Australian Government
Great Barrier Reef Marine Park Authority

INTERNAL POLICY

Risk Management Policy (Revision 0)

***Target audience**: All workers of the agency, whether they undertake paid or unpaid work.*

Purpose

1. The purpose of this policy is to establish and maintain a system for the management of risks that complies with section 16 of the *Public Governance, Performance and Accountability Act 2013* and the Commonwealth Risk Management Policy.

2. The goals of this policy and the broader risk management framework are to explain the agency's approach to risk and the responsibilities of workers, and to enable effective risk management, so that:
   (a) decisions are transparent, defendable and contribute to organisational viability and development
   (b) resources are directed towards threats to the achievement of corporate plans, operational plans, and other objectives of the agency
   (c) the quality of the agency's work and internal controls continuously improves
   (d) exposure to possible litigation, operational disruption and other losses are minimised
   (e) a culture that rewards reporting can be supported
   (f) stakeholder and public confidence is sustained.

Context

What is risk?

3. '**Risk**' means the effect of uncertainty on objectives[1], usually expressed as the likelihood that particular consequences will be experienced.

   (a) 'Effects' mean a deviation from the expected, and may be positive or negative[3].

   Note: Although the explicit management of positive effects is not within the scope of this policy, where the effects of risks may present an opportunity, an explanation of this information should be provided so fully informed decisions can be made.

   (b) Objectives can relate to specific disciplines (e.g., financial, safety, environmental), apply at different levels (e.g., strategic, operational, tactical, project or process) and be expressed using other terms (e.g., purpose, outcome, aim, goal or target)[1].

4. '**Risk management**' means coordinated activities to direct and control an organisation with regard to risk[1]. In practice, risk management can be viewed as the principles, framework and processes applied to reduce how often risks eventuate and/or how serious their effects are.

Why we manage risk

5. All activities in the agency involve risk that must be managed, and managing risk is an essential part of good governance that can help decision-makers to make informed choices, prioritise work and take the most appropriate courses of action. The agency's risk management processes therefore should be considered as part of the normal system of decision-making and management.

6. Consistently applying the principles and processes described by this policy allows workers to manage any form of risk in a systematic, transparent and credible manner within any scope and context — and doing so helps to ensure that risks are managed effectively, efficiently and coherently across the organisation.

The agency's risk management framework

7. As shown by Figure 1, the agency's risk management framework consists of this policy, the Risk Management Framework Guideline (and other internal procedures developed for the assessment of specific risk types), and templates and tools such as the agency's risk register, risk assessment tools, action plans / risk management plans, and risk / hazard reporting forms.

Figure 1: Risk management framework

8. This framework collectively explains the agency's overall approach to managing risk and provides the foundations for the design, implementation, monitoring, review and continuous improvement of risk management[2].

9. This policy forms a part of the agency's internal controls and governance practices, and as such should be read in the context of the Great Barrier Reef Marine Park Authority's Corporate Plan and Agency Operating Plan (as amended from time to time).

Definitions

10. Commonly used terms have been defined within Appendix 1 of this policy.

Related legislation/ standards/ policy

- *Public Governance, Performance and Accountability Act 2013*
- *Great Barrier Reef Marine Park Authority Act 1975*
- *Work Health and Safety Act 2011*
- Commonwealth Risk Management Policy
- Commonwealth's Protective Security Policy Framework
- AS/NZS ISO 31000:2009 Risk Management – Principles and Guidelines
- The agency's Accountable Authority Instructions

Policy statements

Principles of risk management

11. All specific risk management approaches in the agency must be consistent with the principles[1] in Table 1 which outline the core ideals to be considered when undertaking any risk management activities, and contribute to the development of a positive risk culture which the agency seeks to enhance.

Table 1: Principles of risk management[1]

Risk management processes must:	
Principle 1	**create and protect value**, contributing to the achievement of agency objectives
Principle 2	be **integrated into everyday business** and not act as a stand-alone activity
Principle 3	provide **rigor to decision-making** by enabling transparent, informed choices
Principle 4	**explicitly take account of uncertainty** to reduce the probability and/or consequences of unforeseen events, and reduce effort spent in crisis management
Principle 5	be **systematic, structured and timely** to foster a proactive culture with reliable outcomes
Principle 6	be **based on the best available information and data**
Principle 7	be **tailored** to the agency's internal and external contexts
Principle 8	**take into account human and cultural factors**
Principle 9	be **transparent and inclusive** so relevant views are accounted for, as appropriate
Principle 10	be **dynamic and responsive** to change
Principle 11	**facilitate continuous improvement**, so service provision is of a high quality and public confidence is maintained.

Processes of risk management

12. All risk management approaches in the agency should include processes for communicating and consulting, establishing the context, assessing (which consists of identifying, analysing and evaluating risks), responding/ managing risks, and monitoring and reviewing risks.

13. Figure 2 provides the aim of each of these processes, and shows their relationship within the framework and principles of risk management. The internal 'Risk Management Framework Guideline' provides more information on how to implement each of these processes.

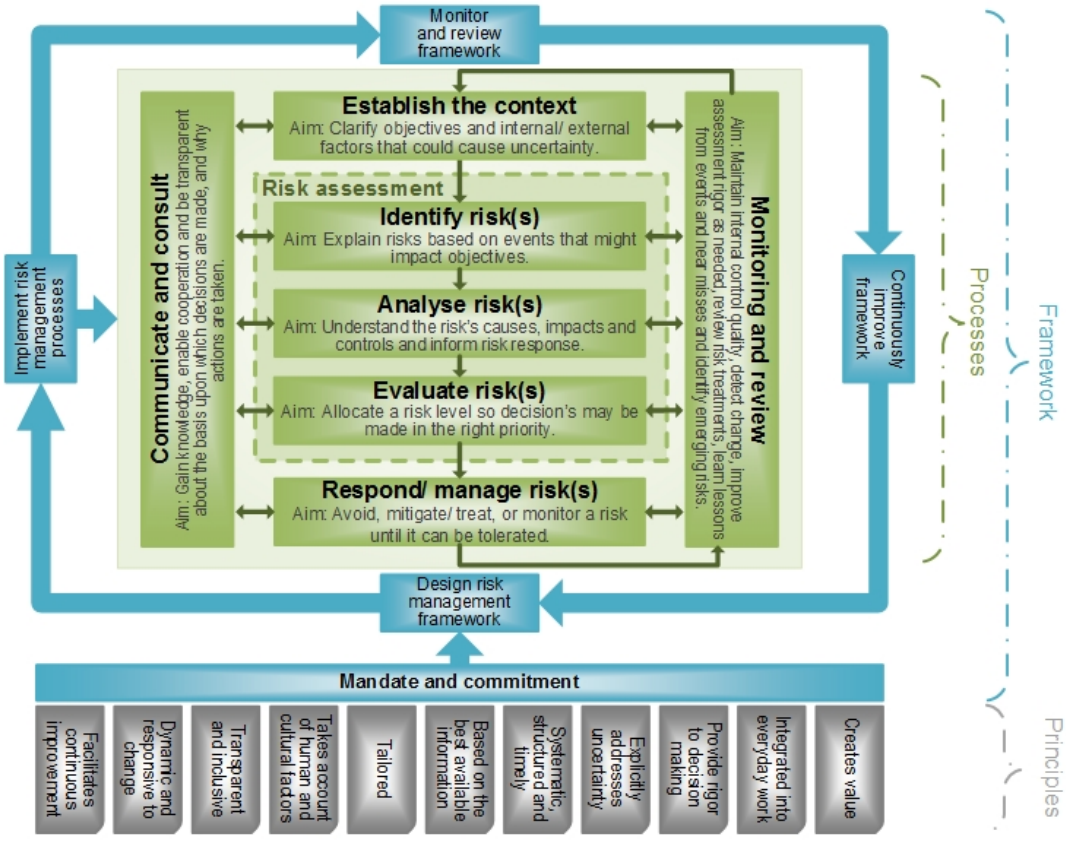

Figure 2: AS/NZS ISO 31000:2009 Risk management principles, framework and processes

Integrating processes of risk management across the agency

14. Risk management processes are not isolated practices — they provide a structured framework for considering everything the agency does and for circumventing problems before they occur.

15. The management of risk should be considered when decisions are made for new systems of work, new equipment use, procurement, capital development, information technology, contractor management, security management, fraud management, work health and safety, workforce management, financial planning and all other areas of operation.

16. Risk management approaches that are consistent with the principles and processes outlined within this policy should be particularly included as a part of:
    (a) planning (strategic, tactical, operational, project and procurement)
    (b) processes for establishing and managing governance arrangements
    (c) policy development and program/project delivery
    (d) day-to-day decision-making.

Reporting, escalating and day-to-day risk management

17. The purpose of reporting and escalating risks is to communicate what could go wrong so proactive action can be taken to reduce possible impacts. Reporting and escalation of risks contributes to effective agency performance by allowing informed decisions to be made.

18. **Reporting** generally involves informing higher levels of authority of risks identified, and what is being done to manage them to tolerable levels, so risk-informed decisions can be made.

19. **Escalating** generally involves transferring risk ownership when higher levels of authority are required to enable decision-making in relation to the management of risks.

20. All workers in the agency have a responsibility for the day-to-day management of risks[2], which includes risk reporting and escalation. To meet this responsibility all workers should:
    (a) be aware of opportunities to identify risks within the agency, and the tools available to document, report and escalate these (e.g., risks may be identified by planning activities or projects, procuring resources or services, identifying hazards, findings from audits and investigations into incidents and near miss events, trends in data, risks escalated within the agency or reported by external people, and reviewing risks that have happened elsewhere)
    (b) when a risk or hazard is identified, take any safe and lawful action necessary to reduce any immediate threat (within the scope of their role, delegations and level of authority)
    (c) escalate to their line manager any risk that is **A**-**B**-**C** (i.e., those that could happen **A**nywhere/time else – especially if the risk is a high level; those outside a worker's **B**udget to manage; or those beyond a worker's **C**ontrol/ level of delegation or authority to manage)
    (d) report to their line manager how risks that are *not* **A**-**B**-**C** have been managed to tolerable levels, considering the agency's risk appetite statement
    (e) report incidents and near misses as soon as possible to the appropriate area or level in the agency
    (f) share information with those who have a demonstrated need to know, so risk management decisions can be appropriately informed.

21. Where an approved internal procedure dictates that a specific process or format should be used for risk reporting or escalation, this should be utilised. Where there are no such specifications, risks should be communicated by any method that enables the following information to be understood[1]:
    (a) The source(s) of risk and the causes/ sequences that may lead to events
    (b) Consequences that may occur, their magnitude and how likely the risk could eventuate
    (c) The controls that exist and how effectively and reliably they act on the risk

(d) The level of risk and how sensitive it is to any assumptions made in determining consequence and likelihood

(e) Where risk treatment (if required) should be directed, and

(f) Where relevant, any potential limitations, uncertainty or concerns regarding the availability, quality and ongoing relevance of data, information, modelling, and expert judgement used.

Agency risk register

22. Risk registers are a tool that can be used to assist prioritisation of risks and the appropriate allocation of resources. They are dynamic in nature and should be used to support decision making and high level visibility (in key committees/ meetings) of risks that have the potential for the most severe consequences.

23. Accordingly, the agency will maintain a register of its most serious risks (high and very high risks) to facilitate regular discussion and decision-making about whether controls remain appropriate, whether treatments are working, and to identify situations where additional treatments may become available[6].

24. Risks which should be added to this overarching risk register are those that are a 'high' or 'very high' level; require a higher level of monitoring; or those that may require escalation to a Minister or the Parliament.

25. A decision to add a risk to the agency's risk register may be made individually, by a member of the Executive Management Group (where accountability and authority is clearly one position), or collaboratively within Executive Management Group and/or Senior Management Team meetings, but must be informed by a documented risk assessment.

26. When risks on the agency's risk register are no longer relevant, no longer exist or have been mitigated to a point where they can be tolerated, active management of the risk may cease and they may be 'retired' from the register. Retired risks should not be removed from risk registers, but their 'retired' status identifiable. Retired risks may be reactivated in the event of a change in objectives, context or other circumstances.

27. The agency's overarching risk register must be kept up to date and reviewed regularly (usually every three months).

External and shared risks

28. A shared risk is one with no single owner, where more than one entity is exposed to or can significantly influence the risk. Shared risks may extend across entities, and may involve other sectors, the community, industry or jurisdictions[2].

29. All workers should report to their line manager identified risks that the agency has no, little, or a shared jurisdiction to manage, so all relevant information can be communicated as quickly as possible (by an appropriately authoritative position) to relevant parties, and responsibilities for managing the risk agreed[2].

30. Where possible, the agency should seek to conduct any joint risk management processes in a manner consistent with the principles and processes of risk management, as outlined within this policy.

Risk appetite and tolerance

31. **Risk appetite** refers to the amount and type of risk that an organisation is willing to pursue or retain[3], in order to achieve its objectives, and is used in the agency to broadly describe attitudes towards risk taking.

32. **Risk tolerance** refers to the level of risk that is acceptable to achieve a specific objective or manage a category of risk[2], and may be viewed as the practical application of risk appetite[4] – or the level at which the agency is ready to bear the consequences should the risk eventuate.

33. Together, risk appetite and tolerance form the key components of the agency's 'risk appetite statement'[4]. The agency's risk appetite statement at Figure 3 is endorsed by the Accountable Authority and may be amended to respond to changes in the operating environment.

Risk Appetite Statement

The agency operates in a complex and challenging environment to manage the Great Barrier Reef Region, involving responsibilities to maintain the area's natural and cultural integrity, while allowing sustainable use.

The size and diversity of the Reef ecosystem, its economic importance, state, local, national and international interests, and jurisdictional, biophysical and social complexities call for a flexible approach to risk management. Although the amount of acceptable risk that may be taken depends on the context and objectives of the work, in general for risks involving consequences to:

- *legal and contractual obligations and/or the physical and psychological health and safety of workers and visitors, the agency has a risk averse appetite, tolerating as little risk as possible. This means that actions to respond to the risk should consider avoiding or mitigating the impacts to so far as is reasonably practicable*
- *the biodiversity or heritage values of the Great Barrier Reef Region, the agency has a moderately risk averse appetite with a cautious approach towards risk taking. This means that actions to respond to the risk should consider avoiding, mitigating or offsetting the impacts to a level where the condition of values are maintained or improved to 'good' or 'very good' levels (as defined by Great Barrier Reef Outlook Report assessment grades)*
- *all other consequences types, the agency has a neutral risk appetite, with a balanced approach to risk taking. This means that actions to respond to the risk should consider reasonably practicable mitigation, taking account of management priorities and potential outcomes.*

Figure 3: Risk appetite statement for the Great Barrier Reef Marine Park Authority

34. Tolerating a risk typically means that no (or no further) treatments are going to be applied, on the understanding that the risk should still be routinely reviewed for as long as it remains relevant to the agency. Tolerating a risk does not imply that it is insignificant, rather tolerance may be chosen either because:

(a) the level of risk is so low that treatment would not be reasonably practicable;

(b) the nature of the risk is such that no treatment options are available; or

(c) the opportunities outweigh the consequences to such an extent that the risk is justified.

35. An informed decision to tolerate a risk may be made by a "risk owner", once all of the following conditions have been met:

(a) Action to minimise the risk to so far as is reasonably practicable has been implemented, and where it applies the *Reef 2050 Plan Policy Guideline for Decision Makers* has been considered
(**Note**: Guidance to determine whether the *Reef 2050 Plan Policy Guideline for Decision Makers* applies is included within the guideline)

(b) Regular monitoring processes (proportionate to the level of risk) have been integrated into everyday work to enable early warning of the risk worsening or eventuating, and where reasonably practicable contingency plans/processes have been developed and routinely tested

(c) The risk has been appropriately documented (e.g., within a risk assessment or a risk management plan) and reported.

Developing the agency's risk culture

36. Organisational culture is fundamental to the agency achieving effective risk management outcomes. Culture defines what the agency is, what it stands for, what it considers important, the way workers are expected to behave, how things are done, and it influences the feelings that people have about the organisation.

37. Within their day-to-day work, all workers in the agency, particularly those who manage others, must encourage, model and reward the attributes of a positive risk culture (as outlined within Table 2), so an open and proactive approach to reporting, escalating and managing risks can be developed[2].

Table 2: Attributes of risk management culture the agency seeks to develop, and how this should be encouraged

Attributes to be developed	Processes, behaviours and mechanisms to encourage attributes[5]
1. Risk management is proactive and informed Aim: to proactively identify risks through regular monitoring of data/ performance measures, and to communicate information to where it's most useful.	• As part of normal business practice, regularly monitor performance data and information. • Establish processes that allow information to flow in the most efficient way to the person most informed and best placed to advise on a plan of action. • Encourage, reward and resource the reporting and investigation of near-miss events – especially those that could have had significant impacts.
2. Action is timely and sustainable Aim: to seek and take account of the views of operational staff so risks can be 'engineered out' at the design stage, and sustainable solutions identified.	• Proactively seek views of operational workers, empowering them to contribute their own perspectives to the design of new programs, projects and ways of working. • Clearly communicate expectations that all workers identify and respond to risks in their own sphere of influence (rather than assuming responsibility always sits with senior managers), and reward when this happens.
3. Good behaviours are rewarded Aim: to appreciate and take seriously the concerns of all workers, so engagement in risk management processes and continuous improvement is maintained.	• Clearly communicate expectations that: - workers inform themselves of who to approach if they need help in managing risks - when workers identify problems or seek help, they should receive support to mitigate impacts as early as possible. • Every time workers appropriately reports risks, engage with them so they know their concerns will be taken seriously, appropriately addressed if needed, and appreciated.

Accountabilities/ responsibilities

38. All workers of the agency must comply with the accountabilities and responsibilities outlined within Table 3, noting that some workers will have more than one set of obligations.

Table 3: Table outlining accountabilities and responsibilities for risk management

Who	Accountability / responsibility	In practice (what does this mean for me?)
All workers	1) Within the scope of their role, delegation(s) and level of authority, responsible for integrating the processes of risk management into their everyday work, as per this policy.[2] 2) Responsible modelling and demonstrating the attributes of a positive risk culture in a strong and sustained way.[2,6] 3) Within the scope of their role, delegation(s) and level of authority, responsible for the day-to-day management of risks by[2]: a. communicating and consulting about risks so transparent, complete and timely information can inform decisions b. assessing and responding to risks in a manner consistent with the agency's risk appetite c. reporting and escalating risks and hazards in a timely manner, to the responsible person d. contributing to the understanding of 'shared' risks (i.e., those that likely require management across entities, sectors, industries and/or jurisdictions) e. complying with the Commonwealth Risk Management Policy, this policy[7] and other procedures or strategies implemented for the management of risks, and f. maintaining a risk management capability commensurate with the agency's resources and the nature and scale of risks being managed[2].	☐ Where needed (normally when a decision needs to be made), integrate risk identification and management processes into your day to day work. ☐ Model the behaviours of a positive risk culture (Table 2), and always report risks and near misses. ☐ When you identify a risk or hazard, take any safe and lawful action necessary to reduce any immediate threat, document the risk assessment and any corresponding action taken so far (if any), and make it a record. ☐ Escalate risks that are **A**-**B**-**C** to manage (that is, risks that could happen **a**nywhere/time else, are outside your **b**udget to manage, or beyond your **c**ontrol (level of delegation/authority), and for risks that are *not* **A**-**B**-**C**, consider the risk appetite statement and manage risks until they can be tolerated. ☐ Share information with those who need to know so shared risks can be managed well. ☐ When incidents and near misses occur, report these as soon as possible to the appropriate area/ level in the agency. ☐ Be aware of your responsibilities, and the tools and templates in place for risk management, and make the most of opportunities to attend training or build on your experience/ knowledge.
All workers **supervising** others	As per all workers, plus: 4) Responsible for managing non-compliance with the mandatory elements of this policy and for nurturing a culture which supports and rewards the reporting of risks and hazards.	As per all workers, plus: ☐ Be aware of the contents of this policy, discuss it with your staff and encourage them to expand their knowledge/ experience in risk management. ☐ When risk assessments are escalated to you, report back down any changes made (which should only be made to improve the defensibility of the assessment) and any agreed actions to be implemented. ☐ Manage performance that contradicts this policy or the behaviours of a positive risk culture, and recognise/reward those who report risks and near misses to you.

Who	Accountability / responsibility	In practice (what does this mean for me?)
Workers of the **Governance Support Unit** (and their responsible Director)	As per all workers, plus: 5) Responsible for establishing and regularly reviewing a risk management policy that: a. defines the agency's approach to risk management and how it supports strategic objectives b. defines the agency's risk appetite and tolerance (as determined by the Accountable Authority) c. outlines key accountabilities and responsibilities for risk management, and d. is endorsed by the Accountable Authority[2]. 6) Responsible for developing, assisting to integrate, and encouraging the use of risk management templates and tools that support the risk management framework. 7) Responsible for adding risks to the agency's risk register when it is: a. requested by the Accountable Authority, Executive Management Group or Senior Management Team, *and* b. informed by a documented risk assessment/ risk management plan. 8) Responsible for providing support and advice as needed on risk management processes and tools. 9) Responsible for supporting regular review and improvement of the risk management framework.	As per all workers, plus: ☐ Develop and regularly review a risk management policy (and the other associated components of the risk management framework) that complies with legislative obligations and is endorsed by the Accountable Authority. ☐ Model the behaviours of a positive risk culture (Table 2), and in particular encourage the use and integration of suitable tools and templates for risk management, providing advice and education as needed. ☐ Add risks to the risk register when requested, but only when informed by a suitably documented risk assessment. ☐ Look for opportunities to encourage regular review and improvement of the risk management framework (e.g., preparing and responding to Comcover's Risk Management Benchmarking Survey, integrating auditing of risk into Strategic Internal Audit Plans). ☐ Provide support and information about the agency's risks and broader risk management framework to those that seek it (e.g., the Board, the Audit Committee, Comcover).
All workers who form a part of the **Senior Management Team** (**SMT**) (generally those at Executive Level 2)	As per all workers and supervisors, plus: 10) Responsible for developing and regularly (usually quarterly, but may be more or less frequent, depending on the risk level) monitoring risk assessments and risk management plans within their area of responsibility in order to: a. detect changes b. review the ongoing validity of any assumptions made c. maintain an understand of these risks d. assure their management is consistent with the agency's risk appetite statement, and e. within their scope, delegation(s) and level of authority, make any necessary adjustments to risk management actions. 11) Responsible for providing the Governance Support Unit completed risk assessments (within their area of responsibility) for risks that the SMT have agreed by consensus	As per all workers and supervisors, plus: ☐ Document and regularly review risk assessments for risks actively being managed. Review risk assessments escalated to you to, assuring their evidence-base and defensibility, and escalate **A**-**B**-**C** risks and/or raise them within SMT meetings. ☐ When SMT agree that a risk should be included on the agency's risk register, provide completed risk assessments (within your area of responsibility) to the Governance Support Unit, copying in the relevant member of EMG. ☐ When you can add value, contribute to discussions about risks and risk assessments within Senior Management Team (SMT) meetings, so risk levels and management actions can be agreed by consensus. ☐ Implement any actions within your area of responsibility that are agreed to for the management of risks, regularly review progress made and check that changes have had the desired effect.

Who	Accountability / responsibility	In practice (what does this mean for me?)
	should be included on the agency's risk register. **Decision support**: Risks which should be added are those that are a 'high' or 'very high' level; require a higher level of monitoring; or may require escalation to a Minister or the Parliament. **Note**: A decision to add a risk to the agency's risk register may be made either: a. by a member of the EMG where accountability and authority is clearly one position, or b. by consensus agreement within SMT or EMG meetings. 12) Responsible for implementing actions that aim to systematically improve the agency's risk management framework so it can mature[2] and adapt to a changing environment.	☐ Implement any actions within your area of responsibility that are agreed to for the improvement of the risk management framework, regularly review progress made and check that changes have had the desired effect.
All workers who form a part of the **Executive Management Group** (**EMG**) (generally those at Senior Executive Services level)	As per all workers, supervisors, and SMT, plus: 13) Responsible for regularly (usually quarterly) reviewing the agency's risk register in order to: a. detect changes b. review the ongoing validity of any assumptions made c. maintain a broad understanding of the agency's risks d. assure their management is consistent with the agency's risk appetite statement, and e. make any necessary adjustments to risk management actions. 14) Responsible for facilitating opportunities for systematic improvement the agency's risk management framework so it may mature[2] and adapt to a changing environment.	As per all workers, supervisors, and SMT, plus: ☐ Regularly review the agency's risk register to assure any underpinning evidence-base is accurate and defensible, and to decide on any necessary adjustments/ prioritisation of actions. **HINT**: Integrating review of the risk register into minuted EMG meetings enables a record of discussion to be made, and achieves risk management principle two. ☐ Communicate back to SMT decisions made regarding the management/ tolerability of risks on the agency's risk register. ☐ When it has been agreed to add a risk to the agency's risk register, provide the completed risk assessment to the Governance Support Unit, copying in the relevant Director(s). ☐ When EMG have agreed to escalate an **A**-**B**-**C** risk to the Minister or an external entity, review the corresponding risk assessment to assure its evidence base and defensibility, and to ensure that wording doesn't leave the agency vulnerable to other risks. ☐ Look for opportunities to regularly review and improve the risk management framework (e.g., reviewing and approving responses to Comcover's Risk Management Benchmarking Survey, approving internal audits of risk management and acting on accepted recommendations, responding to Audit Committee recommendations, reviewing and responding to trends in near misses/ data/ performance).

Who	Accountability / responsibility	In practice (what does this mean for me?)
The agency's **Audit Committee**	As per all workers, plus: 15) Responsible for reviewing the appropriateness of the agency's system of risk oversight and management and system of internal control[8], and making recommendations for improvement if required.	As per all workers, plus: ☐ Look for opportunities to regularly review the risk management framework to assure it is appropriate and operationally effective, making recommendations as needed. (E.g., Review findings of Comcover's Risk Management Benchmarking Survey; assure regular internal audit of risk management and internal controls; review high risk projects/programs; complete Audit Committee checklists).
The **Accountable Authority** (generally, the agency's Chairperson)	As per all workers, supervisors, SMT and EMT, plus: 16) Accountable for establishing and maintaining an appropriate system of risk oversight and management for the agency.[9] 17) Accountable for endorsing the agency's risk management policy and framework, and for determining the agency's risk appetite and tolerance in consultation with the senior executive.[2,10] 18) Accountable for championing the processes of risk management and the tools that operationalise them, and for modelling the attributes of a positive risk culture in a strong and sustained way.[2,6] 19) Responsible for the agency's performance in managing risk.[2]	As per all workers, supervisors, and SMT, and EMG plus: ☐ Demonstrate endorsement of the agency's risk management policy and framework by approving them. ☐ Determine and widely communicate the agency's risk appetite and tolerance. ☐ Explicitly champion the use of common risk tools and templates that can be incorporated into every-day activities. ☐ Look for opportunities to champion embedding risk management into: a. governance arrangements (e.g., internal and external meetings, delegation arrangements, key positions within the agency) b. corporate planning c. projects, programs and activities involving significant change d. audit and assurance programs. ☐ Discuss the agency's key strategic risks with the responsible Minister as necessary. ☐ Personify the behaviours of a positive risk culture (Table 2), ensure any behaviour that contradicts these are swiftly managed, and in particular celebrate quick wins as soon as they occur – highlighting instances where embedding risk management resulted in innovative outcomes or other benefits to the agency.

Appendix 1 – Definitions

Biodiversity	Means the variability among living organisms from all sources (including terrestrial, marine and other aquatic ecosystems and the ecological complexes of which they are part) and includes diversity within species, and diversity of ecosystems.[11]
Consequence	Means the outcome of an event affecting objectives. Consequences may be certain or uncertain and can have positive or negative effects on objectives.[3]
Control [Sometimes called 'risk controls' or 'internal controls']	Means a measure that is modifying risk[3]. Controls take many forms and can include any process, policy, device, practice, or other action that is modifying the causes or consequences of risk (e.g., tangible devices such as software or hardware, minimum criteria, specified skill sets, rules, specified work methods/ procedures, mandated processes/ policies, specific roles, personnel and systems of management)[6]. An integrated system of internal controls reduces the risks an entity must overcome to achieve its objectives[12].
Ecosystem	Means a dynamic complex of plant, animal and microorganism communities and their non-living environment interacting as a functional unit.[11]
Escalation [of risk]	Means a process to transfer risk ownership when higher levels of authority are required to enable decision-making in relation to the management of risks.
Event	Means one or more occurrence(s) or change of a particular set of circumstances. An event can consist of something not happening and can have several causes.[3]
Heritage values	Means the heritage values of the Great Barrier Reef Region that underpin Matters of National Environmental Significance and include Indigenous heritage values, other heritage values, world heritage values, National heritage values and Commonwealth heritage values of the region.[13]
Hazard	Means a source of potential harm.[3]
Incident	For the purpose of this policy means an event which leads to one or more consequences[3]. In simple terms, an incident is a risk (identified or not) that eventuates with effects that can vary in magnitude from an issue to an emergency or disaster situation.
Likelihood	Means 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 probability or frequency over a given time period).[3]
Near miss	Means an event without consequences.[3]
Reasonably practicable	In the context of this policy, has a meaning adopted from s18 of the *Work Health and Safety Act 2011*, and is taken to mean that which is, or was at a particular time, reasonably able to be done to eliminate or minimise a risk, taking into account and weighing up all relevant matters including: (a) the likelihood of the event or risk concerned occurring; and (b) the consequences that might result from the event or risk; and (c) what a person concerned knows, or ought reasonably to know about the event or risk, and ways of eliminating or minimising it; and (d) the availability and suitability of ways to eliminate or minimise the risk; and (e) after assessing the extent of the risk and the available ways of eliminating or minimising it, the cost associated with available ways of eliminating or minimising the risk, including whether the cost is grossly disproportionate to the risk.

Reporting [of risk]	Means a process to inform higher levels of authority of risks identified, and what is being done to manage them to tolerable levels, so risk-informed decisions can be made.
Risk	Means the effect of uncertainty on objectives, usually expressed as the likelihood that particular consequences will be experienced[6], where: (a) effect is the deviation from the expected (positive or negative)[3] (b) uncertainty is the state (or partial state) of deficiency of information related to, understanding or knowledge of an event, its consequences or likelihood[3] (c) objectives are the result(s) to be achieved. An objective may: • relate to different disciplines (such as financial, safety and environmental objectives) • apply at different levels (such as strategic, organisation-wide, tactical, operational, project or process), and • be expressed in other ways 9such as an intended outcome, a purpose, an operational criterion) or by the use of other words with a similar meaning (e.g., aim, goal, target).[14]
Risk appetite	Means the amount and type of risk that an organisation is willing to pursue or retain[3].
Risk culture	Means the shared attitudes, values and behaviours that characterise how the agency considers risk in its day-to-day activities. A positive risk culture is one where risk is appropriately identified, assessed, communicated and managed across all levels of the agency.[2]
Risk management	Means coordinated activities to direct and control an organisation with regard to risk.[1]
Risk management plan	Means the approach, procedures, practices, assignment of responsibilities, resources, sequences and timing of activities applied to the management of risk (at product, process, project or organisation-wide levels).[3]
Risk owner	Means a person or entity with the accountability and authority to manage a risk.[2]
Risk register	Means a record of information about identified risks.[3]
Risk tolerance	Means the levels of risk taking that are acceptable in order to achieve a specific objective or manage a category of risk[2], and when applied may be viewed as the agency's readiness to bear the risk [usually] after treatment[3].
Shared risk	Means a risk with no single owner, where more than one entity is exposed to or can significantly influence the risk. Shared risks may extend across entities and may involve other sectors, the community, industry or jurisdictions.[2]
Treatment [of risk]	Means a measure to modify risk[3]. A risk treatment differs from a risk control in that it has not yet been applied.
Worker	Means a person who carries out work in any capacity for the agency, including work as an employee, contractor or subcontractor, an employee of a contractor or subcontractor, an employee of a labour hire company who has been assigned to work for the agency, an outworker, an apprentice or trainee, a student gaining work experience, a volunteer, or a person of a class prescribed by the *Work Health and Safety Act 2011*.

References/ related material

1 Standards Australia/ Standards New Zealand. 2009, *AS/NZS ISO 31000:2009 Risk Management - Principles and Guidelines*, Standards Australia, Sydney, NSW

2 Department of Finance, Business, Procurement and Asset Management. 2014, *Commonwealth risk management policy*, Commonwealth of Australia, Parkes, ACT

3 International Standards Organisation. 2009, *ISO Guide 73 Risk management - vocabulary*, International Standards Organisation, Switzerland.

4 Department of Finance. 2016, *Understanding Risk Appetite and Tolerance Information Sheet*, Commonwealth of Australia, Parkes, ACT

5 Shergold, P. 2015, *Learning from failure. Why large government policy initiatives have gone so badly wrong in the past and how the changes of success in the future can be improved*, Australian Public Service Commission (Commonwealth of Australia), Canberra, ACT

6 Standards Australia/ Standards New Zealand. 2013, SA/SNZ HB 436:2013 *Handbook risk management guidelines - Companion to AS/NZS ISO 31000:2009*, Standards Australia Limited/ Standards New Zealand, Sydney, NSW

7 Department of Finance, Public Management Reform Agenda. 2016, *Resource Management Guide No. 206 – Model accountable authority instructions – non-corporate Commonwealth entities*, Commonwealth of Australia, Forrest, ACT

8 *Public Governance, Performance and Accountability Rule 2014*, Rule 17 Audit committee for Commonwealth entities

9 *Public Governance, Performance and Accountability Act 2013*

10 Department of Finance, Commercial and Government Services. 2016, *Implementing the Commonwealth Risk Management Policy – Guidance. Resource Management Guide 211*, Commonwealth of Australia, Forrest, ACT

11 *Environment Protection and Biodiversity Conservation Act 1999*

12 Standards Australia. 2005, *Governance, Risk Management and Control Assurance*, HB 254-2005, Standards Australia, Sydney, NSW.

13 *Great Barrier Reef Marine Park Regulations 1983*

14 Standards Australia/ Standards New Zealand. 2016, AS/NZS ISO 9000:2016 *Quality management systems – Fundamentals and vocabulary*, Standards Australia, Sydney, NSW.

Document Control Information			
Approved by:	*Accountable Authority (PN1)*	*Approved date:*	*26-May-17*
Last reviewed:	*26-May-17*		
Next review:	*26-May-20*		
Created:	*26-May-17*		
Document custodian:	*Manager, Governance Support (PN 422)*		
Replaces:	*New*		