

RedR Australia Risk Management Policy



Reviewed by:	Dave Simpson
Approved by:	Drasko Kraguljac
Review date:	28-Feb-19
Next review:	28-Feb-20
Distribution:	Internal only
Version number	2.5

Definitions

Program criticality – the extent to which a program and/or set of activities is deemed necessary for the achievement of organisational objectives.

Reasonable action – that which is acceptable, fair, honest, proper and would be considered reasonable for a similar organisation to take, considering the nature and severity of the risk of harm or loss, knowledge of severity of harm or loss, knowledge of solutions, availability of solutions, legal requirements and cost of solutions.

Risk – effect of uncertainty on objectives [ISO 31000].

Risk assessment – overall process of risk identification, risk analysis and risk evaluation [ISO 31000].

Risk Assessment Matrix – a commonly employed means of quantifying residual risk through cross-comparison of likelihood and consequence.

Risk Criteria – a collective term for tools employed to quantify risk categories, severity and consequence.

Risk factor – an element which can provide a source of risk [ISO 31000].

Risk management – coordinated activities to direct and control an organisation with regard to risk [ISO 31000].

Risk treatment – process to modify risk [ISO 31000].

1. Introduction

It is recognised that the work of RedR Australia (RedR) often places great demands on personnel in conditions of complexity and risk. As a responsible agency RedR has a primary duty of care towards its personnel and takes all reasonable steps to minimise and manage the risks associated with its mission to ensure staff security and wellbeing. This said, individuals are ultimately responsible for their own safety and all behaviour should be governed by this rule.

Robust risk management should not be viewed as an abstract concern. RedR Australia recognises that good organisational safety and security systems are critical to the effective implementation of programmes. As such the organisation seeks to ensure that sound risk management principles are mainstreamed throughout RedR Australia's operations. This document seeks to provide a baseline methodology for the practice of risk management within RedR.

2. Purpose and Scope

The Risk Management Framework and its associated protocols seeks to identify the risks RedR Australia is exposed to, as well as determining the effectiveness of current controls to mitigate those risks.

This policy seeks to embed good practice for risk management in relation to:

- a. Better identification and proactive management of opportunities and threats
- b. Improved incident management and reduction in loss and the cost of risk
- c. The development of a more risk-aware organisational culture through enhanced communication and reporting of risk
- d. A clear understanding by all staff of their roles, responsibilities and authorities for managing risk
- e. More confident and rigorous decision making and planning from a corporate governance perspective
- f. Improved compliance with relevant legislation
- g. Improved stakeholder confidence and trust

Effective risk assessment can help ensure alignment with RedR Australia's organisational risk appetite and objectives. As such (prior to commencement) risk assessments should be conducted on any and all new:

- Contractual activities
- Partnership agreements
- RedR events (including training events)
- Associated fundraising and communications activities

This policy applies to work both in Australia and overseas. Included in its scope are board members, staff, volunteers as well as other key stakeholders such as (and not limited to) overseas partners.

3. Roles and Responsibilities

Risks will be identified, reviewed and monitored on an ongoing basis at nominated levels within RedR; this process will be led by the **Manager Risk, Safety and Security**. Further, stakeholders including **staff** will, through agreed consultative processes, be involved in assisting **The Board** to determine the acceptable level of risk (risk appetite) which will exist in relation to the activities of RedR under the identified categories.

The **Chief Executive Officer** (CEO), via the delegated authority of **The Board**, is responsible for ensuring that RedR decisions and practices comply with the requirements of the relevant legislation, regulations and codes of conduct and practice. By extension, RedR **managers** will, with the support of the **Manager Risk, Safety and Security**, ensure that **staff** within their teams understand their responsibilities with respect to operational risk, and will assist in fostering a risk aware culture and application of risk management tools.

The **Board, SMT** and **staff** have a responsibility to make themselves aware of situations where someone or something may be at risk of harm or loss. They must then take reasonable action (see definitions) to remove or reduce those risks and escalate this information to the RedR **Senior Management Team**.

Any risks falling in the 'Extreme' Residual Risk category will be urgently brought to the attention of the **Board** via the **CEO**. Over time, it is expected that some risks will rise to 'Extreme' and then, through the application of appropriate mitigation actions, be reduced in significance and thereby be taken off the **Board** agenda.

4. Policy

Organisational approach to risk. RedR Australia considers risk management a crucial prerequisite for the long term viability of the organisation. The protection of personnel, earnings, assets and liabilities against known and unknown losses in a cost effective manner is a critical component of 'business as usual' (BAU) operations.

RedR Australia will adopt a planned and systematic approach to the management of risk. The requisite resources will be provided to enable successful implementation and continuous improvement of risk management processes in order to:

- i. Protect human life
- ii. Minimise trauma
- iii. Protect reputation (organisation, host agency and individual)
- iv. Protect information
- v. Protect equipment and other physical assets

RedR Australia utilises a Risk Assessment Matrix approach to quantifying risk (see **Annex B**). This, in conjunction with robust context analyses and consideration of program criticality, is used to inform a holistic approach to risk management that draws upon best practice as described by ISO 31000:2009 (see **Annex D**). **Annex C** summarises the relationship between this document (the Risk Management Framework) and the processes of both risk management and risk identification.

Ensuring that an appreciation for risk management processes is present within all functional areas of the organisation is a core tenet of RedR Australia's approach to safety; risk management will be incorporated into the strategic and operational planning processes at all levels within RedR.

Partner organisations. RedR Australia will engage, consult and involve partner organisations in the risk management strategy so they are aware of RedR risk policies and can assist in identifying and mitigating risks. Involving partner organisations will also assist them to gain information that informs their own risk management strategies.

Risk Identification Framework. Incident classification plays a vital role in the effective monitoring and analysis of incident trends. **Annex A** summarises the way in which RedR Australia categorises risk. Risks (together with any incidents, or 'eventuated risks') are categorised by both type and sub-type.

5. Documentation Framework

The framework of operational risk management documentation is laid out in Annex C. These processes/documents are also referenced in the RedR Operations Manual.

It is important to note that considerations regarding security are integral to RedR in all of its work; therefore, many related policies related to Human Resources, Finance, Communications and Training all affect security. Contracts, both employment and for services, will also have an impact on security management.

6. Implementation

Risk management will be monitored using the RedR Australia Risk Assessment Criteria/Matrix on an ongoing basis and as a standing item of business at the Senior Management Team meeting.

The Chief Executive Officer's Board Reports will document and speak to Risk Management through an Exceptions Report which outlines risk and actions taken to avert or mitigate risk.

The Risk Register will be revised and updated by the Senior Management Team of RedR. The revision will address and identify risk in order of priority, identify strategy to reduce risk, time frame, person responsible and expected outcome.

RedR Risk Management policy and associate assessment tools will be discussed, reviewed and updated as a component of annual Board strategic review meetings. This information will be revised and included on the Strategic Plan.

This policy will be revised annually by the Manager Risk, Safety and Security, with modifications or amendments approved by the Board.

7. References and related documents

- a. Child Protection Policy
- b. Travel Policy
- c. Global Security Policy
- d. Incident Response Handbook
- e. Ethics Hotline Policy
- f. Anti-Bribery and Corruption Policy
- g. RedR Values and Code of Conduct
- h. ISO 31000:2009 *Risk Management – Principles & Guidelines*

Annex A: Risk Identification Framework

Category	Type	Sub-type	Description
A	Overseas	Medical Illness Medical Injury Dental Loss/Theft Behavioural Corruption/Bribery Equipment Espionage Safeguarding Security Transport/Logistics Wellbeing/Compassionate	Any overseas risk event with the potential to impact the health or wellbeing of deployees/staff and/or directly impact service delivery.
B	Financial	Compliance	Cash flow, change of government, insurance, fraud. <i>Incidents of alleged/suspected fraud on DFAT funded programmes must be reported (via SMT) within five working days.</i>
C	Training	Trg. Medical Illness Trg. Medical Injury Trg. Equipment Trg. Wellbeing	Risk events associated with training and other contracted work.
D	Human Resources	Disciplinary/Grievance Equal Opportunities OH&S Recruitment Staff Wellbeing	Staff turnover, employment risk events, cohesion between Board and staff, staff leave, volunteer management, succession planning, OH&S, compliance with law and codes.
E	Organisational/ Governance	Reputation Communications IP IT & Systems	Board and governance, IT, data loss/corruption intellectual property rights, privacy.
F	Strategic Partnerships	3rd Party	Risk events associated with external relations and organisational reputation including events management and fundraising, relations with program partners and donors.
G	Other	Facilities	Physical access to buildings. Other risk events not captured by the above.

Fig.2: Risk Categorisation Matrix

Annex B: Risk Criteria/Matrix and Acceptability

Impact (Consequence) Rating. Indicates the impact of the risk on RedR operations.

Severity		Operational	Medical/Wellbeing	Financial	Reputational	Other	
1	Insignificant	No or very limited disruption to field/work day.	Very minor medical/wellbeing incident self-managed or attended to by medical specialist and/or First Aider.	Net impact of less than 1% of turnover (organisational) or self-funded (individual).	No significant direct reputational impact.	<i>Risk Descriptors are not presented in an attempt to capture an exhaustive list of events with the potential to impact the organisation.</i>	
2	Minor	Field day(s) disrupted as a result of administrative and/or bureaucratic issues.	Medical/wellbeing incident requiring brief attention by medical/wellbeing specialist.	Net impact of 1-2% of turnover.	Potential for adverse reputational impact internally or within sector.	<i>Rather they offer examples of what incidents of the respective severity may look like in four key areas of organisational risk (Operational, Medical/Wellbeing, Financial, and Reputational) in order to promote a shared/consistent understanding of the magnitude of each level.</i>	
3	Moderate	Multiple field days disrupted as a result of minor to moderate administrative issues.	Medical/wellbeing incident requiring out-patient admission (e.g. insect-borne disease, compassionate repat).	Net impact of 3-5% of turnover.	Adverse reputational impact at state/national level.		
4	Major	Multiple field days disrupted as a result of a serious (e.g. missing staff, illegal detention, relocation/evacuation from conflict/disaster) event.	Life-altering (non-life threatening medical/wellbeing incident or event).	Net impact of 6-20% of turnover.	Major adverse reputational impact at international level.		
5	Catastrophic	Proximate threat to organisational integrity. Forced suspension or cessation of operations, and/or loss of a substantial part of the organisation.	One or more fatalities. Kidnapping or abduction. Proximate threat to life/long-term wellbeing.	Net impact of greater than 20% of annual turnover, or any time RedR's financial obligations threaten to exceed its capacity to fulfil them.	Potential for irreparable/unrecoverable reputational damage.	<i>Risk Owners are then able to apply this more specifically to their area of responsibility/expertise.</i>	
-NM	Near Miss	Lessons can be learnt from causal factors when something almost goes wrong, not only when it does. The suffix 'NM' (e.g. 3NM) denotes a near miss; this signifies an incident where only a fortunate break in the chain of events leading up to the occurrence prevents harm from eventuating.					

Risk Likelihood. Provides an assessment of the likelihood of the risk occurring.

Level	Scale	Description	Probability*
1	Rare	The event is likely to occur only in highly exceptional circumstances, there is no known occurrence. Extremely remote chance of occurrence in a financial year. 'Once in a lifetime' event.	< 2%
2	Unlikely	The event could occur at some time and has occurred sometime in the world. However, it would not be classed as a common occurrence and would only occur in certain remote circumstances.	2-16%
3	Probable	The event might occur at some time. Has occurred in Australia in the past. Occurs either in RedR or the industry on a regular basis and frequently enough to be more than a remote possibility.	17-50%
4	Likely	The event will probably occur in most years and has occurred within RedR history. Knowledge or evidence either within RedR or within the industry suggests this event occurs at regular intervals.	51-84%
5	Almost Certain	This event is expected to occur in most circumstances. Has occurred within RedR within the last year. The occurrence of this event is common and expected.	> 85%

*In a calendar year.

Inherent/Residual Risk Levels (Risk Matrix). Risk levels are assessed by combining the impact of a given risk with the likelihood of it occurring. In this way the table below shows the risk grading of activities. The potential subjectivity of such quantification notwithstanding, using tables such as the below can be a useful means of identifying indicative levels of risk against which to contextualise the need to apply controls and/or reconsider activities.

		Impact (Consequence) Rating				
		(1) Insignificant	(2) Minor	(3) Moderate	(4) Major	(5) Catastrophic
Likelihood	(5) Almost Certain	(5) Moderate	(10) High	(15) Very High	(20) Extreme	(25) Extreme
	(4) Likely	(4) Moderate	(8) High	(12) Very High	(16) Very High	(20) Extreme
	(3) Probable	(3) Low	(6) Moderate	(9) High	(12) Very High	(15) Very High
	(2) Unlikely	(2) Low	(4) Moderate	(6) Moderate	(8) High	(10) High
	(1) Rare	(1) Low	(2) Low	(3) Low	(4) Moderate	(5) Moderate

Control Requirements/Risk Acceptability. The below table indicates a general expectation for corrective actions required (i.e. controls) relative to inherent/residual risk. This table is indicative only. Regardless of Risk Level, proportionate steps should be taken to minimise exposure to risk at all times in a given operation.

Risk Level	Actions/Acceptability
Low	Activity can proceed.
Moderate	Activity can proceed. Logic demonstrating a correlation between primary threats/hazards and reasonable actions to mitigate them exists, and all reasonable steps have been taken to lower risk.
High	Activity can proceed only if there is a clear logic demonstrating a correlation between primary threats/hazards and reasonable actions to mitigate them and all reasonable steps have been taken to lower risk. Where this is the case, activity may proceed with the stated caveat that the risk is acceptable <i>'within the context of a fully (UN) supported deployment to an environment acknowledged as being complex and potentially hostile'</i> .
Very High	Activity can generally not proceed until risk level is lowered. SMT permission could be sought for specific/reasoned exemptions only where justified by exceptional circumstances/mission criticality.
Extreme	Activity cannot proceed until risk level is lowered.

Annex C: Operational Risk Management Documentation Framework

Governance Level	Direction from Board			
Strategic Level	1. Risk Management Policy			
	1.1. Risk Register			
	1.2. Incident Log			
Policy Level	PREPARATION 2. Global Safety and Security Policy	PREPARATION 3. Training Course Risk Management Policy	RESPONSE/RECOVERY 4. Incident Response Handbook	REPORTING 5. Incident Reporting Policy
Implementation/Documentation	2.1. In-Country Support Guidelines	3.1. Course-Specific Risk Assessments*	4.1. Standard Operating Procedures*	5.1. Incident Reporting Form A
	2.2. Country Notes	3.2. Site-Specific Risk Assessments*	4.2. Field Connect Procedures	
	2.3. Field Mission Travel Request	Related policies: <ul style="list-style-type: none"> • MEAL Framework • HR (including Code of Conduct, Staff Travel Policy) • Finance and Administration (including IT) • Business Continuity Plan • OH&S • Communications (including Social Media) • Relevant national and international standards 		
	2.4. RedR Higher Threat SRA Template			
	2.5. Overseas Driving Policy/Request Form			

Policies/procedures in grey are to be drafted. Policies suffixed with an asterisk are currently being updated.

Annex D: Compliance notes on Risk Management Frameworks

There are many different risk management frameworks available to the risk manager. In Australia, AS/NZS/ISO 31000:2009 *Risk management - Principles and guidelines* (referred to herein as simply 'ISO 31000') is the Australian Standard risk management framework. ISO 31000 requires consideration of the following:

1. The mandate and commitment to risk management
2. Designing a framework for managing risk
3. Implementing a Risk Management Process
4. Monitoring and reviewing the framework
5. Continual improvement of the framework

FRAMEWORK FOR MANAGING RISK

Within the risk management framework provided by ISO 31000 is an additional framework for 'managing risk'. This requires consideration of the following:

- **Context.** Evaluating and understanding operational context
- **Risk management policy.** Establishing policy that states risk management objectives and commitments
- **Accountability.** Ensuring that those responsible for management of risk are appropriately competent, accountable and have the appropriate authority
- **Integrated processes.** Risk management processes are integrated and embedded into organisational practices and processes, so they are not separate from other practices and processes
- **Resourcing.** Adequate resources are allocated to risk management
- **Internal reporting and communication mechanisms.** Accountability and ownership of risk is supported and encouraged by establishing internal reporting and communication
- **External reporting and communication mechanisms.** Appropriate mechanisms are planned and implemented to communicate effectively with external stakeholders, including cases where there are legal or regulatory requirements

RISK MANAGEMENT PROCESS

Risk management processes involve systematic application of management policies, procedures and practices to the task of identifying, analysing, evaluating, treating and monitoring risk. While various models may achieve this goal, a Risk Management Process should incorporate the following steps:

- **Establish the context.** What is the purpose, who is involved, in what threat environment are they operating, what oversight is required and what equipment may be needed?
- **Identify all hazards and risks.** What could potentially cause harm or loss (see also Risk Identification Framework below)?
- **Assess the risks.** Assess and prioritise risks and address in priority order. What could happen and what might be the consequences?
- **Evaluate risks and control measures.** Assess and choose measures to control the risks. Can you eliminate, avoid, reduce or manage the risk?
- **Treatment of risks.** Implementing the appropriate control measures to manage the risks.
- **Monitor and review.** An ongoing process needs to monitor and review the risk and control measures (see also the Dynamic Risk Assessment framework below). Are the measures working, does the process meet relevant standards, what needs amending and/or are the activity goals or outcomes still being achieved?

Throughout the steps communication between all relevant stakeholders should occur. This enables important information to be shared and integrated into the Risk Management Process.

RISK IDENTIFICATION FRAMEWORK

Utilising specific, organisationally-appropriate risk categorisation can assist in the structured identification and management of risk. Consideration should be given to each of these risk categories in relation to the specific activities

being undertaken and the type of participants involved. This consideration of participants should extend to specific understandings of risk as heightened/mitigated relative to individual capabilities and experience.

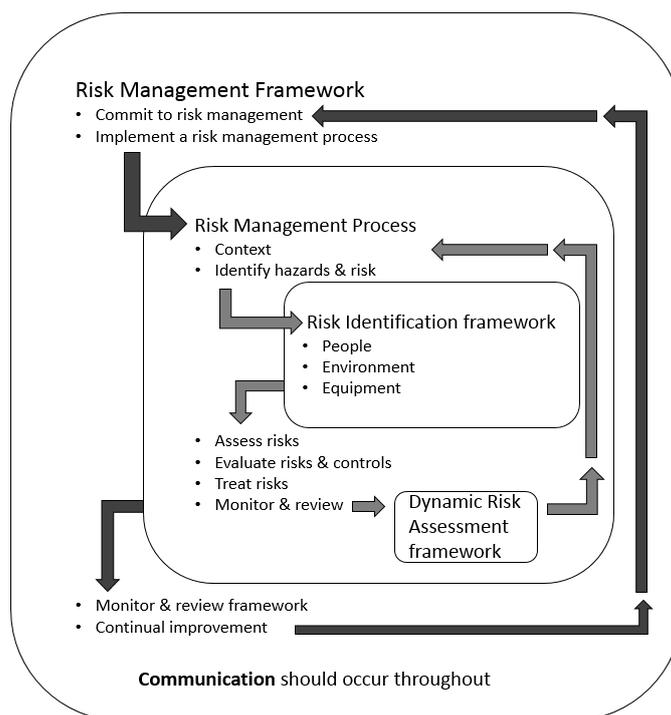


Fig.4: Risk Management Framework (ISO 31000:2009)

DYNAMIC RISK ASSESSMENT PROCESS

Hazards and risks are rarely static, and often change overtime; this calls for more dynamic forms of risk management that can assist in adapting formal, published risk assessments to the realities of operations at a given point and time. This furthermore reinforces the importance of maintaining situational awareness to identify and address hazards and risks using dynamic risk assessment.

The following diagram outlines a process of dynamic risk assessment:

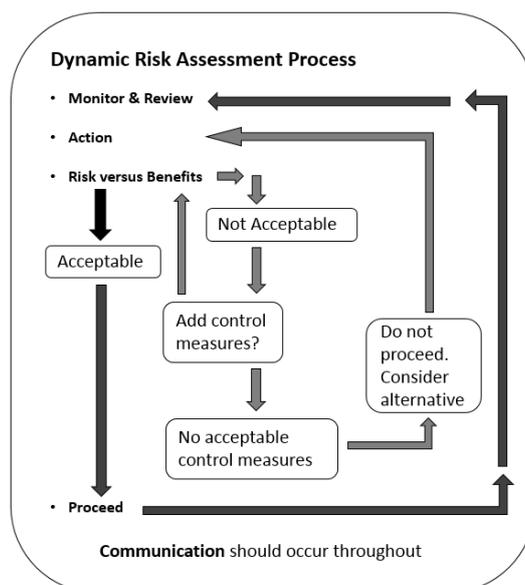


Fig.5: Dynamic Risk Assessment Process (ISO 31000:2009)

Dynamic risk assessment addresses the need to consider changes to risk over time, and (vitality) that have occurred since a more formal risk assessment process has taken place. It is not to be used as a reason to avoid actions identified in risk management plans, or to increase the level of risk participants are to be exposed to above the planned level in risk management plans.

Actions taken/the acceptable risk derived from a dynamic risk assessment should not:

- Increase the level of risk previously identified in the Risk Management Plan
- Increase the level of risk beyond individual/organisational risk appetites
- Negate or reduce the effectiveness of control measures identified in the Risk Management Plan

Dynamic risk assessment should be undertaken on an ongoing basis at all levels of an organisation.

RISK MANAGEMENT PLAN

By using the Risk Management Process and Risk Identification Framework, a 'Risk Management Plan' that identifies and treats risks can be completed. This is a key output from the Risk Management Process.

When developing and/or reviewing Risk Management Plans, consideration should be given to previous incidents and risk assessment outcomes that may include (and is not limited to):

- What has occurred within the organisation
- What is public knowledge (e.g. inquests) based on similar organisations' experiences
- What is public knowledge based on the type of organisational activity being undertaken
- What is public knowledge based on similar types of organisational activities to that being undertaken (e.g. remote work undertaken by the development, security or even leisure sectors).

RISK MANAGEMENT IMPLEMENTATION

Risk management is not something that stops after completing a Risk Management Framework and Plan. The Risk Management Plan actions need to be implemented and continually reviewed and adjusted. Any such review and adjustment during an activity is captured under the Dynamic Risk Assessment Process.