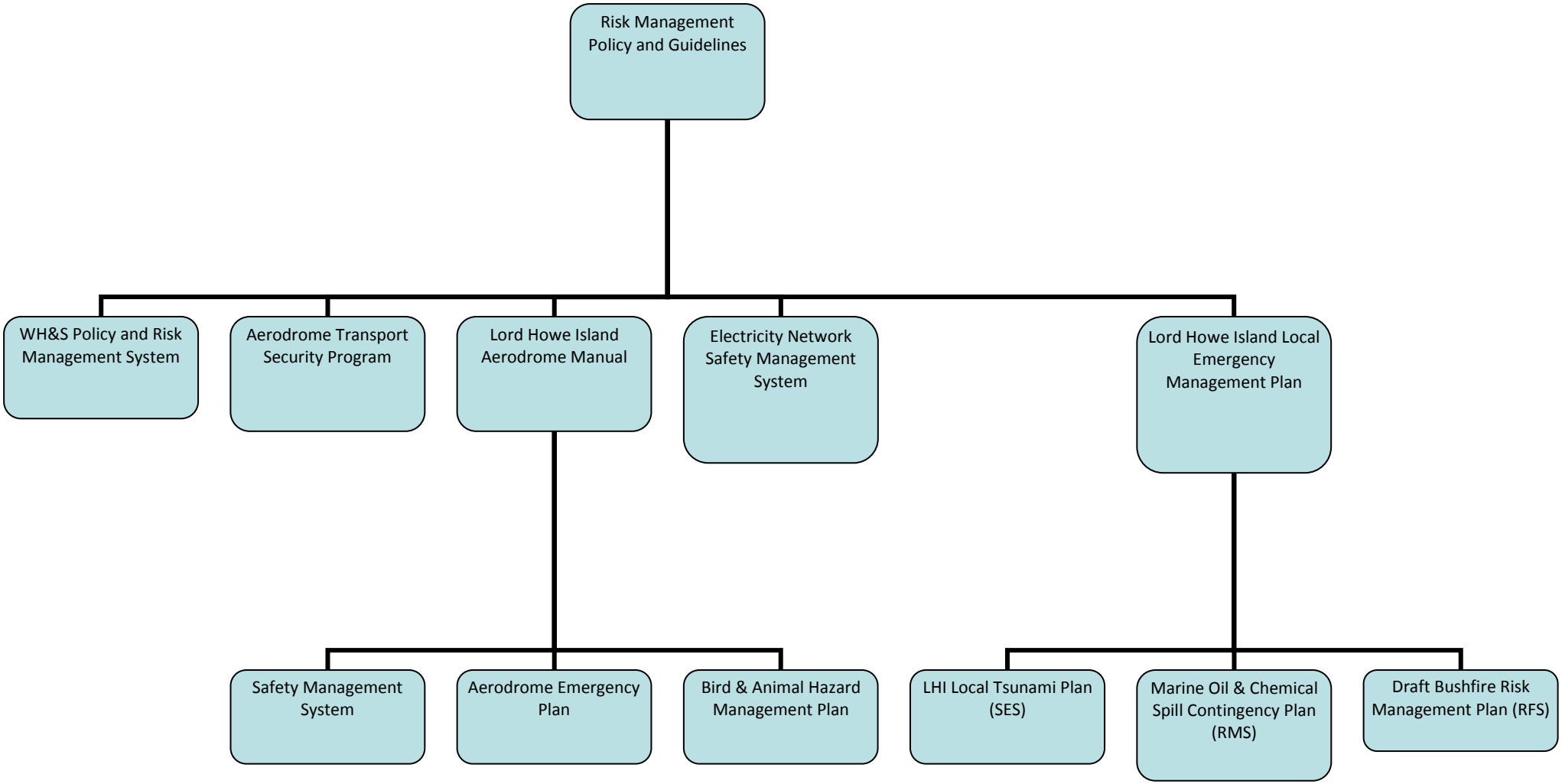
Appendix A: Risk Management Process



Appendix B – Integration of LHIB Risk Management Policy and Guidelines with Operational and Business Activities

The integration of this Risk Management Policy and Guidelines with the operational and business activities of the LHIB are shown in the chart on the following page.

Integration of LHIB Risk Management Policy and Guidelines with Operational and Business Activities



14 Appendix C – Risk Management Glossary

Risk Management Glossary	
Consequence	Outcome of an **event** affecting objectives. • An event can lead to a range of consequences. • A consequence can be certain or uncertain and can have positive or negative effects on objectives. • Consequences can be expressed qualitatively or quantitatively. • Initial consequences can escalate through knock-on effects.
Control	An existing process, policy, device, practice or other action that acts to minimise negative risk or enhance positive opportunities
Event	Occurrence or change of a particular set of circumstance. • An event can be one or more occurrences, and can have several causes. • An event can consist of something not happening. • An event can sometimes be referred to as an “incident” or “accident”. • An event without **consequences** can also be referred to as a “near miss”, “incident”, “near hit” or “close call”.
Frequency	Measure of the number of occurrences per unit of time
Hazard	A source of potential harm
Likelihood	Chance of something happening. • In risk management terminology, the word “likelihood” is used to refer to the chance of something happening, whether defined, measured or determined objectively or subjectively, qualitatively or quantitatively, and described using general terms or mathematically (such as a probability or a frequency over a given time period). • The English term “likelihood” does not have a direct equivalent in some languages; instead, the equivalent of the term “probability” is often used. • However, in English, “probability” is often narrowly interpreted as a mathematical term. • Therefore, in risk management terminology, “likelihood” is used with the intent that is should have the same broad interpretation as the term “probability” has in many languages other than English.
Loss	Any negative consequence, financial or otherwise

Risk Management Glossary

Mitigation	Action taken to reduce or moderate an unwanted consequence, to lessen its intensity, force or frequency
Monitor	To check, supervise, observe critically, or measure the progress of an activity, action or system on a regular basis in order to identify change from the performance level required or expected
Remediation	The remedying of a deficiency, especially applied to controlling or minimising hazards
Residual risk	Risk remaining after implementation of risk treatment
Risk	The effect of uncertainty on objectives • An effect is a deviation from the expected – positive and/or negative. • Objectives can have different aspects (such as financial, WHS, and environmental goals and can apply at different levels (such as strategic, project, product and process). • Risk is often characterised by reference to potential events and consequences, or a combination of these. • Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated **likelihood** of occurrence. • Uncertainty is the state, even partial, of deficiency of information related to, understanding or knowledge of an event, its consequence, or likelihood.
Risk analysis	Systematic process to understand the nature of and to deduce the level of risk.
Risk assessment	Overall process of risk identification, risk analysis and risk evaluation
Risk avoidance	A decision not to become involved in, or to withdraw from, a risk situation
Risk criteria	Terms of reference by which the significance of risk is assessed
Risk evaluation	Process of comparing the level of risk against risk criteria
Risk identification	Process of determining what, where, when, why and how something can happen
Risk management	Coordinated activities to direct and control an organisation with regard to **risk**
Risk management framework	Set of elements of an organisation's management system concerned with managing risk

Risk Management Glossary

Risk management process	Systematic application of management policies, procedures and practices to the tasks of communicating, establishing the context, identifying, analysing, evaluating, treating, monitoring and reviewing risk
Risk appetite	Amount and type of risk that an organisation is willing to pursue or retain
Risk management plan	Scheme with the **risk management framework** specifying the approach, the management components and resources to be applied to the management of **risk**. • Management components typically include procedures, practices, assignment of responsibility, sequence and timing of activities. • The risk management plan can be applied to a particular product, process and project, and part or whole of the organisation.
Risk management policy	Statement of the overall intentions and direction of an organisation related to **risk management**.
Risk owner	The person or entity with the accountability and authority to manage a risk
Risk reduction	Actions taken to lessen the likelihood, negative consequences, or both, associated with a risk.
Risk register	A record of risks, to which new risks are added as they are identified and from which other risks are removed once they have been satisfactorily addressed
Risk retention	Acceptance of the burden of loss, or benefit of gain, from a particular risk
Risk sharing	Sharing with another party the burden of loss, or benefit of gain, from a particular risk
Risk source (Hazard)	Element which alone or in combination has the intrinsic potential to give rise to a risk. (a risk source can be tangible or intangible)
Risk tolerance	The levels of risks that management deems acceptable
Risk treatment	Process of selection and implementation of measures to modify risk